Державний торговельно-економічний університет

В. І. Чубаєвський

КОРПОРАТИВНА ІНФОРМАЦІЙНА БЕЗПЕКА

Монографія

Київ 2022

УДК 004.056.55
Ч-81

Автор В. І. Чубаєвський, канд. політ. наук, доц.

Рецензенти: М. І. Цюцюра, д-р техн. наук, проф. каф. інформаційних технологій Київського національного університету будівництва і архітектури;
С. І. Мельник, д-р екон. наук, завідувач каф. фінансів та обліку Інституту управління, психології та безпеки Львівського державного університету внутрішніх справ;
С. В. Демедюк, канд. юрид. наук, заступник Секретаря Ради національної безпеки і оборони України;
С. І. Бай, д-р екон. наук, проф., завідувач каф. менеджменту Державного торговельно-економічного університету

Рекомендовано до друку вченою радою Державного торговельно-економічного університету
(протокол № 7 від 30 червня 2022 р.)

Чубаєвський В. І.

Ч-81 Корпоративна інформаційна безпека : монографія / В. І. Чубаєвський. – Київ : Держ. торг.-екон. ун-т, 2022. – 272 с.

ISBN 978-966-918-054-4
DOI: 10.31617/m.knute.2022-242

У монографії розглянуто сутність та детермінанти управління корпоративною інформаційною безпекою підприємства в умовах глобальних викликів XXI століття. Здійснено компаративний аналіз еволюції та тлумачення структури корпоративного інформаційного простору, стану й тенденцій інформаційних загроз розвитку та функціонуванню бізнесу. Досліджено трансформацію видів економічної ефективності діяльності підприємств під впливом цифровізації економіки. Представлено концепцію формування корпоративної інформаційної безпеки. На основі дослідження світових та вітчизняних тенденцій розвитку системи захисту корпоративної інформації обґрунтовано пріоритети у виборі політики інформаційної безпеки, критерії та показники оцінки її економічної ефективності. Шляхом розкриття демаскувальних ознак конфіденційних корпоративних даних представлено інструментарій ідентифікації несанкціонованого доступу до корпоративної інформації, дієві засоби оцінювання економічної ефективності її захисту та контролю.

Для працівників органів державного управління, науковців, викладачів, аспірантів і студентів закладів вищої освіти економічного профілю, а також для практичних дослідників у сфері економічної та інформаційної безпеки бізнесових структур.

УДК 004.056.55

ISBN 978-966-918-054-4

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЕМ – Event Management (управління подіями)
АІБ – аудит інформаційної безпеки
АС – автоматизовані системи
БМ – байєсівські мережі
ЕК – елементарні класифікатори
ЖЦ – життєвий цикл
ЗОТ – засоби обчислювальної техніки
ЗЗІ – засоби захисту інформації
ЗІ – захист інформації
ІІС – інтелектуальні інформаційні системи
ІБ – інформаційна безпека
ІКТ – інформаційно-комунікаційні технології
ІР – інформаційні ресурси
ІС – інформаційні системи
ІТ – інформаційні технології
КВІ – канали витоку інформації
КІС – корпоративні ІС
МАІ – метод аналізу ієрархій
НЛ – нечітка логіка
НСД – несанкціонований доступ
ОБІ – об’єкт інформатизації
ПЕМВН – побічне електромагнітне випромінювання та наведення
ПІБ – політики інформаційної безпеки
ПЗ – програмне забезпечення
ПС – простір станів
РОМ – розподілені обчислювальні мережі
СЗІ – системи захисту інформації
СППР – системи підтримки прийняття рішень
СУІБ – системи управління інформаційною безпекою
ТЗР – технічні засоби розвідки
ТКПІ – технічні канали передавання інформації
ТСЗІ – технічні системи захисту інформації
ШНМ – штучна нейронна мережа

ВСТУП

Інтенсивна інформатизація всіх сфер життєдіяльності суспільства нині є одним з визначальних глобальних чинників подальшого соціально-економічного, інтелектуального та духовного розвитку людства, а на рівні підприємства інформаційні ресурси розглядають як важливий самостійний елемент виробництва. Розвиток інформаційних технологій, з одного боку, суттєво полегшує процес прийняття 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 швидкого оброблення великих баз даних тощо), а з іншого – створює нові загрози та ризики для функціонування підприємства, рівень та інтенсивність виникнення яких зростає в геометричній прогресії.

Експерти прогнозують, що до 2023 року інтернетом користуватиметься 70 % людства. Така тенденція – вагомий крок на шляху до розвитку глобального інформаційного суспільства, та водночас сигнал про необхідність зміцнити кіберзахист мережевих користувачів на національному рівні. Разом з тим завдяки збільшенню використання комунікативних технологій вартість кіберзлочинності також зростатиме. Останніми роками спостерігається посилення інтенсивності нових кібератак на корпоративні інформаційні системи підприємства, а традиційні заходи кібербезпеки не можуть у повному обсязі запобігти чи стримати такі атаки через зростання швидкості та частоту їх проявів.

Яскравим прикладом таких загроз є масштабна хакерська атака 2017 року, від якої постраждали переважно саме українські підприємства та державні установи: протягом дня удару зазнали сотні компаній, банків та державних установ. За припущеннями тодішнього міністра фінансів України О. Данилюка, загальні збитки в масштабах країни

могли становити близько 0,5 % ВВП держави, тобто понад 14 млрд грн, хоча більшість фахівців навіть не беруться оцінювати масштаби збитків та можливі негативні наслідки таких атак. Таким чином, актуальності набуває проблематика захисту інформації й протидії кібератакам, що потребує розроблення нових рішень та підходів, які відповідають не тільки реаліям сьогодення, а й мають значний потенціал розвитку, враховуючи сучасні тенденції ІТ-галузі в цілому.

Зазначене вище підкреслює й такий вже загальновизнаний факт, що інформаційний простір стає місцем боротьби за вплив і ресурси. Особливого загострення ця проблема набуває під час війни. Так, за даними Державної служби спеціального зв'язку та захисту інформації, лише за один місяць війни було здійснено майже втричі більше хакерських атак різного виду, ніж за аналогічний період минулого року. Найпопулярнішими видами атак залишаються фішингові розсилання, розповсюдження шкідливого програмного забезпечення. Як зазначає голова Держспецзв'язку Юрій Щиголь, атакують передусім державні установи, фінансовий та оборонний сектори, операторів зв'язку, місцеві органи влади, логістичні компанії, медіа. І ця тенденція, на жаль, зростає.

Так, за даними Євростату, у 2019 році 93 % підприємств ЄС з чисельністю персоналу більше 10 осіб запроваджували в систему стратегічних цільових показників щонайменше один вимірник для контролю інформаційної безпеки.

За даними державної служби статистики України, у 2021 році 86,6 % підприємств України мали доступ до мережі Інтернет. Проте, на жаль, статистичних спостережень щодо запровадження підходів із забезпечення інформаційної безпеки підприємствами України на сьогодні немає. Водно-

час стан інформаційної безпеки України опосередковано демонструє її місце у глобальному та національному індексах кібербезпеки. Наприклад, у 2018 році Україна посіла 54 місце серед 180 країн у глобальному рейтингу кібербезпеки, піднявшись 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 водночас – про наявний потенціал та необхідність запровадження заходів з посилення інформаційної безпеки.

Україна посідає четверте місце у світі за кількістю сертифікованих ІТ-спеціалістів, входить до 30 провідних локацій для передання замовлень на розроблення ПЗ. Це свідчить про наявність величезного потенціалу зростання як для ІТ-галузі, так і для формування систем кіберзахисту національної економіки. Команда реагування на комп'ютерні надзвичайні події України CERT-UA постійно робить кроки для взаємодії з Cisco Talos Intelligence Group та іншими державами – членами CERT з питань подолання наслідків кібератак на критично важливу інформаційну інфраструктуру і виявлення причин та обставин таких інцидентів. CERT-UA також допомагає усунути загрози безпеці приватного сектора України та іноземних партнерів. Відповідно до чинного вітчизняного законодавства CERT-UA та Центр реагування на кіберзлочини координують заходи з оперативного реагування на кібератаки, а також контролюють впровадження контрзаходів, що передбачають мінімізацію вразливості систем зв'язку.

Україна також бере участь у роботі Агентства ЄС з кібербезпеки, Європейського центру з досліджень і компетенції в сфері кібербезпеки та у навчаннях з реалізації Спільної оперативної схеми реагування ЄС і держав – членів на кібератаки.

Зазначені процеси та тенденції обумовили формування концепції інформаційної безпеки та виокремлення окремого 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 – з іншого.

Так, і Європейський Союз, і уряди більшості країн – членів ЄС мають давній та великий досвід законодавчого і проєктного супроводу розвитку інформаційної сфери суспільства. Умовною точкою відліку вважають появу у 1994 році документа-рекомендації для Європейської Ради «Європа і глобальне інформаційне суспільство» (*Recommendations to the European Council «Europe and the global information society»*), підготовленого групою експертів під головуванням Мартіна Бангеманна і відомого нині як «доповідь Бангеманна». Після цього були ініціативи «eEurope» (2000 р.), «eEurope 2002», «eEurope 2005», «i2010: Інформаційне суспільство та медіа для подальшого зростання і нових робочих місць», «Цифровий порядок денний для Європи» (*Digital agenda for Europe*) у межах Стратегії «Європа 2020» і зараз – «Цифровий компас ЄС до 2030» у межах Проєкту стратегії сталого розвитку «Європа–2030».

Питання розвитку інформаційного суспільства та забезпечення інформаційної безпеки в Україні регламентуються низкою нормативно-правових актів, а саме: Конституцією України, Законом України «Про Концепцію Національної програми інформатизації», Воєнною доктриною, Законом «Про інформацію», Законом «Про телекомунікації», Стратегією кібербезпеки України та ін. На сьогодні обґрунтовано Проєкт Закону України «Про цифровий порядок денний України» в межах Проєкту стратегії «Україна–2030».

Питання захисту інформації, формування системи інформаційної безпеки досліджується у низці наукових праць закордонних та вітчизняних фахівців. Аналіз значного масиву публікацій дав змогу нам виокремити три принципові підходи до вивчення систем захисту інформації: 1) у складі вивчення теоретико-методологічних та практичних способів формування економічної безпеки, де інформаційна безпека розглядається як її важливий елемент; 2) як самостійний об'єкт дослідження з акцентом на управлінські, організаційні, правові аспектах формування системи інформаційної безпеки; 3) як самостійний об'єкт дослідження з переважним акцентом на технічні засоби забезпечення інформаційної безпеки.

Так, науковці G. Menahem, V. Cherilova, B. Carayon, Ю. М. Харазішвілі, Е. В. Дронь, В. М. Геєць, М. О. Кизим, О. І. Черняк, З. С. Варналій, О. В. Панасюк, Я. А. Жаліло, В. В. Кузьменко, О. В. Арєф'єва, О. М. Бондаренко, В. А. Сухецький, Г. В. Козаченко, В. П. Пономарьов, О. М. Ляшенко, В. Л. Ортинський, І. С. Керницький, С.М. Шкарлет та ін. досліджували методологічні засади формування системи економічної безпеки економічних систем різного рівня (держави, регіону, підприємства), виокремлюючи її основні елементи, окреслювали методологію оцінювання, принципи формування систем забезпечення та напрями їх зміцнення. У зазначених працях інформаційна безпека розглядається як компонент більш складної системи, управління якою здійснюється в контексті та на загальних засадах керування економічною безпекою.

У дослідженнях N. Moinet, В. В. Андріанова, С. Л. Зефірова, В. Б. Голованова, А. А. Анісімова, О. В. Герасименка, А. В. Козак, М. І. Глухова, О. О. Кузнецова, С. П. Євсеєва, П. Д. Біленчука, З. Б. Живка, О. О. Косиці, В. С. Панченка,

Л. Г. Чистоклєтова, В. Ю. Світличної, Т. В. Полозової, М. Ю.Журавля, О. В. Стороженка, А. О. Чередниченка, Л. В. Шмалія, С. П. Міщенка, К. П. Боримської увагу приділено питанням регулювання, правового забезпечення інформаційної безпеки, формування організаційного механізму системи захисту інформації на підприємстві.

Технічним аспектам захисту інформації, зокрема вдосконаленню графів атак для моніторингу кібербезпеки, оперуванню похибками, обробленню циклів, відображенню інцидентів і автоматичному вибору захисних заходів присвячено роботи таких 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 займалися та займаються 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 іноземних вчених зосереджені на вираженні використання мережевого трафіку для створення моделей прогнозування. Подібні дослідження представлені в роботах таких вчених, як E. Pontes, A. E. Guelfi, S. T. Kofuji, A. A. Silva та ін. Інші науковці, як-от E. Gandotra, D. Bansal, S. Sofat, P. Chakraborty, P. Khadivi, B. Lewis, A. Mahendiran, J. Chen, P. Butler, E. O. Nsoesie, S. R. Mekaru, J. S. Brownstein,

які здійснюють кіберпрогнозування за допомогою статистичного та алгоритмічного моделювання.

Незважаючи на досить потужний пласт досліджень з проблематики інформаційної безпеки, на сьогодні немає комплексних міждисциплінарних розвідок, які б окреслювали методологію та практичний інструментарій формування ефективних систем захисту корпоративної інформації, котрі 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 в умовах 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. Тому саме обґрунтуванню теоретико-методологічних засад формування ефективних (з т. зв. досягнення цілей захисту та цільових показників економічної ефективності) систем інформаційної безпеки присвячено це дослідження. Зокрема, у монографії окреслено авторський погляд на комплексне наукове та практичне вирішення проблеми забезпечення економічної ефективності захисту корпоративної інформації.

Монографія призначена для науковців, студентів, фахівців-практиків, які займаються проблематикою корпоративної інформаційної безпеки.

Розділ 1

ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ СИСТЕМ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ: ТРАНСФОРМАЦІЯ ПОГЛЯДІВ

1.1. Корпоративний інформаційний простір: еволюція та структура

Розвиток постіндустріального суспільства загалом та економічних систем різного рівня зокрема значною мірою визначається станом, ефективністю оброблення та використання інформації. Не випадково синонімом постіндустріальної епохи є вислів «інформаційне суспільство». Свідченням важливої ролі інформації в суспільному розвитку є суттєвий дослідницький доробок, присвячений вивченню її сутності, особливостям використання тощо. Так, Д. Аткінсон зазначає, що інформація є однією з найскладніших, повністю не досліджених таємничих проблем сучасної науки [1]. У роботах Е. Тоффлера [2], Є. Дюннінга [3], К. Охмає [4], J. Nye [5] та ін. [6–8] досліджуються закономірності розвитку інформаційного суспільства, роль інформації у різних галузях суспільства тощо.

У розвідках В. В. Домарьова [9], С. В. Мельниченко [10], М. Г. Чумаченка [11], М. П. Денисенка, І. В. Колос [12], А. Є. Батюка, З. П. Двуліт [13], В. Іванової [14] проаналізовано теоретико-методологічні основи та прикладні аспекти створення й функціонування інформаційних систем на підприємствах, їх роль у забезпеченні економічних процесів.

Посилення ролі інформації у функціонуванні суспільства та економічних системах різного рівня, ускладнення структури та обсягу інформаційних потоків сприяють появі нової термінології. Так, усе частіше в науковому обігу зустрічаються поняття інформаційного простору, інформаційного середовища [15, 16].

Інформаційний простір є невід'ємним і постійним атрибутом людського буття, який, власне, існує завдяки самій людині. Вивченню його феномена та розвитку завжди приділяли особливу увагу філософи, соціологи, культурологи, а згодом і економісти в контексті дослідження ресурсного потенціалу окремих економічних систем. З часом та розвитком інформаційного суспільства увага науковців до функціонування та трансформації інформаційного простору лише зростає з огляду на посилення ролі інформації, як у житті окремого індивіда, так і у функціонуванні економічних систем різного рівня. Однак попри потужний пласт наукових досліджень у різних галузях науки на сьогодні не існує однозначного трактування поняття «інформаційний простір», підходів до його структуризації та методів регламентації й керування ним.

Так, Марина Яковенко на основі дослідження та узагальнення філософських тлумачень понять «простір» та «інформація» визначає інформаційний простір як форму освоєння реального світу, що вміщує й надає нам певну картину дійсності [17].

У найзагальнішому вигляді під інформаційним простором зазвичай розуміється сукупність результатів семантичної діяльності людства [18].

Із наведених визначень очевидними є важливі сутнісні ознаки інформаційного простору: *по-перше*, його визначальним генератором є людина, тобто інформаційний простір не може без неї існувати; *по-друге*, інформаційний простір є одночасно результатом та способом пізнання світу.

Gregory Newby розглядає інформаційний простір як сукупність понять та відносин між ними, які організовано в інформаційну систему, що описує діапазон можливих значень або смислів, які об'єкт може приймати за даними правилами та обставинами [19].

Таким чином, автор виокремлює таку важливу сутнісну характеристику інформаційного простору, як організованість у систему; обумовленість правилами та нормами.

У межах авторської «реляційної теорії інформаційного простору» М. М. Слюсаревський розглядає інформаційний простір як стан (і водночас результат) перманентної взаємодії процесів виробництва та споживання інформації, тобто інформаційний простір він простежує як простір розгортання інформаційних процесів. Існування інформації, на думку автора концепції, вважається можливим, коли вона кимось сприймається, тобто обов'язковою передумовою інформаційних процесів є наявність комунікативної системи «джерело – одержувач інформації», а параметри інформаційного простору вважаються обумовленими темпорально-психологічними характеристиками перебігу інформаційних процесів і соціально-психологічними характеристиками споживачів інформації. Відповідно, пропонується визначати цю категорію не стільки за обсягами вироблення інформаційної продукції чи площиною поширення інформації, скільки за обсягами та інтенсивністю її споживання. Як наслідок наведеного, на думку дослідника концепції, категорія інформаційного простору наповнюється власним теоретико-комунікативним та соціально-психологічним змістом, позбувається географічних та інших нашарувань та починає виконувати самостійні гносеологічні функції. Центром інформаційного простору є суб'єкт, який у ході своєї діяльності створює, накопичує, зберігає та передає інформацію. Таким суб'єктом може бути як особистість, так і соціальна група, організація, підприємство або навіть державний орган, тобто будь-які користувачі інформаційних технологій [20].

Отже, на основі зазначеного вище можна виокремити таку важливу сутнісну ознаку інформаційного простору, як безперервність процесу виробництва та споживання інформації, іншими словами – наявність постійної комунікації між суб'єктами.

До окреслених вище сутнісних характеристик інформаційного простору нами пропонується додати ще таку характеристику: «інформаційний простір є чинником розвитку системи та об'єктом управління», адже стан інформаційного простору, характер його організації створюють передумови

для пошуку нових можливостей та розвитку системи, прийняття управлінських та інших рішень, тобто система трансформується під впливом інформаційного простору. Інформаційний простір є важливим об'єктом управління, адже його формування та функціонування має сприяти економії ресурсів, підвищенню ефективності функціонування системи, її виживанню та розвитку.

Отже, інформаційний простір можна охарактеризувати таким чином (рис. 1.1).

Рис. 1.1. Сутнісні характеристики інформаційного простору

Джерело: узагальнено та доповнено за [17, 19, 20]

Таким чином, на основі узагальнення та розвитку сучасних підходів можна сформулювати зміст поняття інформаційного простору як **«сукупність інформації та інформаційних процесів, яка є станом, засобом та результатом функціонування системи, чинником її розвитку та формою представлення»**.

Для уточнення поняття «корпоративний інформаційний простір» потребує з'ясування термін «корпорація».

В українському правовому полі цей термін трактується неоднозначно. Так, з одного боку Господарський кодекс

України до корпоративних підприємств зараховує ті, що утворюються, як правило, двома або більше засновниками за їх спільним рішенням (договором), діють на основі об'єднання майна та/або підприємницької чи трудової діяльності засновників (учасників), їх спільного управління справами на основі корпоративних прав, у тому числі через органи, що ними створюються, участі засновників (учасників) у розподілі доходів та ризиків підприємства [19].

З іншого боку, стаття 120 Господарського кодексу України визначає корпорацію як договірне об'єднання, створене на основі поєднання виробничих, наукових і комерційних інтересів підприємств, що об'єдналися, з делегуванням ними окремих повноважень централізованого регулювання діяльності кожного з учасників органам управління корпорації [19, ст. 120].

За визначенням Конференції ООН з торгівлі та розвитку (ЮНКТАД), транснаціональні корпорації (ТНК) – це «підприємства, що складаються з материнського підприємства та його закордонних філіалів», при цьому ТНК можуть як набувати статусу корпорації, так і не мати цього статусу [22].

Таким чином, є очевидним, що трактування корпорації в міжнародному праві подібне до терміна «корпоративне підприємство» в українському правовому полі. Такого підходу дотримуються і переважна більшість авторів, які займаються дослідженнями в сфері корпоративного управління. Наприклад, на думку Р. Райх, корпорація – це договірне господарське об'єднання, створене на основі загальних економічних інтересів виробничих працівників і акціонерів для одержання максимального прибутку від виробничої діяльності та вкладених інвестицій [23]. Аналогічне визначення цього терміна дають і українські науковці О. В. Арєф'єва та Н. В. Васюткіна [24]. Використовуючи поняття «корпоративний», надалі ми будемо дотримуватись саме такого змістовного навантаження терміна «корпорація», розглядаючи її як правову форму бізнесу, що відрізняється і відокремлена від конкретних осіб, які ними володіють.

Отже, розуміння дефініцій «інформаційний простір» та «корпорація» дає змогу сформулювати поняття **корпоративного інформаційного простору як організовану систему інформації та інформаційних процесів корпорації, яка є станом та результатом її функціонування, способом її розвитку та представлення.**

Корпоративний інформаційний простір зазнав суттєвої трансформації за останні 100 років, темпи та інтенсивність якої особливо відчутні у XXI сторіччі.

Так, слушно зазначає С. О. Довгий: «Людина завжди існувала в інформаційному просторі, що її оточував. Розширенню інформаційного простору сприяли поява друкарства і пошти, винахід телеграфу і телефону, відкриття радіо і телебачення. Значний і вирішальний внесок у глобалізацію інформаційного простору внесло масове застосування у всіх сферах діяльності людини сучасних інформаційно-комунікаційних технологій, які істотно змінюють не тільки спосіб виробництва товарів і послуг, а й організацію і форми проведення дозвілля, реалізації людиною своїх громадянських прав, методи і форми виховання та освіти. Вони впливають на соціальну структуру суспільства, економіку, політику, розвиток суспільних інститутів» [25].

Імплементуючи зазначений вислів до розвитку корпоративного інформаційного простору, на нашу думку, можна визначити наступні етапи його еволюції (табл. 1.1).

Таблиця 1.1

Етапи еволюції корпоративного інформаційного простору

Назва етапу	Період	Основні ознаки
«Паперовий» (до широкого використання в практиці ПЕОМ)	До середини 1970-х років	– локальність; – обмеженість; – низька інтенсивність поширення; – високі витрати часу на формування на оброблення інформації

Закінчення табл. 1.1

Назва етапу	Період	Основні ознаки
«Автоматизований» (після винаходу та широкого запровадження в практику ПЕОМ)	З середини 1970-х до початку 1990-х рр.	– локальність; – обмеженість; – низька інтенсивність поширення; – скорочення витрат часу на формування на оброблення інформації
«Мережевий» (після початку широкого використання інтернету в комерційних цілях)	З початку 1990-х років і до цього часу	– глобальність; – відсутність фізичних меж зберігання інформації; – висока інтенсивність та швидкість поширення; – «надлишковість» та складність вибору релевантної інформації; – низькі витрати часу на формування, обмін та оброблення інформації; – зростання витрат на захист інформації; – посилений вплив інформаційного простору на трансформацію бізнес-моделі, організаційної структури тощо.

Джерело: складено автором

Так, за останні 50 років відбулася суттєва трансформація корпоративного інформаційного простору, а з особливою інтенсивністю цей процес відбувався в останні 30 років після широкого застосування інтернету. Якщо до цього корпоративний інформаційний простір мав локальний характер, потребував високих витрат на збирання та оброблення інформації, то вже з середини 90-х років XX сторіччя почав набувати глобального характеру; на сьогодні спостерігається високий рівень інтенсивності та швидкості поширення інформації: будь-яка інформація може бути поширена або знайдена «в один клік»; дуже часто інформація є «надлишковою», потребує відбору. Водночас суттєво знижуються витрати часу на оброблення та аналіз інформації, натомість на убезпечення інформаційного простору –

зростають. Важливою особливістю корпоративного інформаційного простору за сучасних умов є його значний вплив на трансформацію бізнес-моделі, організаційної структури підприємства, способу виробництва товарів та послуг. Таким чином, можна говорити про значне зростання ролі корпоративного інформаційного простору в розвитку підприємства.

На думку І. І. Новаківського, сучасні корпорації повинні ставити перед собою не завдання адаптації до сучасної соціально-економічної ситуації, а завдання формування адаптивної бізнес-оболонки з метою посилення конкурентоспроможності, стабільності розвитку та стійкості. Автор вважає, що першочерговим завданням корпорації є формування розвиненого корпоративного простору на основі неперервної розбудови корпоративної інформаційної інфраструктури й залучення до неї на умовах співпраці середніх та малих підприємств [26].

Розвиваючи підхід І. І. Новаківського, можна виокремити такі основні тенденції розвитку корпоративного інформаційного простору на сучасному етапі його еволюції (рис. 1.2).

Сучасному корпоративному інформаційному простору властива мережева структура з поєднанням вертикальних і горизонтальних каналів обміну інформації та взаємодії. Інформаційний обмін стає швидким і надлишковим, постійно виникає проблема у відборі релевантних даних для прийняття рішень. Мережевість та необхідність постійної адаптації до умов зовнішнього середовища призводить до домінування децентралізованих систем управління інформацією з високим ступенем автономії та взаємодії. Відбувається розмивання меж зберігання інформації. Якщо раніше вся інформація зберігалась фізично в межах підприємства, то зараз міститься в різних місцях і виходить за межі «офісу» (у відокремлених сервісних центрах, на «хмарних» сервісах тощо). Таким чином, під впливом розвитку корпоративного інформаційного простору здійснюється трансформація структури самої корпорації: її межі розмиваються, формуються сучасні мережеві організаційні структури, котрим притаманний більш демократичний, гнучкий та адаптивний характер.

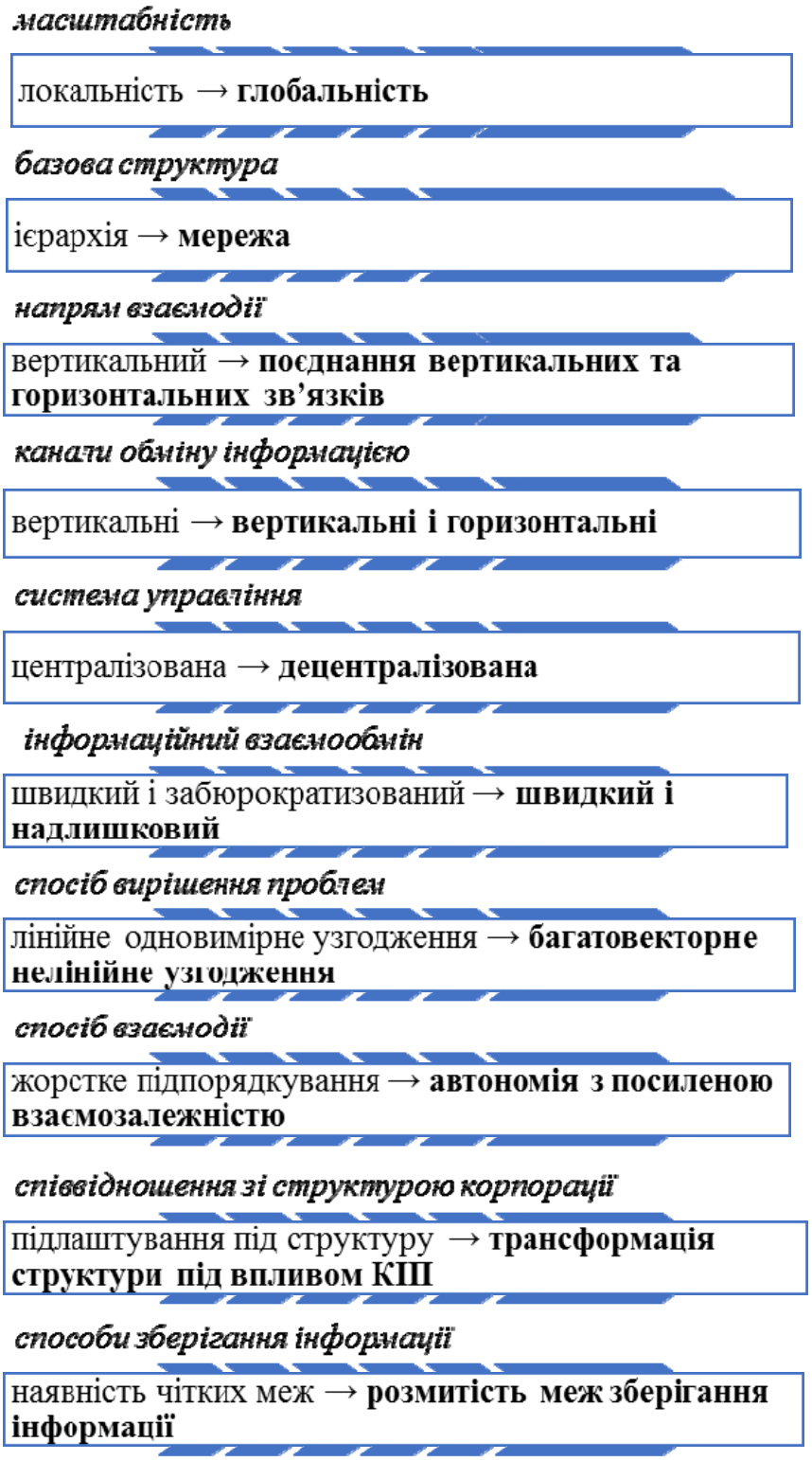


Рис. 1.2. Тенденції розвитку корпоративного інформаційного простору на сучасному етапі його еволюції

Джерело: розвинено автором на основі [26]

Корпоративний інформаційний простір має складну структуру, яка також зазнала трансформації в процесі його еволюції. Проте серед дослідників відсутнє єдине бачення структури інформаційного простору загалом та корпоративного інформаційного простору зокрема.

Так, ще у середині 90-х років XX ст. окремі вчені до складу інформаційного простору включали такі компоненти.

1. Інформаційна інфраструктура – середовище, що забезпечує можливість збирання, зберігання, передавання, автоматизованого оброблення та поширення інформації у суспільстві. Інформаційна інфраструктура суспільства створюється сукупністю інформаційно-телекомунікаційних систем (ІТС) та мереж зв'язку, індустрії засобів інформатизації, телекомунікації та зв'язку; систем формування та забезпечення зберігання інформаційних ресурсів; систем забезпечення доступу до ІТС, систем зв'язку та інформаційних ресурсів; індустрії інформаційних послуг та інформаційного ринку; системи підготовки та перепідготовки кадрів, проведення наукових досліджень.

2. Інформаційні ресурси на машинних носіях, а також розподілені по web-сайтах у мережі Internet. Інформаційні ресурси можуть бути державними та недержавними й перебувати у власності громадян, органів державної влади, органів місцевого самоврядування, підприємств, організацій, установ та громадських об'єднань. Є такі особливості, що відрізняють інформаційні ресурси від інших видів ресурсів: вони піддаються не фізичному, а моральному зношуванню; вони нематеріальні та не зводяться до фізичного носія, у якому втілені; їх використання дає змогу різко скоротити споживання інших видів ресурсів, що у кінцевому підсумку призводить до значної економії коштів.

3. Засоби та методи прикладної математики – це алгоритми та програмні засоби, що забезпечують функціонування апаратних платформ (систем).

4. Організаційні заходи, що забезпечують функціонування компонентів інформаційного простору.

5. Правові методи (норми), тобто інформаційне законодавство, міжнародні угоди та інші національні й міжнаціональні правові акти.

6. Ринок інформаційних технологій, засобів зв'язку, інформатизації та телекомунікації, інформаційних продуктів та послуг [27].

Це одне з найпоширеніших трактувань компонентного складу інформаційного простору. Якщо застосувати зазначений підхід до корпоративного інформаційного простору, то логічним буде висновок про відсутність у його складі ринку інформаційних технологій. Однак, на нашу думку, дискусійним є віднесення до складу інформаційного простору системи організаційних заходів, оскільки вони є результатом впливу управлінської дії на його стан та наслідки функціонування.

Натомість, на думку І. Кармелюка, інформаційний простір складається з таких головних компонентів, як:

– інформаційні ресурси, що містять дані, відомості та знання, зафіксовані на відповідних носіях інформації;

– організаційні структури, що забезпечують функціонування та розвиток єдиного інформаційного простору, зокрема, збирання, оброблення, зберігання, розповсюдження, пошук і передавання інформації;

– засоби інформаційної взаємодії громадян та організацій, що забезпечують їм доступ до інформаційних ресурсів на основі відповідних технологій, котрі включають програмно-технічні засоби й організаційно-нормативні документи [28].

Однак, на нашу думку, виділення організаційних структур, що забезпечують функціонування та розвиток інформаційного простору в контексті дослідження корпоративного інформаційного простору, є дискусійним з огляду на наявність чіткої усталеної диференціації поняття організаційної структури підприємства, до складу якої варто зараховувати також ті підрозділи, які є елементом забезпечення функціонування корпоративного інформаційного простору.

Дослідниця О. М. Кузьміна розглядає компонентну структуру корпоративного інформаційного простору з двох позицій: змістовної та організаційно-технічної. Так, із змістовної точки зору інформаційний простір включає [29]:

– інформаційне поле – сукупність усієї зосередженої в просторі інформації, безвідносно до її форми і стану, що перебуває у відриві як від об'єкта відображення, так і від суб'єкта сприйняття. Рух інформації в інформаційному полі здійснюється за допомогою фізичного зв'язку між одержувачем і джерелом інформації, що матеріалізується в інформаційному потоці;

– інформаційний потік – сукупність інформації, що переміщується в інформаційному просторі через канали комунікації. Інформаційні потоки можуть протікати як усередині окремих інфосфер, так і між ними, залежно від наявності каналів комунікації. Організаційний аспект структури інформаційного простору становлять множини баз даних і банків даних, сховищ даних, технологій їх ведення, використання, інформаційних систем, мереж, застосувань, організаційних структур, що функціонують на основі певних принципів і за встановленими правилами, що забезпечують інформаційну взаємодію об'єктів.

В організаційно-технічному аспекті структуру інформаційного простору становить:

– сукупність баз і банків даних, технологій їх супроводу, використання;

– сукупність інформаційно-телекомунікаційних систем, мереж, додатків та організаційних структур, що функціонують на основі певних принципів і за встановленими правилами, а це забезпечує інформаційну взаємодію користувачів та задоволення їхніх інформаційних потреб.

Слушною, на нашу думку, є пропозиція О. М. Кузьміної щодо виділення окремим компонентом побудови інформаційного простору віртуальної реальності. Так, дослідниця зазначає, що, «крім перерахованих вище, в інформаційному просторі можна виділити особливий компонент, який має назву віртуальна реальність (ВР), сформована у вигляді віртуальних аналогів реальних об'єктів і процесів (як-от чати і форуми, електронний банкінг, система електронної торгівлі, геоінформаційні системи, системи електронного документообігу,

системи автоматизованого проєктування і моделювання фізичних процесів тощо), які базуються на відповідних програмно-апаратних платформах та інформаційно-телекомунікаційних мережах і системах зв'язку й сприймаються людиною (користувачем) як модель-замінник дійсної реальності. Під сучасною ВР, як правило, розуміють віртуальну модель дійсності, побудовану на інформаційних технологіях, які дають можливість:

– формувати в кіберпросторі цілком адекватну дійсній реальність (або довільно, цілеспрямовано і зловмисно змінену) ВР як певну модель світу (об'єктів, процесів) у будь-якій зручній для сприйняття людською свідомістю формі;

– прив'язувати до елементів цієї моделі будь-які необхідні дані й оперувати ними;

– моделювати результати впливу (управління) до їх реалізації в реальному світі;

– впливати на об'єктивну (дійсну) реальність через її сполучення з ВР шляхом передачі інформаційних повідомлень (керуючих впливів)» [29].

Справді, віртуальна реальність у сучасному інформаційному суспільстві відіграє важливу роль. За її допомогою компанія може реалізувати політику репрезентації своєї діяльності в суспільстві. Тому інформація на сайтах, спеціальних каналах комунікації може представлятись у певному вигляді, який відповідає інтересам компанії щодо формування іміджу, реалізації політик в інших різних сферах діяльності, «акцентуючи увагу» на певних здобутках і позитивних рисах. Проте авторка не конкретизує місце цього компоненту інформаційного простору серед інших його складових.

Якщо з двоаспектним тлумаченням інформаційного простору О. М. Кузьміною в цілому можна погодитись, то виділення нею окремим компонентом інформаційного простору інформаційної системи є дещо дискусійним. Так, дослідниця зазначає, що «основним компонентом структури інформаційного простору є інформаційна система, яка являє собою:

– організаційно впорядковану сукупність фахівців, інформаційних ресурсів та інформаційних технологій, що реалізують інформаційні процеси – отримання вхідних даних;

– оброблення цих даних та/або зміну власного внутрішнього стану (внутрішніх зв'язків / відношень), видачу результату або зміну свого зовнішнього стану (зовнішніх зв'язків / відношень)» [29].

Але, по-перше, зміст інформаційної системи в трактуванні О. М. Кузьміної дублює окремі компоненти інформаційного простору у змістовому та організаційно-технічному аспектах; по-друге, не зрозуміло, як автор співвідносить між собою окремі компоненти інформаційного простору в його загальній структурі.

В окремих дослідженнях зустрічається також вузьке трактування компонентної структури корпоративного інформаційного простору. Так, Л. Р. Матвєєва корпоративний інформаційний простір розуміє як сукупність інформаційних систем і технологій, зокрема таких, як ERP, CRM, BPM та інших подібних систем і відповідних модулів [30]. Такий звужений підхід визначає єдиний інформаційний простір підприємства як інформаційно-технологічну інфраструктуру, у межах якої забезпечується прозорість і легкість доступу до будь-якої інформації, що циркулює в інформаційній системі на основі реалізації єдиних методів зберігання, доступу, оброблення інформації. До неї автори відносять АСУ, АСУ ТП та САПР.

На нашу думку, вузький підхід до трактування структури корпоративного інформаційного простору не надає повного уявлення його змісту і віддзеркалює лише його техніко-технологічну складову.

Важливо не лише визначити складові частини корпоративного інформаційного простору, а й також ідентифікувати його структуру, чого не роблять більшість дослідників, адже саме структура відображає сукупність стійких закономірних зв'язків між елементами системи.

Так, у дослідженні Н. Ю. Науменко пропонується авторська концепт-модель структури інформаційного простору на основі діаграми Дж. Венна, де центральним компонентом є користувач, який використовує інформаційні ресурси. Також компонентами моделі інформаційного простору автор пропонує виділяти інформаційні засоби взаємодії, системи оброблення інформації, інформаційну інфраструктуру та поля предметної області [31].

Узагальнюючи та розвиваючи наявні підходи, пропонуємо виокремлювати чотири принципові компоненти корпоративного інформаційного простору: суб'єкти, семантичну складову (інформаційний контент), інформаційну інфраструктуру, регламенти та норми.

Центральним та системоутворюючим складником корпоративного інформаційного простору є його суб'єкти, серед яких варто виокремити первинний та вторинний рівні. Так, 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 умовно поділяємо на:

– інформаційні поля;
– інформаційний процес;
– віртуальну реальність;
– інформаційну культуру.

Так, погоджуючись з думкою О. М. Кузьміної, інформаційне поле можемо трактувати як сукупність усієї зосередженої у корпоративному просторі інформації, безвідносно до її форми і стану, що перебуває у відриві як від об'єкта відображення, так і від суб'єкта сприйняття.

Корпоративне інформаційне поле складається з великої кількості різнорідної інформації, яку в найбільш узагальненому вигляді можна класифікувати за певними ознаками (табл. 1.2).

Таблиця 1.2

Класифікація інформації корпоративного інформаційного поля

Класифікаційна ознака	Види інформації
За предметною сферою	– фінансово-економічна; – операційна; – кадрова; – маркетингова; – про логістичну діяльність; – юридична
За функціями управління	– фактична (первинна); – аналітична; – організаційна; – планова; – контрольна
За формою зберігання	– усна; – на паперових носіях; – електронна (на електронних носіях); – образно-віртуальна
За режимом доступу та захисту	– загальнодоступна для внутрішніх користувачів; – публічна (для оприлюднення у зовнішньому середовищі); – з обмеженим режимом доступу
За місцем формування	– внутрішня; – зовнішня
За регламентованістю	– неформальна; – формальна (офіційна)
За відповідністю окремому рішенню, проєкту тощо	– релевантна; – нерелевантна

Джерело: складено автором

Інформаційний процес ми визначаємо як процес комунікації, що супроводжується рухом інформації за різними

комунікаційними каналами. Тобто інформаційний процес складається з двох органічно взаємопов'язаних компонент – комунікаційного процесу та інформаційних потоків. Під комунікаційним процесом ми розуміємо процес спілкування між суб'єктами корпоративного інформаційного поля та зовнішнього інформаційного поля за різними каналами комунікації. Комунікаційний процес супроводжується односторонн ім або зустрічним рухом інформації: вербально, письмово, за допомогою різноманітних техніко-технологічних засобів.

Таким чином, інформаційний потік можна визначити як сукупність розподіленої в часі та за обсягом інформації, що рухається в перебігу комунікації за різними каналами.

Окремим компонентом семантичної складової є віртуальна реальність, яка відображає або певною мірою модифікує стан дійсної реальності.

Також важливим компонентом семантичної складової вважаємо корпоративну інформаційну культуру, яка є складним утворенням та віддзеркалює корпоративну філософію комунікацій і містить формальну та неформальну складові.

Семантична складова безпосередньо становить інформаційний ресурс підприємства, по суті є основною цінністю корпоративного інформаційного поля, яку використовують у процесі прийняття рішень. Так, інформація в інтерпретації Н. Лумана є не структурою, а подією, яка змінює стан системи. Коли інформація виявляється, вона не зникає безслідно, а залишає структурний ефект, змінюючи стан системи. Реагуючи на цю зміну, трансформується вся система. Н. Луман підкреслює, що інформація завжди функціонує як нове, що створює сенс [32]. Тобто саме семантична складова є важливим елементом ресурсного потенціалу підприємства, який впливає на розвиток підприємства й у взаємодії з іншими ресурсами детермінує ефективність функціонування економічної системи.

Важливим компонентом корпоративного інформаційного простору є інформаційна інфраструктура, яка складається з технічних засобів збирання, оброблення, зберігання,

передавання, поширення та технологічних засобів (програмних продуктів). Якість та інноваційність інформаційної інфраструктури суттєво впливає на ефективність інформаційного процесу в цілому та на ефективність функціонування підприємства зокрема.

Регламенти та норми як компонент корпоративного інформаційного простору визначають параметри семантичної компоненти: інформаційних полів, інформаційного процесу, корпоративної інформаційної культури, оскільки обумовлює зміст, формат, терміни формування, передавання та оброблення інформації.

Таким чином, корпоративне інформаційне поле – це складне багатокомпонентне утворення, окремі складники якого перебувають у взаємообумовленому зв’язку.

Список бібліографічних посилань

1. Atkinson D. Thinking the art of management : stepping into 'Heidegger's Shoes'. Basingstoke: Palgrave Macmillan, 2008. 280 p.

2. Toffler A. Powershift: Knowledge, Wealth, and Power at the Edge of the 21st Century. Bantam; Reissue edition. Nov.1, 1991. 640 p.

3. Dunning J. Regions, Globalization and the Knowledge Economy // Regions, Globalization, and the Knowledge-Based Economy. Oxford, 2000. P. 8–10.

4. Ohmae K. The Invisible Continent // Four Strategic Imperatives of the New Economy. N. Y., 2000. P. 227–231. URL : http://dialogs.org.ua/project_ua

5. Nye J. Soft Power. The Means to Success in World Politics. N. Y., 2004.

6. Building Knowledge Economies: Opportunities and Challenges for EU Accession Countries. N. Y., 2002.

7. Ibidem. Communication: From Information Society to Knowledge Societies // UNESCO. The New Courier. 2003. № 3, October.

8. Sustainable Development and the New Economy // OECD Forum – 2001. Paris, 2001.

9. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. Київ : ООО «ТИД Diasoff», 2002. 686 с.

10. Мельниченко С. В. Інформаційні технології в туризмі: теорія, методологія, практика : монографія. Київ : Київ. нац. торг.-екон. ун-т, 2007. 493 с.

11. Чумаченко М. Г. Економічний аналіз : навч. посіб. Київ : КНЕУ, 2001. 540 с.

12. Денисенко М. П., Колос І. В. Інформаційне забезпечення ефективного управління підприємством. *Економіка та держава*. 2006. № 7. С. 19–24.

13. Інформаційні системи в менеджменті / А. Є. Батюк, З. П. Двуліт, К. М. Обельовська та ін. Львів : Інтелект-Захід, 2004. 520 с.

14. Іванова В. Щодо формування системи інформаційного забезпечення розвитку економіки України. *Економіст*. 2008. № 4. С. 61–73.

15. Коваленко О. О. Створення інформаційного мережевого простору організації. Методологія та моделювання : монографія. Вінниця : ВЦ ВФЕУ, 2009. 232 с.

16. Бобров С. В., Левшенко О. С., Поривай О. В. Методи формування єдиного інформаційного середовища в установі // Збірник наукових праць Центру воєнно-стратегічних досліджень Нац. ун-ту оборони України імені Івана Черняховського. 2013. № 3 (49). С. 26–32.

17. Яковенко М. Інформаційний простір: філософські аспекти формування поняття. *Вісник Нац. ун-ту «Львівська політехніка». Філософські науки*. 2011. № 692. С. 22–27.

18. Інформаційний простір // Зв’язки з громадськістю в органах влади / М.М. Васильєва. 2014. URL : https://stud.com.ua/64427/zhurnalistika/informatsiyniy_prostir

19. Gregory Newby. MIRE: a multidimensional information retrieval engine for structured data and text. Proceedings.

International Conference on Information Technology: Coding and Computing. ISBN 0769515061. Doi : 10.1109/ itcc.2002.1000391

20. Слюсаревський М. М. Інформаційний простір : критика існуючих визначень і спроба побудови теорії. *Вісник ХДУ*. Серія «Психологія, політологія : Особистість і трансформаційні процеси у суспільстві». Харків. 1999. № 439. Ч. 4–5. С. 337–342.

21. Господарський кодекс України від 16 січня 2003 року № 436-IV. Дата оновлення: 27.05.2022. URL : https://zakon. rada.gov.ua/laws/show/436-15 (дата звернення: 10.06.2022).

22. World Investment Report 2007: Transnational Corporations, Extractive Industries and Development. – UNCTAD, United Nations. New York and Geneva, 2007.

23. Reich R. B. The Work of Nations: Preparing Ourselves for 21st Century Capitalism. NY, 1992. 331 p.

24. Ареф'єва О. В., Васюткіна Н. В. Корпоративне управління: еволюція, становлення, розвиток : монографія. Київ : Ліра-К, 2013. 180 с.

25. Довгий С. О. Інститут телекомунікацій і глобального інформаційного простору. URL : http://www.itel.nas.gov.ua (дата звернення: 10.06.2022).

26. Новаківський І. І. Засади формування інформаційного простору структурних бізнес-оболонок / Lviv Polytechnic National University Institutional Repository. URL : http://ena.lp. edu.ua (дата звернення: 10.06.2022).

27. Alberts D., Richard E. H. Information Warfare Workshop. Decision Support Working Group Report. 1996; Information Warfare, complex organisations and the power of disruption. University of Arisona, 1997. 222 p.

28. Кармелюк І. М. Розвиток інформаційного простору як запорука вдосконалення управління державою власним гуманітарним капіталом. *Теорія та практика державного управління*. 2009. Вип. 3. С. 294–299.

29. Кузьміна О. М. Актуалізація формування єдиного інформаційного середовища організації. Східна Європа: економіка, бізнес та управління. № 5 (16). 2018. С. 289–292.

30. Матвєєва Л. Р. Управління інвестиційними проектами в умовах ризику та невизначеності. URL : https://stud.com. ua/150142/strahova_sprava/upravlinnya_investitsiynimi_proektami_v_umovah_riziku_ta_neviznachenosti (дата звернення: 10.06.2022).

31. Науменко Н. Ю. Особливості конкретизації методології формування інформаційного простору регіональних соціально-економічних систем. *Modern Economic*. № 14. 2019. С. 186–192.

32. Скороварова Є. Концепція комунікації Н. Лумана // Ученые записки Таврического национального ун-та им. В. И. Вернадского. URL : http://snphilcultpolsoc.crimea.edu/arhiv/2013/uch_24_1_2_filosof/008skvor.pdf (дата звернення: 10.06.2022).

1.2. Інформаційні загрози як нова реальність бізнесу

В інформаційному суспільстві з ряду причин неможливо повністю уникнути різноманітних інформаційних загроз, серед яких найбільш суттєвими є ті, що пов'язані з комп'ютерними злочинами (кіберзлочинами). На сьогодні зростання таких загроз є елементом нової реальності для бізнесу та чинником впливу на корпоративний інформаційний простір.

Термін «кіберзлочин» є не тільки інтуїтивно зрозумілим, а й має законодавче визначення в Україні:

Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [1, ч. 1, п. 8].

Проте єдиної визнаної класифікації кіберзлочинів, яку можна було б використати в процесі дослідження, в Україні на сьогодні немає. Є декілька підходів, що використовуються різними правоохоронними органами в процесі укладання звітності про скоєні (виявлені, облікові) та розслідувані (супроводжувані) злочини.

Згідно з Єдиним звітом про кримінальні правопорушення, що укладається Офісом генерального прокурора України, де-факто кіберзлочинами визнано злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, до яких належать кримінальні правопорушення за такими статтями Кримінального кодексу України (далі – ККУ):

• 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

• 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут.

• 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації.

• 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

• 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється.

• 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку [2].

Дані звіту Офісу Генерального прокурора України є у відкритому доступі за період з 2013 року [3]. Кіберзлочини, що відображені у ньому, в цьому дослідженні далі називатимуться **основними кіберзлочинами.**

Необхідно зауважити, що відомості про основні кіберзлочини не дозволяють повною мірою оцінити всі кримінальні правопорушення, що підпадають під визначення кіберзлочину, оскільки не враховують злочини відповідно до ККУ:

– у сфері обігу протиправного контенту і телекомунікацій – за статтями 176, 229, 301 (ч. 3, 4 та 5);

– у банківській сфері – за статтями 185, 200 та 231;

– окремі різновиди онлайн-шахрайств – за статтею 190 (ч. 3 та 4).

Ці три зазначені різновиди злочинів у цьому дослідженні далі називатимуться **супутніми кіберзлочинами.** Щодо них вдалося отримати дані лише за період з 2016 по 2020 рік та фрагментарні дані за перший квартал і 8 місяців 2021 року на основі звітності Національної поліції України [4] та інформації, наданої РНБО України за офіційним запитом КНТЕУ [5].

З урахуванням усіх названих вище різновидів кіберзлочинів (основних та супутніх) для їхньої узагальненої класифікації у цьому дослідженні також використовується поділ на 4 групи (відповідно до методології РНБО України):

1) у сфері обігу протиправного контенту і телекомунікацій;

2) у банківській сфері;

3) окремі різновиди онлайн-шахрайств;

4) у сфері комп’ютерних систем.

Таким чином, склад кіберзлочинів, інформація про які відображається в звітності правоохоронних органів України, можливо проілюструвати за допомогою рис. 1.3.

Від кіберзлочинів необхідно відрізняти кіберінциденти, кіберподії та кібератаки (відповідно до законодавчої термінології), які не мають статусу злочинів. Зазначені різновиди подій некримінального характеру потребують окремого дослідження, оскільки є важливими для оперативного моніторингу стану корпоративного інформаційного простору та кібербезпеки в країні загалом.

З метою розширення інформаційної бази дослідження були надіслані офіційні запити від університету у відповідні державні органи (зокрема, в Департамент захисту інформації Адміністрації Держспецзв’язку, Національне агентство з ак-

редитації України та РНБО України) про надання необхідної додаткової інформації про кіберзлочини та інформаційну безпеку в Україні загалом.

	Основні кіберзлочини	**Супутні кіберзлочини**
Кіберзлочини у сфері обігу протиправного контенту і телекомунікацій		ст. 176, 229, 301 (ч. 3, 4 та 5)
Кіберзлочини у банківській сфері	ст. 362	ст. 185, 200, 231
Окремі різновиди онлайн-шахрайств		ст. 190 (ч. 3 та 4)
Кіберзлочини у сфері комп'ютерних систем	ст. 361, 361-1, 361-2, 363, 363-1	

Рис. 1.3. Склад кіберзлочинів (узагальнена класифікація, що використовується у цьому дослідженні, із зазначенням статей ККУ)

Джерело: складено автором на основі [3–5] та власних досліджень

Проте, як виявилось, значна частина цієї інформації має обмежений доступ, тобто має статус конфіденційної, службової або таємної відповідно до Закону України «Про інформацію» [6]) і не підлягає оприлюдненню. З цієї причини сформувати повну необхідну інформаційну базу за досить тривалий період не було змоги. Використання наявних фрагментарних даних хоч і негативно вплинуло на отримані результати, проте не унеможливило дослідження загалом.

Стан кіберзлочинності є комплексним поняттям, що узагальнює практику скоєння кіберзлочинів та результати протидії цим злочинам з боку правоохоронних органів. Його характеризують різноманітні кількісні та якісні показники, систематизація яких є предметом окремого дослідження. Серед показників стану кіберзлочинності ключове місце посідають

показники кількості кіберзлочниів за даними звітності правоохоронних органів. Розрізняють кількість зареєстрованих (виявлених) злочинів за певний період та інші показники кількості злочинів.

Кількість зареєстрованих основних кіберзлочинів в Україні за період з 2013 по 2020 рік, як свідчить рис. 1.4, збільшилася загалом майже у 5 разів на тлі зменшення сукупної кількості зареєстрованих кримінальних правопорушень за цей період більше, ніж на третину.

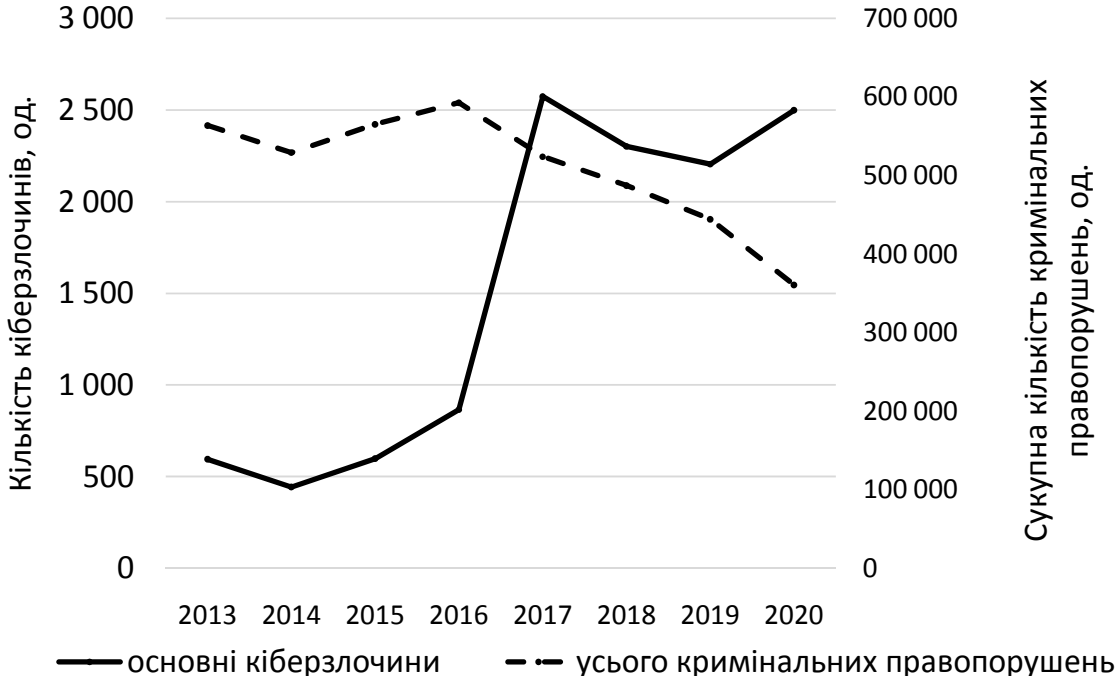


Рис. 1.4. Динаміка кількості зареєстрованих основних кіберзлочинів у порівнянні з сукупною кількістю зареєстрованих кримінальних правопорушень в Україні за 2013–2020 рр.

Джерело: складено автором на основі [3]

На перший погляд, виявлена динаміка кількості зареєстрованих основних кіберзлочинів є ознакою погіршення стану кіберзлочинності та кібербезпеки в країні загалом. Проте такий висновок не відображає якісних змін у роботі правоохоронних органів, що протидіють кіберзлочинності. Зокрема, стрімке

зростання кількості зареєстрованих основних кіберзлочинів у 2017 році можна частково пояснити позитивними змінами у виявленні таких злочинів кіберполіцією, що була створена 05.10.2015 як структурний підрозділ Національної поліції. Після невдалих спроб організувати ефективну роботу кіберполіції впродовж 2016 року, в межах проєкту «Розбудова спроможностей кіберполіції» у березні 2017 року міжнародні донори передали їй близько 130 позицій інформаційних та комунікаційних технологій, а 19 липня 2017 року представники координатора проєктів ОБСЄ в Україні передали підрозділам кіберполіції 194 одиниці спеціалізованої техніки. Також з 2017 року почали давати віддачу заходи щодо підвищення кваліфікації правоохоронців, які спеціалізуються на протидії кіберзлочинності.

Після стрибкоподібного збільшення у 2017 році та впродовж двох наступних років (2018 та 2019) кількість зареєстрованих основних кіберзлочинів зменшувалася і лише у 2020 році зросла на 13,3 % в умовах пандемії Covid-19. Таку динаміку, з огляду на здатність правоохоронних органів ефективно виявляти кіберзлочини, можна вважати задовільною.

Масштаби кіберзлочинності в Україні за показником частки основних кіберзлочинів у сукупній кількості зареєстрованих кримінальних правопорушень (див. табл. 1.3) є незначними: за підсумками 2020 року ця частка становила лише 0,69 %, хоча демонструвала щорічне зростання впродовж усього періоду дослідження (за винятком 2018 року).

Склад зареєстрованих основних кіберзлочинів, як свідчать дані табл. 1.3, упродовж 2013–2020 рр. зазнав помітних змін. Кількість кримінальних правопорушень за всіма статтями ККУ збільшилася, окрім тих, що підпадають під найбільш важливу статтю 361, котрі були суттєво нижчими у порівнянні з рештою статей та загальною кількістю, що призвело до структурних зрушень. Також зміни кількості окремих різновидів основних кіберзлочинів досить суттєво корелювали зі змінами загальної кількості цих злочинів (див. табл. 1.3), крім найменш вагомих статей 363 та 363-1, для яких коефіцієнт парної кореляції свідчить про недостатньо сильний статистичний взаємозв’язок. Окреме зауваження стосується волатильності (мінливості) кількості

зареєстрованих основних кіберзлочинів – вона як загалом, так і для окремих різновидів суттєво перевищує волатильність сукупної кількості зареєстрованих кримінальних правопорушень, про що свідчать значення коефіцієнтів варіації у табл. 1.3.

Таблиця 1.3

Склад зареєстрованих основних кіберзлочинів в Україні за 2013–2020 рр.

Рік / показник	Кількість зареєстрованих основних кіберзлочинів						УКП*	Частка,
	усього	у т. ч. за статтями ККУ						
		361	361-1	361-2	362	363 та		
2013	595	408	12	20	152	3	563 560	0,11
2014	443	344	10	11	73	5	529 139	0,08
2015	598	432	21	59	75	11	565 182	0,11
2016	865	494	15	28	311	17	592 604	0,15
2017	2 573	1 795	35	64	670	9	523 911	0,49
2018	2 301	1 023	134	52	1 070	22	487 133	0,47
2019	2 204	1 183	191	57	762	11	444 130	0,50
2020	2 498	1 187	114	131	1 047	19	360 622	0,69
Коефіцієнт кореляції**	1,000	0,932	0,721	0,705	0,934	0,541	-0,724	0,965
Середнє значення	1 510	858	67	53	520	12	508 285	0,32
Коефіцієнт варіації, %	59,4	56,8	98,3	66,1	75,7	51,7	14,0	69,0
Середній темп приросту, %	22,7	16,5	37,9	30,8	31,7	30,2	-6,2	30,8

* УКП – усього зареєстрованих кримінальних правопорушень;

** коефіцієнт парної кореляції із сукупною кількістю зареєстрованих основних кіберзлочинів.

Джерело: складено автором на основі [3] та власних досліджень

Основні зміни у структурі основних кіберзлочинів, що відбулися за 2013–2020 рр., стосувалися співвідношення часток кримінальних правопорушень за статтями 361 та 362 ККУ. Ці зміни ілюструють рис. 1.5 та 1.6.

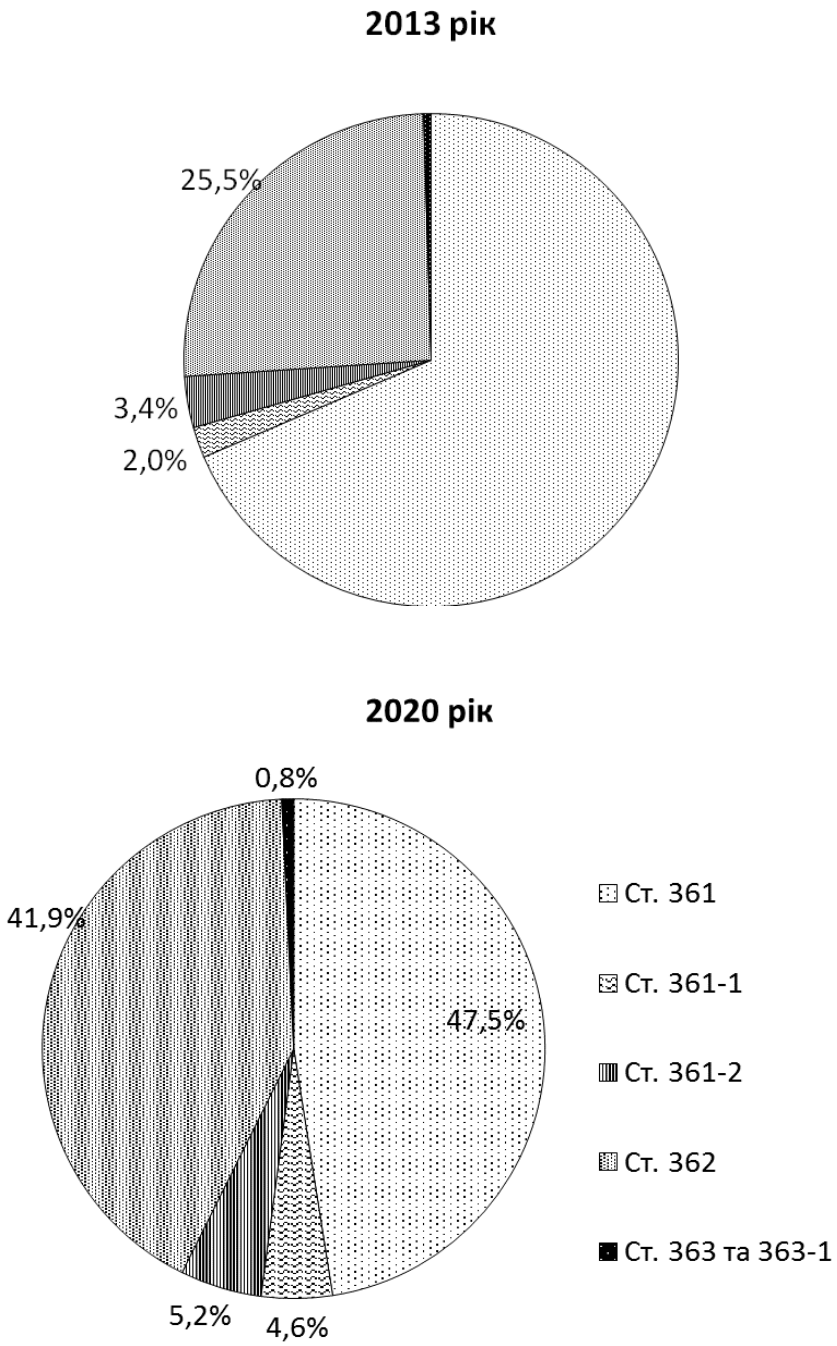


Рис. 1.5. Структура кількості зареєстрованих основних кіберзлочинів в Україні за 2013 та 2020 рр.

Джерело: складено автором на основі [3]

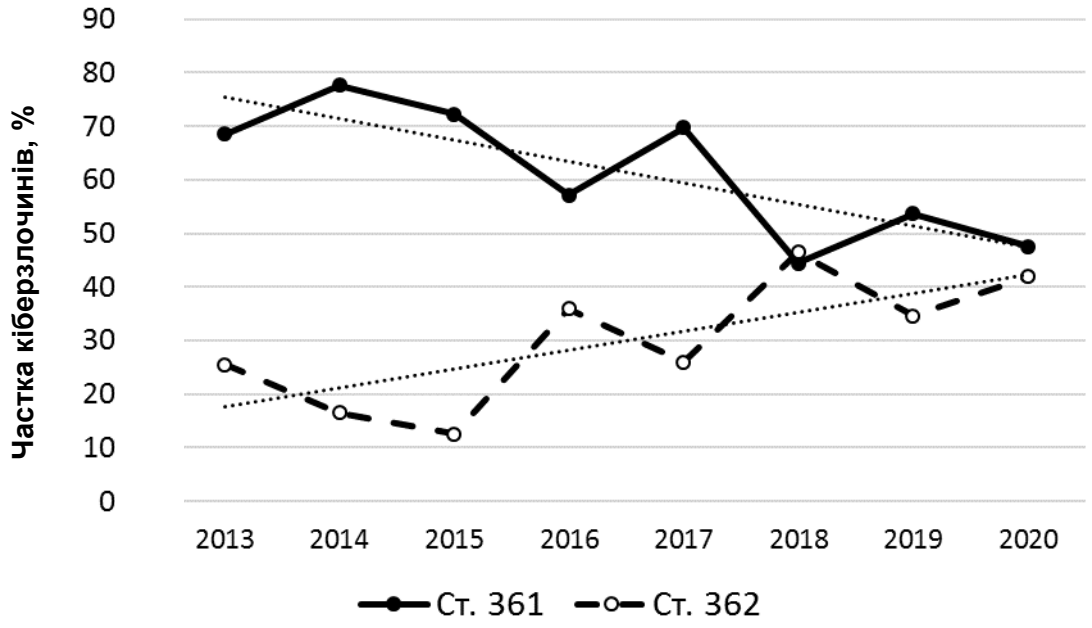


Рис. 1.6. Динаміка зареєстрованих основних кіберзлочинів за статтями 361 та 362 Кримінального кодексу України за 2013–2020 рр.

Джерело: складено автором на основі [3] та власних досліджень

Як свідчить рис. 4, є підстави говорити про наявність тенденцій у динаміці часток зареєстрованих основних кіберзлочинів за статтями 361 та 362: частка злочинів за ст. 361 демонструє тенденцію до зменшення, а за ст. 362, навпаки, – до збільшення. Якщо у 2013 році частка зареєстрованих злочинів за ст. 361 більше ніж у 2,5 раза перевищувала частку злочинів за ст. 362, то у 2020 році ці показники майже зрівнялися.

Склад зареєстрованих основних кіберзлочинів доцільно розглянути також в аспекті діяльності правоохоронних органів, що виявляли злочини. Цей склад характеризує табл. 1.4.

Серед основних кіберзлочинів переважна більшість була виявлена підрозділами Національної поліції (див. табл. 1.4), якою за період з 2013 по 2020 рік було викрито таких кіберзлочинів понад 95 % у середньому щорічно (найнижче значення – 93 % – було зафіксовано у 2015 р., а найвище – 97,7 % – у 2017 р.) від тієї кількості, яку зареєстрував і відобразив у своїй звітності Офіс

Генерального прокурора. В свою чергу, у складі Національної поліції приблизно половина виявлених основних кіберзлочинів припадає на департамент кіберполіції.

Таблиця 1.4

Роль Національної поліції та департаменту кіберполіції (ДКП) у виявленні основних кіберзлочинів в Україні за 2013–2020 рр.

Рік	Виявлено (зареєстровано) основних кіберзлочинів						
	Сукупна кількість (100 %)	Національною поліцією		ДКП (у складі Національної поліції)		іншими правоохоронними органами	
		кіль-кість	частка, %	кіль-кість	частка, %	кіль-кість	частка, %
2013	595	568	95,5	×	×	27	4,5
2014	443	418	94,4	×	×	25	5,6
2015	598	556	93,0	×	×	42	7,0
2016	865	818	94,6	388	44,9	47	5,4
2017	2573	2514	97,7	1199	46,6	59	2,3
2018	2301	2241	97,4	1120	48,7	60	2,6
2019	2204	2088	94,7	983	44,6	116	5,3
2020	2498	2338	93,6	1247	49,9	160	6,4

Джерело: складено автором на основі [3] [4]

Крім Національної поліції, до виявлення кіберзлочинів були причетні також Державне бюро розслідувань; органи безпеки; органи, що здійснюють контроль за додержанням податкового законодавства; Національне антикорупційне бюро. Саме вони фігурують у табл. 1.4 під назвою «інші правоохоронні органи», роль яких є незначною.

Окрім основних кіберзлочинів, підрозділи Національної поліції виявляли та розслідували переважну більшість супутніх кіберзлочинів. Динаміку кількості цих злочинів за даними звітності Національної поліції ілюструє рис. 1.7.

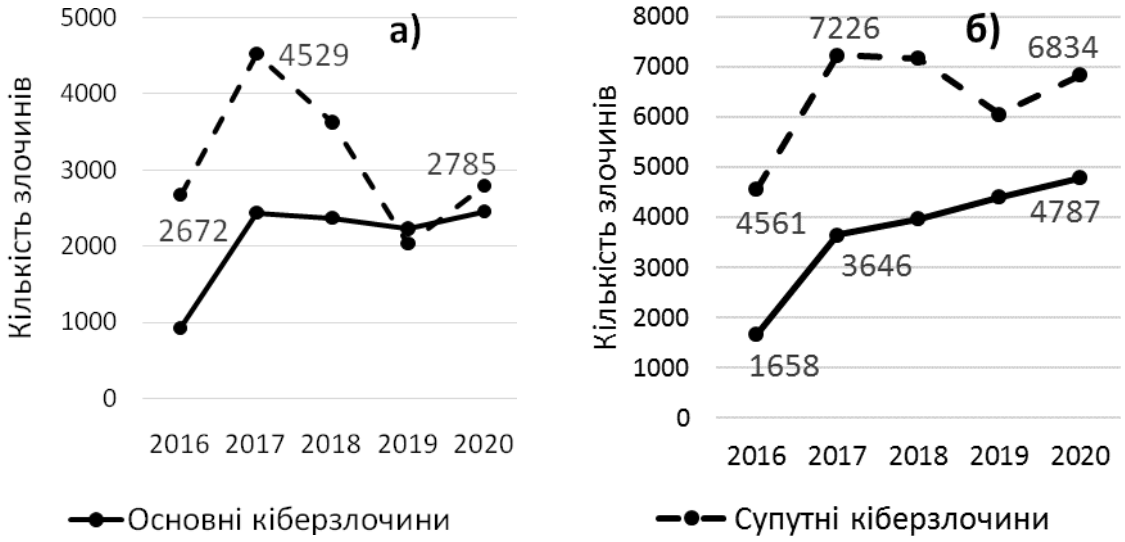


Рис. 1.7. Виявлення та супроводження кіберзлочинів підрозділами Національної поліції України протягом 2016–2020 рр.: а) виявлені злочини; б) злочини, що перебували у провадженні

Джерело: складено автором на основі [4]

Як свідчать дані рис. 1.7, кількість супутніх кіберзлочинів, які виявила та супроводжувала Національна поліція, перевищує число основних кіберзлочинів (винятком є лише кількість виявлених кіберзлочинів у 2019 році). Також важливим є той факт, що кількість кіберзлочинів, що перебували у провадженні, суттєво перевищує кількість виявлених кіберзлочинів (і особливо значним це перевищення є для супутніх кіберзлочинів). Цей факт є свідченням того, що підрозділи Національної поліції не в змозі закінчити провадження всіх виявлених кіберзлочинів впродовж року. Таке становище не є критичним за умови, що кількість злочинів, які перебували у провадженні та досудове розслідування за якими не закінчено, не починає зростати експоненціально.

Відсутність гострої проблеми стрімкого зростання кількості кіберзлочинів, що перебували у провадженні підрозділів Національної поліції, ілюструє рис. 1.8.

Рис. 1.8. Кількість кіберзлочинів (загалом, основних та супутніх), що перебували у провадженні підрозділів Національної поліції, в Україні за 2016–2020 рр.

Джерело: складено автором на основі [4]

Стрімке збільшення кількості кіберзлочинів, що перебували у провадженні підрозділів Національної поліції, у 2017 році (див. рис. 1.8) частково пояснюється змінами у виявленні цих злочинів кіберполіцією (про що йшла мова вище у коментарі до рис. 1.3), тому не може оцінюватися як фактор погіршення стану кіберзлочинності.

Так само не спостерігалося експоненціального (або іншого стрімкого) зростання кількості кіберзлочинів, досудове розслідування за якими не було закінчено за підсумками року, як свідчать дані табл. 1.5.

Хоча за даними табл. 1.5 має місце зростання коефіцієнта незакінчених досудових розслідувань кіберзлочинів, його середньорічний темп приросту є незначним – таким, що не підтверджує наявність загальної проблеми накопичення нерозслідуваних кіберзлочинів.

Таблиця 1.5

Незакінчені досудові розслідування кіберзлочинів Національною поліцією (усього) та підрозділами департаменту кіберполіції (ДКП) в Україні за 2016–2020 рр.

Рік / показник	Кількість кіберзлочинів, що перебували у провадженні		Кількість кіберзлочинів, досудове розслідування за якими не закінчено		Коефіцієнт незакінчених досудових розслідувань кіберзлочинів	
	Усього	ДКП	Усього	ДКП	Усього	ДКП
2016	6219	2984	3084	1076	0,496	0,361
2017	10872	5328	4930	1574	0,453	0,295
2018	11131	4864	6035	1841	0,542	0,378
2019	10459	3734	6087	1790	0,582	0,479
2020	11621	4783	6333	2125	0,545	0,444
Середнє значення	10060	4339	5294	1681	0,526	0,387
Коефіцієнт варіації, %	19,5	19,7	22,8	20,8	8,5	16,7
Середній темп приросту, %	16,9	12,5	19,7	18,5	2,4	5,4

Джерело: складено автором на основі [4] та власних досліджень

Якщо розглянути склад сукупної кількості кіберзлочинів (основних та супутніх), до виявлення та супроводження яких безпосередньо причетні підрозділи Національної поліції, з огляду на окремі групи злочинів (відповідно до рис. 1.3), то загалом його можна охарактеризувати як нестабільний. Зокрема, кількість скоєних та виявлених кіберзлочинів трьох (із чотирьох наявних) груп за 2016–2020 рр. демонструвала значні коливання. Лише кількість кіберзлочинів у сфері обігу протиправного контенту і телекомунікацій демонструвала динаміку поступового зменшення, що ілюструє рис. 1.9.

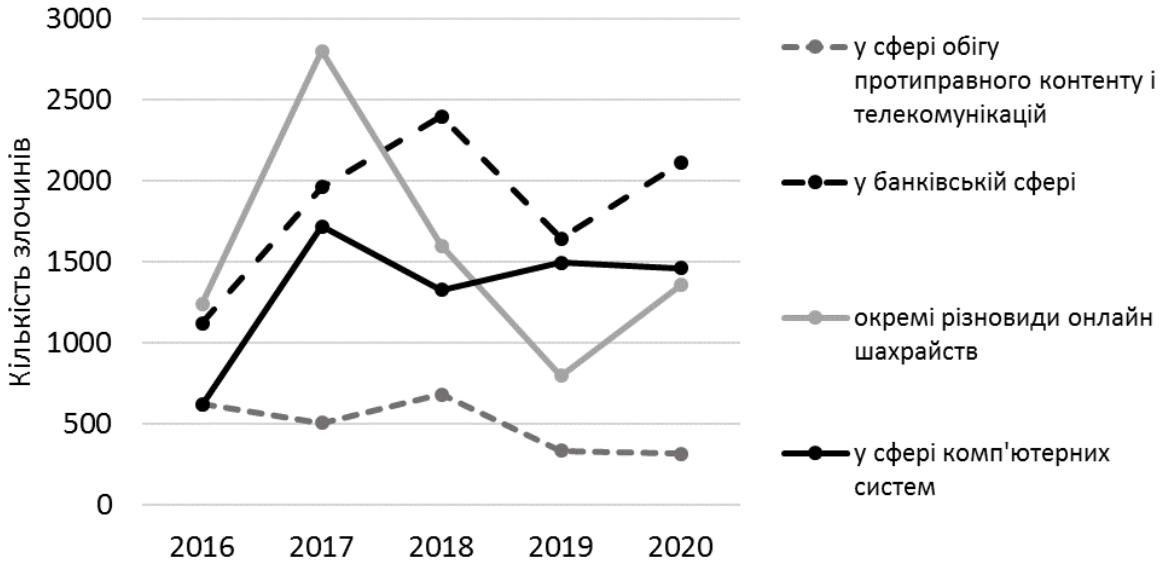


Рис. 1.9. Загальна кількість кіберзлочинів, скоєних в Україні і виявлених Національною поліцією за 2016–2020 рр., в аспекті окремих груп

Джерело: складено автором на основі [4] та власних досліджень

Така нестабільність складу кіберзлочинів, серед іншого, є негативним чинником впливу на поглиблення спеціалізації окремих підрозділів та підвищення професійного рівня фахівців підрозділів Національної поліції, що забезпечують боротьбу з кіберзлочинністю.

Нестабільна динаміка кількості скоєних кіберзлочинів окремих груп, що видно з рис. 1.9, призвела до структурних зрушень, серед яких привертають увагу:

– по-перше, суттєве зменшення частки супутніх кіберзлочинів;

– по-друге, суттєве збільшення кількості кіберзлочинів у банківській сфері (ця група за кількістю скоєних злочинів є першою і суттєво переважає будь-яку з решти груп) та у сфері комп’ютерних систем (ця група, яка була останньою у 2016 році, стала другою у 2020 році) (рис. 1.10).

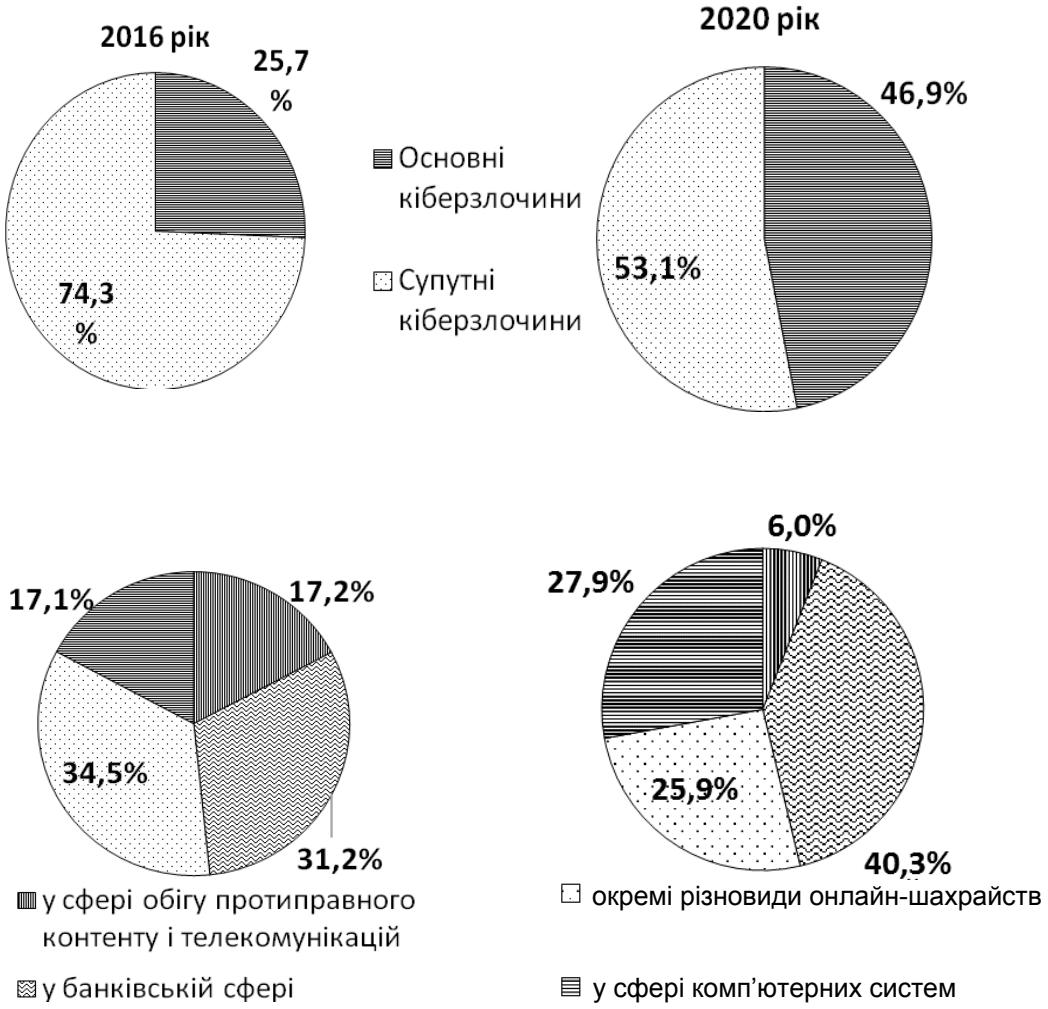


Рис. 1.10. Структура загальної кількості кіберзлочинів (основних та супутніх), скоєних в Україні і виявлених Національною поліцією за 2016 та 2020 рр.

Джерело: складено автором на основі [4] та власних досліджень

Нестабільність окремих груп кіберзлочинів виявилась пов'язаною з проблемою накопичення нерозслідуваних злочинів. Якщо загалом (для всіх кіберзлочинів разом), як було показано вище, ця проблема виглядає малозначущою, то для найбільш нестабільної групи – окремих різновидів онлайн-шахрайств – вона постає досить гостро як для підрозділів Національної поліції загалом, так і для департаменту кіберполіції зокрема.

Окремою специфічною складовою здослідження стану кіберзлочинності є її аналіз за окремими регіонами України. Актуальність такого аналізу зберігається, незважаючи на загальнонаціональний та навіть інтернаціональний характер окремих кіберзлочинів, оскільки об'єкти кіберзлочинної інфраструктури мають територіальне розташування і місце скоєння злочину зазвичай ідентифікується.

Розподіл кількості зареєстрованих основних кіберзлочинів за регіонами України на основі даних за 2020 рік та за січень–березень 2021 року, а також значення показників кількості цих злочинів на 100 тис. жителів ілюструє табл. 1.6.

Таблиця 1.6

Основні кіберзлочини, що зареєстровані за регіонами України, за 2020 р. та січень–березень 2021 р.

Область	2020 рік				січень-березень 2021 року			
	Зареєстровано, усього		На 100 тис. жителів		Зареєстровано, усього		На 100 тис. жителів	
	кількість	ранг	кількість	ранг	кількість	ранг	кількість	ранг
Україна*	2706	×	6,48	×	864	×	2,08	×
Вінницька	22	23	1,43	23	26	10	1,70	8
Волинська	192	5	18,65	3	70	5	6,82	2
Дніпропетровська	99	10	3,13	17	34	8	1,08	15
Донецька	46	17	1,12	24	50	6	1,22	12
Житомирська	63	16	5,24	12	12	16	1,01	17
Закарпатська	347	1	27,72	1	152	1	12,17	1
Запорізька	38	19	2,27	19	8	21	0,48	23
Івано-Франківська	108	8	7,91	9	79	4	5,81	3
Київська	76	13	4,26	14	15	13	0,84	18
Кіровоградська	64	15	6,91	11	4	25	0,44	24
Луганська	14	25	0,66	25	7	23	0,33	25
Львівська	126	7	5,03	13	85	3	3,41	5
Миколаївська	262	4	23,52	2	12	16	1,08	14
Одеська	294	3	12,39	4	38	7	1,61	9
Полтавська	27	21	1,96	22	25	11	1,83	7
Рівненська	94	12	8,17	8	15	13	1,31	11
Сумська	22	23	2,07	21	6	24	0,57	22
Тернопільська	23	22	2,22	20	12	16	1,17	13
Харківська	95	11	3,59	16	18	12	0,68	21

Закінчення табл. 1.6

Область	2020 рік				січень-березень 2021 року			
	Зареєстровано, усього		На 100 тис. жителів		Зареєстровано, усього		На 100 тис. жителів	
	кількість	ранг	кількість	ранг	кількість	ранг	кількість	ранг
Херсонська	41	18	4,01	15	11	19	1,08	16
Хмельницька	36	20	2,88	18	30	9	2,42	6
Черкаська	131	6	11,05	5	9	20	0,77	20
Чернівецька	71	14	7,90	10	13	15	1,45	10
Чернігівська	108	8	10,98	6	8	21	0,82	19
м. Київ	307	2	10,35	7	125	2	4,22	4

** Без урахування тимчасово окупованої території Автономної Республіки Крим і м. Севастополя*

Джерело: складено автором на основі [5], [7] та власних досліджень

За даними табл. 1.6, у 2020 році лідером за кількістю зареєстрованих кіберзлочинів була Закарпатська область, яка помітно випередила столицю. У січні–березні 2021 року м. Київ так само залишав на другому місці, поступаючись Закарпаттю, при тому, що ранги показника кількості зареєстрованих основних кіберзлочинів (колонка «Зареєстровано, усього» у табл. 1.6) решти областей (крім Волинської, Київської та Житомирської) зазнали змін.

Також привертає особливу увагу той факт, що Закарпатська область за підсумками 2020 року та січня–березня 2021 року має найбільше значення показника зареєстрованих кіберзлочинів на 100 тис. жителів порівняно з іншими регіонами України (див. табл. 1.6). Для з'ясування причин такої ситуації необхідно провести додаткові поглиблені дослідження на регіональному рівні.

Для оцінювання рівномірності розподілу кількості зареєстрованих основних кіберзлочинів за регіонами України був обчислений коефіцієнт Джині (*Gini*) за формулою:

$$G = \frac{2 \cdot \sum_i^n i \cdot y_i}{n \cdot \sum_{i=1}^n y_i} - \frac{n+1}{n} = \sum_{i=1}^n X_i \cdot Q_{i+1} - \sum_{i=1}^n X_{i+1} \cdot Q_i, \qquad (1.1)$$

де G – коефіцієнт Джині, причому $0 \leq G \leq 1$ (чим ближче значення до нуля, тим більш рівномірним є розподіл показника, що досліджується);

y – показник, однорідність якого досліджується, – частка регіону у загальній кількості зареєстрованих основних кіберзлочинів в Україні – причому $y_i \leq y_{i+1}$ (тобто передбачається попереднє ранжування показників для всіх регіонів у порядку зростання);

n – кількість регіонів України, $n = 25$ (без урахування тимчасово окупованої території Автономної Республіки Крим і м. Севастополя);

X – кумулятивна частка (інтегральний відсоток) від загальної кількості регіонів України, $X_i = i / n$, а $X_n = 1$ (або 100 %);

Q – кумулятивна частка (інтегральний відсоток) від загальної суми показника, однорідність якого досліджується, $Q_n = 1$ (або 100 %).

За даними 2020 року розподіл кількості зареєстрованих основних кіберзлочинів між регіонами України виявився більш нерівномірним, ніж розподіл населення (див. рис. 1.11).

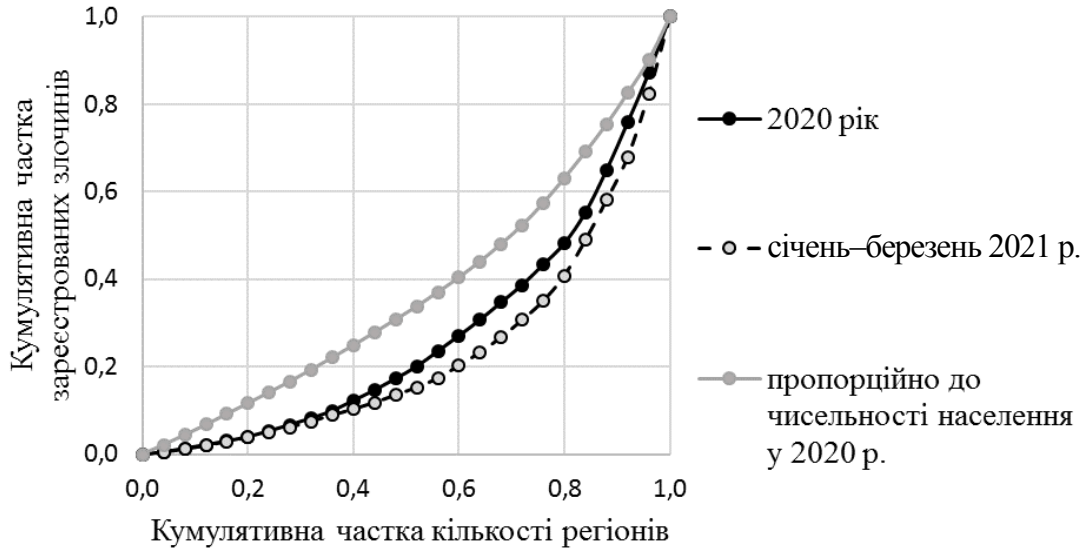


Рис. 1.11. Криві Лоренца, що характеризують рівномірність розподілу зареєстрованих основних кіберзлочинів між регіонами України за 2020 р. та січень–березень 2021 р.

Джерело: складено автором на основі [5] та власних досліджень

У січні–березні 2021 року нерівномірність розподілу кількості зареєстрованих основних кіберзлочинів між регіонами України посилилася, про що свідчать криві Лоренца на рис. 1.11 та значення коефіцієнтів Джині:

• за 2020 рік – 0,452;

• за січень–березень 2021 року – 0,528;

• пропорційно до чисельності населення у 2020 році (довідково, для порівняння) – 0,253.

Загалом стан кіберзлочинності в Україні за результатами проведеного аналізу можна вважати задовільним, а серед виявлених проблем виділимо такі:

1. Відсутність повної інформації про кіберзлочини у відкритих джерелах, без чого проведення поглиблених досліджень за цією темою неможливе.

2. Неузгодженість щодо класифікації кіберзлочинів під час укладання звітності тими органами, які відповідають за боротьбу з кіберзлочинністю (зокрема, Офісом Генерального прокурора та Національною поліцією).

3. Щорічне зростання частки основних кіберзлочинів у сукупній кількості зареєстрованих кримінальних правопорушень (впродовж усього періоду дослідження, починаючи з 2013 року, за винятком 2018 року), хоча масштаби кіберзлочинності в Україні залишались порівняно незначними.

4. Нестабільність складу кіберзлочинів, що створило негативні передумови для спеціалізації окремих підрозділів та підвищення професійного рівня фахівців органів, які відповідають за боротьбу з кіберзлочинністю.

5. Суттєва нерівномірність розподілу кількості зареєстрованих основних кіберзлочинів між регіонами України, яка посилилася в умовах пандемії Covid-19.

6. Аномально високі показники кількості зареєстрованих основних кіберзлочинів у Закарпатській області, для пояснення чого необхідно провести додаткові дослідження на регіональному рівні.

Список бібліографічних посилань

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. Дата оновлення: 15.12.2021. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 13.06.2022).

2. Кримінальний кодекс України від 05.04.2011 № 2341-III. Дата оновлення: 23.04.2022. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 13.06.2022).

3. Статистика. Єдиний звіт про кримінальні правопорушення // Офіс Генерального прокурора. URL : https://www.gp.gov.ua/ua/stat_n_st?dir_id=104402 (дата звернення: 13.06.2022).

4. Річні звіти // Національна поліція. URL : https://www.npu.gov.ua/activity/zviti/richni-zviti/ (дата звернення: 13.06.2022).

5. Доступ до публічної інформації // Рада національної безпеки і оборони України. URL : https://www.rnbo.gov.ua/ua/-Publichna-informatsiia.html (дата звернення: 13.06.2022).

6. Про інформацію : Закон України від 02.10.1992. № 2657-XII. Дата оновлення: 01.01.2022. URL : https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 13.06.2022).

7. Статистична інформація. Державна служба статистики України. URL : http://www.ukrstat.gov.ua (дата звернення: 13.06.2022).

1.3. Захист корпоративної інформації як інструмент забезпечення ефективності підприємства

Основним трендом сучасного світу є трансформація індустріального суспільства в постіндустріальне, яка відбувається в умовах посилення глобалізаційних процесів, розширення сфери послуг і нематеріального виробництва, впливу інформаційно-комунікативних технологій (далі – ІКТ) на процеси розвитку науково-технічного прогресу, у тому

числі масштабного, глибинного й динамічного проникнення ІТ в усі сфери життєдіяльності особи, суспільства, суб'єктів господарювання й держави. При цьому абсолютно очевидною є залежність рівня цифровізації суспільства від рівня його добробуту і темпів економічної динаміки.

З огляду на це «розвиток інформаційного суспільства в Україні та впровадження новітніх ІКТ в усі сфери суспільного життя і в діяльність органів державної влади та органів місцевого самоврядування визнається одним з пріоритетних напрямів державної політики» [1].

Так, відповідно до Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр. основними стратегічними цілями розвитку інформаційного суспільства в Україні є:

– прискорення розробки та впровадження новітніх конкурентоспроможних ІКТ в усі сфери суспільного життя, зокрема в економіку України і в діяльність органів державної влади та органів місцевого самоврядування;

– забезпечення комп'ютерної та інформаційної грамотності населення, насамперед шляхом створення системи освіти, орієнтованої на використання новітніх ІКТ у формуванні всебічно розвиненої особистості;

– розвиток національної інформаційної інфраструктури та її інтеграція зі світовою інфраструктурою;

– державна підтримка нових «електронних» секторів економіки (торгівлі, надання фінансових і банківських послуг тощо);

– створення загальнодержавних інформаційних систем, насамперед у сферах охорони здоров'я, освіти, науки, культури, охорони довкілля;

– збереження культурної спадщини України шляхом її електронного документування;

– державна підтримка використання новітніх ІКТ засобами масової інформації;

– використання ІКТ для вдосконалення державного управління, відносин між державою і громадянами, становлення електронних форм взаємодії між органами державної влади та органами місцевого самоврядування і фізичними та юридичними особами;

– досягнення ефективної участі всіх регіонів у процесах становлення інформаційного суспільства шляхом децентралізації та підтримки регіональних і місцевих ініціатив;

– захист інформаційних прав громадян, насамперед щодо доступності інформації, захисту відомостей про особу, підтримки демократичних інститутів та мінімізації ризику «інформаційної нерівності»;

– вдосконалення законодавства з регулювання інформаційних відносин;

– покращення стану інформаційної безпеки в умовах використання новітніх ІКТ [1].

Відповідно до згаданого Закону, саме реалізація завдань розвитку інформаційного суспільства дасть змогу досягти найважливіших завдань розвитку держави, зокрема:

– підвищити національну конкурентоспроможність за рахунок розвитку людського потенціалу, насамперед у високоінтелектуальних сферах праці, а також розширити експортний потенціал ІКТ-індустрії України;

– поліпшити життєвий рівень населення завдяки економічному зростанню, забезпеченню прав і свобод людини, наданню рівного якісного доступу до інформації, освіти, послуг закладів охорони здоров’я та адміністративних послуг органів державної влади та органів місцевого самоврядування, створенню нових робочих місць і розширенню можливостей щодо працевлаштування населення, забезпеченню соціального захисту вразливих верств населення, зокрема людей, що потребують соціальної допомоги та реабілітації;

– сприяти становленню відкритого демократичного суспільства, яке гарантуватиме дотримання конституційних прав громадян щодо участі у суспільному житті, прийнятті відповідних рішень органами державної влади та органами місцевого самоврядування [1].

Водночас в умовах цифровізації суспільства, зростаючої ролі інформації як у житті людини, так і у функціонуванні підприємства в геометричній прогресії збільшуються ризики втрати інформації, особливо внаслідок кібератак. Усвідомлення негативного впливу втрати інформації на стан економічних систем різного рівня потребує захисту інформації, інформаційного простору, розроблення дієвих механізмів протидії різноманітним загрозам інформаційній безпеці. Необхідність запровадження заходів та політик з протидії інформаційним загрозам декларується як на рівні держави, так і на рівні окремих суб'єктів господарювання.

У наукових дослідженнях останніх років велика увага приділяється збереженню економічної безпеки підприємства, складовою якої є інформаційна безпека. Вже аксіоматичною визнана залежність результатів функціонування, досягнення цілей від рівня економічної безпеки та її інформаційної складової. У працях науковців зустрічаються різні тлумачення поняття «інформаційна безпека».

Так, О. Сороківська, В. Гевко інформаційну безпеку підприємства трактують як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [2]. Таким чином, автори фактично переводять термін «інформаційна безпека» з розряду «понять» до розряду «категорій». Проте варто зазначити, що більшість дослідників, вивчаючи зміст інформаційної безпеки, залишаються на полі понятійного апарату і розглядають її як певний стан.

На думку Л. Дж. Хофмана, інформаційна безпека – це стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації [3].

Натомість О. Горбатюк, вважає, що інформаційна безпека становить стан захищеності потреб в інформації особистості, суспільства і держави, за якого забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх чи зовнішніх інформаційних загроз. [4].

Подібне тлумачення інформаційної безпеки надається більшістю авторами, зокрема В. Богуш [5]. Загалом воно відповідає вітчизняному законодавчому визначенню цього поняття, згідно з яким інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [1].

Переважна більшість науковців, законодавчі акти України визначають інформаційну безпеку як «стан захищеності» інтересів суб'єктів різного рівня від недобросовісних дій щодо інформації. Зважаючи на те, що важливим суспільним суб'єктом суспільства є підприємство, корпоративну інформаційну безпеку пропонуємо розглядати як стан захищеності інтересів підприємства від недобросовісних дій (умисних та неумисних) стосовно корпоративної інформації, що спрямовані на всі компоненти корпоративного інформаційного простору. Відтак можна прослідкувати чіткий взаємозв'язок між захистом корпоративної інформації та досягненням високих результатів функціонування підприємства, які і є відображенням його інтересів (див. рис. 1.12).

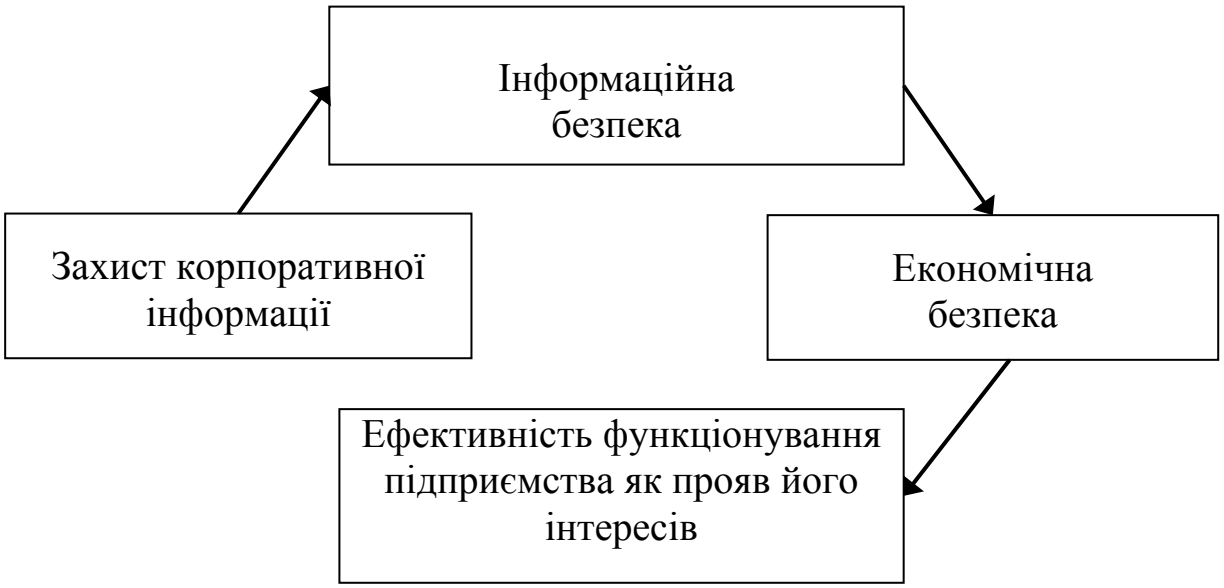


Рис. 1.12. Логіка взаємозв'язку захисту корпоративної інформації та ефективності функціонування підприємства

Джерело: складено автором

Розглянемо докладніше механізм зазначеного вище логічного зв'язку між захистом корпоративної інформації та ефективністю функціонування підприємства.

Так, корпоративний інформаційний простір характеризується низкою параметрів. У сучасних наукових дослідженнях сьогодні відсутня їх систематизована характеристика. На основі аналізу, узагальнення та розвитку поглядів науковців щодо змістовного наповнення цього поняття та його авторського бачення пропонуємо виокремлювати такі параметри корпоративного інформаційного поля (КІП):

1. Інтенсивність інформаційного обміну між внутрішніми суб'єктами КІП та зовнішнім середовищем підприємства. Адже, як слушно зазначає Н. Науменко, «ефективність розвитку системи багато в чому забезпечується за рахунок інтенсивності інформаційного обміну та залежить від характеристики та умов розповсюдження потоків інформації в просторі» [4]. Таку інтенсивність можна охарактеризувати кількістю «інформаційних транзакцій» між учасниками інформаційного процесу.

2. Насиченість інформаційних полів, яка характеризується кількістю, деталізованістю, систематизованістю інформаційних показників, які зберігаються в інформаційному просторі підприємства. «В процесі обміну відбувається збільшення інформації за рахунок крос-взаємодії інформаційного фактора їх суб'єктів, і, отже, можна зробити висновок про незворотний характер зростання інформації як умови і результату еволюції систем» [4].

3. Рівень цифровізації КІП, яку можна охарактеризувати рівнем охоплення процесів зберігання, оброблення, передачі інформації за допомогою цифрових технологій.

4. Цифрова компетентність персоналу, котра може вимірюватись його вмінням користуватися сучасними інформаційними технологіями.

5. Рівень інноваційності інформаційної інфраструктури, що характеризує ступінь використання найбільш нової техніки та технологій для процесів зберігання, оброблення, передачі інформації.

6. Рівень корпоративної інформаційної культури, який характеризує ступінь поваги та дотримання задекларованої філософії інформаційних комунікацій підприємства як всередині нього, так і з зовнішнім середовищем.

7. Ступінь захищеності КІП від потенційних загроз втручання та заподіяння шкоди окремим компонентом КІП.

8. Якість регламентації КІП, тобто наявність, зміст регламентних документів, які визначають порядок здійснення інформаційного процесу як всередині підприємства, так і з суб'єктами зовнішнього середовища.

Зазначені параметри перебувають у тісному взаємозв'язку, тобто один з параметрів може впливати на інші. Наприклад, рівень цифровізації КІП, цифрова компетентність персоналу суттєво впливають на інтенсивність інформаційного обміну та насиченість інформаційних полів. Рівень захищеності КІП суттєво обумовлюється рівнем цифрових компетентностей персоналу, рівнем корпоративної інформаційної культури, якістю регламентації КІП тощо. Система

окреслених параметрів визначає якість корпоративного інформаційного поля та здатність виконувати ним його важливі функції.

Корпоративний інформаційний простір як сфера розгортання важливих процесів на підприємстві виконує комплекс важливих функцій його розвитку, до яких переважна більшість науковців зараховують такі [7, 8 та ін.]:

– інтегрувальна – об'єднує в єдине просторово-комунікативне і соціокультурне середовище різні види економічної діяльності;

– комунікативна – створюється особливе середовище транскордонної, інтерактивної і мобільної комунікації різних суб'єктів економічної діяльності, у межах якого вони здійснюють інформаційний обмін;

– актуалізуюча – в інформаційному просторі здійснюється актуалізація інтересів різних суб'єктів економічної діяльності шляхом реалізації ними інформаційної політики;

– геополітична – формуються власні ресурси й змінюється значущість традиційних ресурсів, створюючи нове середовище геополітичних відносин і конкуренції;

– соціальна – інформаційний простір трансформує суспільство і змінює характер та зміст соціально-економічних відносин у всіх сферах: політиці, культурі, науці, релігії тощо.

Критично-конструктивний аналіз наявних підходів, їх розвиток та імплементація щодо підприємства дозволили нам таким чином визначити функції корпоративного інформаційного простору:

– інтегрувальна – об'єднує в єдине просторово-комунікативне і соціокультурне середовище різні служби та підрозділи підприємства, спрямовуючи їх на досягнення спільних корпоративних цілей;

– комунікативна – створюється особливе середовище інтерактивної і мобільної комунікації різних служб та підрозділів підприємства, у межах якого вони здійснюють інформаційний обмін;

– актуалізуюча – в інформаційному просторі здійснюється актуалізація інтересів підприємства у зовнішньому середовищі шляхом реалізації ним інформаційної політики та актуалізація цілей і завдань підприємства, їх трансляція для внутрішніх користувачів інформації;

– соціальна – інформаційний простір трансформує суспільство і змінює характер та зміст соціально-економічних відносин, у тому числі всередині самого підприємства;

– навчальна – корпоративний інформаційний простір створює умови для навчання персоналу, трансформуючи підприємство в організацію, що навчається;

– інноваційна – корпоративний інформаційний простір є сприятливим середовищем для створення інновацій, пошуку та прийняття інноваційних рішень;

– акселеруюча – корпоративний інформаційний простір створює передумови для підвищення ефективності використання всіх видів ресурсів підприємства за рахунок швидкого обміну інформацією щодо їх стану.

Зв'язок між параметрами корпоративного інформаційного поля та здатністю ним виконувати покладені функції репрезентує рис. 1.13.

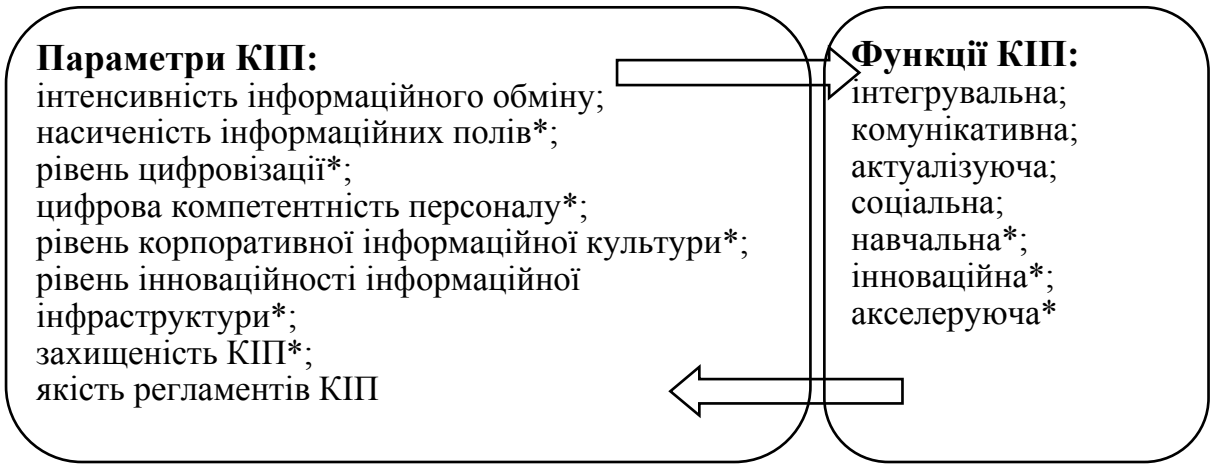


Рис. 1.13. Взаємозв'язок параметрів та функцій корпоративного інформаційного поля

** Запропоновано автором*

Джерело: складено та розвинено автором за [7, 8 та ін.]

Висока якість параметрів корпоративного інформаційного поля дозволяє йому на якісному рівні виконувати свої функції, що, у свою чергу, дає змогу в цілому підвищувати результати діяльності за рахунок більш ефективного використання всього пулу ресурсів, а також вдосконалювати параметри корпоративного інформаційного простору.

Захищеність корпоративного інформаційного простору, будучи його важливим параметром, впливає на стан інших параметрів КІП та здатність виконувати ним свої функції на високому рівні, забезпечуючи інформаційну безпеку підприємства та реалізацію його інтересів.

Проте за сучасних умов в геометричній прогресії зростають загрози порушення корпоративного інформаційного простору, тобто створюється ситуація інформаційної небезпеки.

Здебільшого інформаційну безпеку характеризують трьома основними складовими: конфіденційність, цілісність і доступність інформації. Конфіденційність належить до захисту чутливої інформації від несанкціонованого доступу. Цілісність означає захист точності й повноти інформації та програмного забезпечення. Доступність – це забезпечення доступності інформації і основних послуг для користувача в потрібний для нього час [9].

Таким чином, всі дії, ситуації, фактори, події, які порушують зазначені характеристики шляхом впливу на компоненти корпоративного інформаційного поля, порушуючи інтереси підприємства, можна вважати загрозами інформаційній безпеці. У сучасних наукових дослідженнях відсутні одностайні та вичерпні підходи до класифікації таких загроз.

Так, вітчизняне законодавство визначає такі загрози інформаційної безпеки: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [1, ст. 102].

Пунктом 4 Державного стандарту України «Захист інформації. Технічний захист інформації. Основні положення» – ДСТУ 3396.0-96 визначено, що загрози можуть здійснюватися:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів [10].

Дослідник В. Ліпкан пропонує класифікувати загрози інформаційній національній безпеці відповідно до їх загальної класифікації: за джерелами походження: природного походження, техногенного походження, антропогенного походження; за ступенем гіпотетичної шкоди: загроза та небезпека; за повторюваністю вчинення: повторювані та продовжувані; за сферами походження: екзогенні та ендогенні; за ймовірністю реалізації: вірогідні, неможливі, випадкові; за рівнем детермінізму: закономірні та випадкові; за значенням: допустимі та неприпустимі; за структурою впливу: системні, структурні та елементні; за характером реалізації: реальні, потенційні, здійснені, уявні; за ставленням до них: об'єктивні та суб'єктивні [11].

Натомість А. Логінов визначає загрози як:

• розкриття інформаційних ресурсів;

• порушення цілісності інформаційних ресурсів;

• збій у роботі обладнання [12].

З метою вироблення рекомендацій щодо організації дієвих форм і методів забезпечення інформаційної безпеки Л. Євдоченко визначає і класифікує загрози за такими критеріями: за способом впливу на об'єкти інформаційної безпеки

(інформаційні, фізичні й програмно-математичні, організаційно-правові); за джерелами надходження (внутрішні та зовнішні); за характером вияву (політичні, економічні, організаційно-технічні) [13].

Наприклад, М. Макарова виділяє загрози, які характерні суто для мережі. Зокрема, вона ідентифікує такі загрози:

• дані навмисно перехоплюються, читаються або змінюються;

• користувачі ідентифікують себе неправильно (з шахрайською метою);

• користувач отримує несанкціонований доступ з однієї мережі до іншої [14].

Аналогічний, але дещо ширший підхід до виокремлення загроз інформаційній безпеці пропонує А. Погребняк, зазначаючи, що загрози можуть бути як випадковими, так і навмисними.

До випадкових загроз автор відносить: а) помилки обслуговуючого персоналу і користувачів; б) втрата інформації внаслідок неправильного її зберігання; в) випадкове знищення або заміна; г) збій у роботі устаткування, електроживлення, дискових систем, комплектуючих елементів мережі; д) некоректна робота програмного забезпечення, зокрема внаслідок зараження комп'ютерними вірусами тощо [15].

До навмисних він зараховує: а) несанкціонований доступ до інформації і мережевих ресурсів; б) розкриття і модифікація даних і програм, їх копіювання; в) розкриття, модифікація або підміна трафіка обчислювальної мережі; г) розроблення і поширення комп'ютерних вірусів, введення в програмне забезпечення логічних бомб; д) крадіжка магнітних носіїв і розрахункових документів; е) руйнування архівної інформації або навмисне її знищення; є) фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому; ж) перехоплення та ознайомлення з інформацією, яка передана по каналах зв'язку [15].

Узагальнюючи та розвиваючи зазначені підходи, пропонуємо таку класифікацію загроз інформаційній безпеці підприємства (табл. 1.7).

Варто зазначити, що цю класифікацію не потрібно вважати сталою. Інтенсивний розвиток інформаційних технологій, тенденції цифровізації суспільства в цілому і бізнесу зокрема призводять до постійного зростання інтенсивності та видів загроз.

Таблиця 1.7

Класифікація загроз інформаційній безпеці підприємства

Класифікаційна ознака	Види загроз
Спрямованість загрози за компонентами корпоративного інформаційного поля*	загрози інформаційним полям; загрози інформаційному процесу; загрози інформаційній культурі; загрози інформаційній інфраструктурі
За середовищем походження	зовнішні; внутрішні
За ступенем гіпотетичної шкоди	загрози; небезпека
За джерелами походження	природного походження; техногенного походження; антропогенного походження
За повторюваністю вчинення	повторювані; продовжувані
За ймовірністю реалізації	вірогідні; неможливі; випадкові
За рівнем ймовірності	з високим рівнем імовірності; з середнім рівнем імовірності; з низьким рівнем імовірності
За рівнем детермінованості	закономірні; випадкові
За потенційними наслідками*	допустимі; критичні; катастрофічні
За характером реалізації	реальні; потенційні; здійснені; уявні
За характером шкоди	неповнота, невчасність та невірогідність інформації, що використовується;

Закінчення табл. 1.7

Класифікаційна ознака	Види загроз
	негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації
За наявністю умислу	умисні; випадкові
За проявом та правовими наслідками	злочин; шахрайство; хуліганство
За типом	програмні; апаратні; інші
За метою	оперативні; тактичні; стратегічні

** Запропоновано автором*

Джерело: розвинено за [1, 11, 14, 15, 16, 17]

Водночас погоджуємося з тезою О. Золотар та І. Трубіна про важливе теоретико-прикладне значення класифікації загроз інформаційній безпеці. «Вона обумовлена потребою внутрішньо-логічної впорядкованості цієї системи і виконує дві важливі функції – евристичну та аналітичну. Евристична функція забезпечує пошук, виявлення існуючих загроз, орієнтацію в них, вивчення сукупності певних груп, що стосуються окремих об'єктів та суб'єктів безпеки, умов часу і простору. Аналітична функція полягає у розробленні методів аналізу цих загроз, перевірки її достовірності, виявлення шляхів їх нейтралізації» [18]. Тобто розуміння, вміння ідентифікувати, аналізувати загрози інформаційній безпеці, розробляти шляхи запобігання їм, нейтралізації лежить в основі захисту корпоративної інформації.

Таким чином, **захист корпоративної інформації пропонуємо визначати як систему принципів, методів та процесів протидії загрозам інформаційній безпеці підпри-**

ємства, які спрямовані на порушення функціонування корпоративного інформаційного поля, і передбачає їх ідентифікацію, аналіз, запобігання та нейтралізацію.

Узагальнюючи викладений вище матеріал, можна представити концепт-модель місця захисту корпоративної інформації у забезпеченні ефективного функціонування підприємства (рис. 1.14).

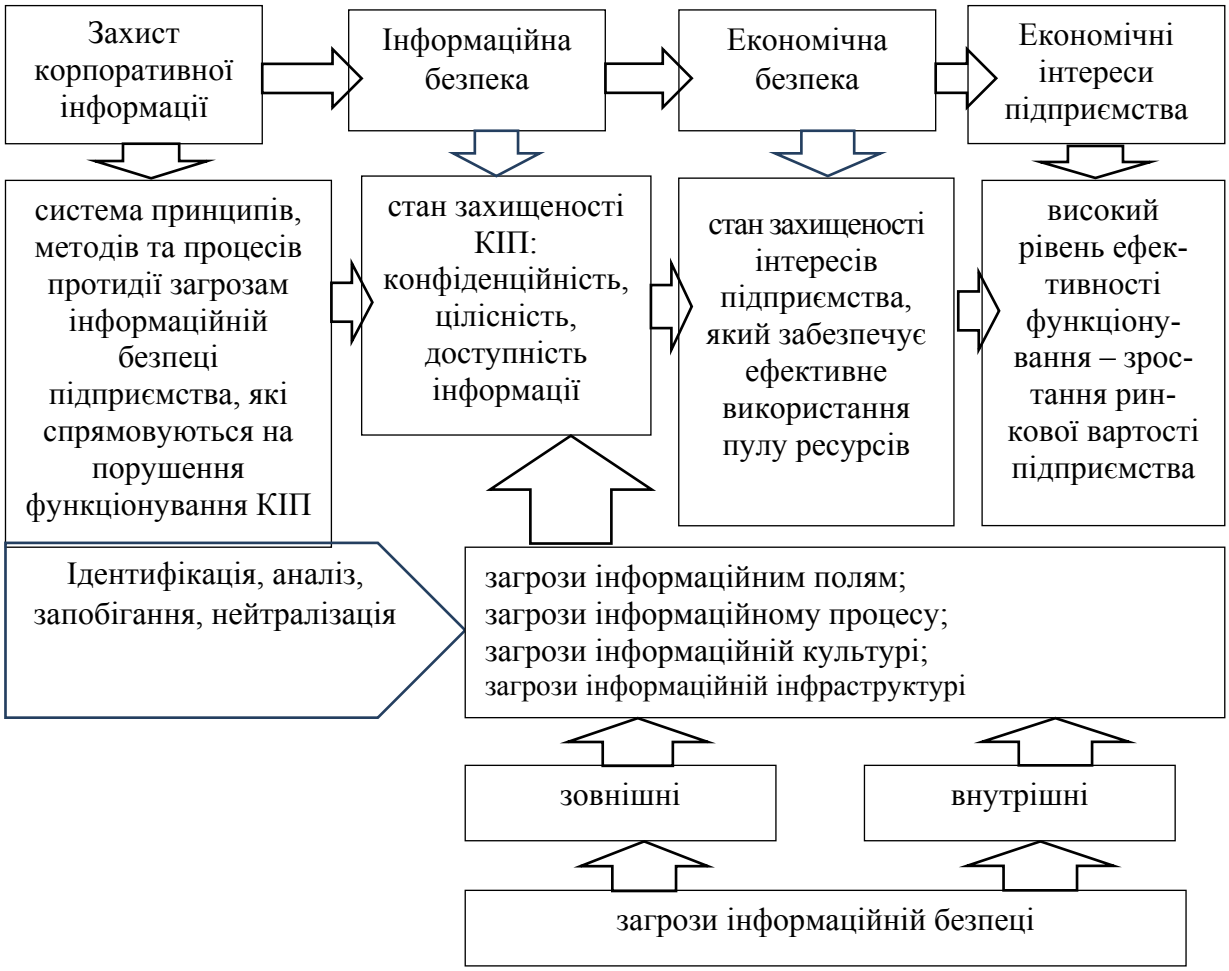


Рис. 1.14. Концепт-модель місця захисту корпоративної інформації у забезпеченні ефективного функціонування підприємства

Джерело: складено автором

Захист корпоративної інформації потребує розроблення дієвих механізмів протидії загрозам інформаційній безпеці підприємства, які узгоджуватимуться з сучасними концептуальними положеннями ефективності функціонування економічних систем.

Список бібліографічних посилань

1. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 № 537-V. Дата оновлення: 06.02.2007. URL : https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 13.06.2022).

2. Сороківська О. А., Гевко В. Л. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісник Хмельницького Нац. ун-ту*. 2010. № 2. Т. 2. С. 32–35.

3. Hoffman L. J., Lawson-Jenkins K., Blum J. Trust beyond security: an expanded trust model // Communications of the ACM. 2006. Vol. 49, № 7, P. 94–101.

4. Горбатюк О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. *Вісник Київського університету імені Т. Шевченка*. 1999. Серія «Міжнародні відносини». Вип. 14. С. 46–48.

5. Богуш В., Юдін О. Інформаційна безпека держави / Гол. ред. Ю.О. Шпак. Київ : «МК-Прес», 2005. 432 с.

6. Науменко Н. Ю. Особливості конкретизації методології формування інформаційного простору регіональних соціально-економічних систем. *Modern Economic*. № 14. 2019. С. 186–192.

7. Кузьміна О. М. Актуалізація формування єдиного інформаційного середовища організації. *Східна Європа: економіка, бізнес та управління*. № 5 (16). 2018. С. 289–292.

8. Дубняк К. А. Інформаційний простір: структура та функціональні параметри. *Держава та регіони*. Серія «Соціальні комунікації». № 4 (24). 2015. С. 21–25.

9. Близнюк І. М. Інформаційна безпека України та заходи її забезпечення. Науковий вісник Національної академії внутрішніх справ України. 2008. № 5. С. 206–214.

10. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення [Чинний від 1997.01.01]. Вид. офіц. Київ : Держстандарт України, 1996. 7 с.

11. Ліпкан В. А. Національна безпека України : навч. посіб. Київ : КНТ, 2009. 576 с.

12. Логінов А. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.07 / А. В. Логінов. Нац. академія внутрішніх справ України. Київ, 2005.

13. Євдоченко Л. О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації : автореф. … дис. канд. наук з держ. упр. : 25.00.01. Львів, 2011. 24 с.

14. Макарова М. В. Електронна комерція : посіб. для студ. вищ. навч. закладів. Київ : видавнич. центр «Академія», 2002. 272 с.

15. Погребняк А. В. Технології комп'ютерної безпеки : монографія. Рівне : МЕГУ, 2011. 117 с.

16. Бурячок В. Л., Гулак Г. М., Толубко В. Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : підручник. Київ : ТОВ «СІК ГРУП УКРАЇНА», 2015. 449 с.

17. Моделювання та аналіз безпеки розподілених інформаційних систем : навч. посіб. для студ. спец. 121 «Інженерія програмного забезпечення» / В. В. Литвинов, В. В. Казимир, І. В. Стеценко та ін. Чернігів : Чернігів. нац. технол. ун-т, 2016. 254 с.

18. Золотар О. О., Трубін І. О. Класифікація загроз інформаційній безпеці. *Інформація і право*. № 3 (9). 2013. С. 105–112.

1.4. Трансформація видів економічної ефективності управління підприємством в умовах інформатизації бізнесу

Ефективність є однією з базових економічних категорій, яка активно досліджується теоретиками та науковцями прикладного спрямування тривалий час. Це не випадково, адже ефективність є невід'ємною умовою існування підприємства в ринкових умовах.

Незважаючи на значний доробок з проблематики ефективності, на сьогодні немає єдиного підходу до трактування її змісту, а зміна умов господарювання призводить до трансформації її видів та методів вимірювання.

Ефективність підприємства як комплексний вимірник його функціонування обумовлюється значною кількістю чинників, роль та значимість яких змінюється залежно від умов функціонування. До числа таких завжди включають стан зовнішнього середовища та рівень управління підприємством, адже останній визначає здатність підприємства адаптуватися до змін, що відбуваються на ринку, та якість управлінських рішень, які забезпечують всі види діяльності підприємства. Таким чином, очевидною є значимість ефективності управління у забезпеченні ефективного функціонування підприємства.

Насамперед потребують з'ясування змісту поняття «економічна ефективність» та «економічна ефективність управління», їх розмежування та співвідношення.

Здебільшого, коли мова йде про економічну ефективність, її трактують як:

– відношення між витратами ресурсів і виробленим у результаті їх використання обсягом товару або послуги, або прибутку;

– виробництво продукту певної вартості за найменших витрат ресурсів;

– міра витрат підприємства на досягнення поставлених цілей [1].

Варто зазначити, що останнє трактування є більш близьким за змістом до поняття «результативність», дослідження якої вже виокремилось в окремий напрям [1–5]. Таким чином, доходимо висновку, що ефективність все ж таки характеризує співвідношення між певними економічними результатами функціонування підприємства та використаними для їх одержання ресурсами / понесеними витратами. Водночас наявні методичні підходи до оцінювання ефективності орієнтуються на використання фінансової звітності, даних аналітичного бухгалтерського обліку при розрахунку конкретних показників ефективності. Проте бухгалтерський облік не враховує таку важливу в економіці категорію, як «альтернативні витрати», тому важливим аспектом економічної ефективності є необхідність врахування альтернативних витрат.

Завжди актуальним питанням залишається вибір результативних показників діяльності, вимірників ресурсів та витрат, які мають співвідноситись у процесі оцінювання економічної ефективності. Такий вибір саме й обумовлюється тим, який вид економічної ефективності прагне оцінити аналітик.

Нині виокремлюють різні види ефективності.

Так, *за характером здійснюваних витрат* розрізняють ефективність всіх ресурсів та ефективність витрат (спожитих ресурсів). До ефективності всіх ресурсів відносять: ефективність виробничих засобів, ефективність трудових ресурсів, ефективність нематеріальних активів. До ефективності витрат належать: ефективність капітальних вкладень, ефективність поточних витрат, ефективність сукупних витрат. Такий поділ ґрунтується на постійній дилемі: при визначенні ефективності отриманий ефект потрібно відносити до всієї сукупності ресурсів чи лише її спожитої частини. Єдиної думки з цього приводу серед науковців немає і досі, тому погоджуємося з думкою про доцільність застосування обох видів ефективності.

Поширеним є поділ економічної ефективності *за видами діяльності*. Однак за цією класифікаційною ознакою окремі науковці при визначенні видів ефективності орієнтуються на види діяльності, що регламентуються П(С)БО [1], а інші

деталізують на основі функціональних напрямів управління [2, 3, 4]. Нам імпонує перша точка зору, проте ми повною мірою не погоджуємось із трактовкою змісту цих видів ефективності, що запропоновані С. П.Лобовим Відповідно, за цією ознакою варто виокремити такі види економічної ефективності й таке їх змістовне навантаження:

– ефективність операційної діяльності, яка характеризує міру отриманого ефекту від операційної діяльності до ресурсів підприємства;

– ефективність інвестиційної діяльності, котра відображає міру ефекту від інвестування коштів у різноманітні активи;

– ефективність фінансової діяльності, яка в узагальненому вигляді відображає співвідношення рівня дохідності активів до середньозважених витрат на залучення капіталу.

Розвиток процесного підходу призвів до виокремлення видів ефективності за видами бізнес-процесів, але єдиної позиції щодо видів ефективності за цією класифікаційною ознакою немає, а ті, що пропонуються в літературі, мають фрагментарний характер [1–5]. Ми рекомендуємо виокремлювати за цією ознакою види ефективності за бізнес-процесами верхнього рівня, зокрема:

– економічна ефективність основних бізнес-процесів, яку варто розуміти як міру ефекту від реалізації основного процесу щодо витрат на їх забезпечення (за аналогією можна трактувати економічну ефективність інших видів бізнес-процесів);

– економічна ефективність допоміжних (обслуговуючих) бізнес-процесів;

– економічна ефективність бізнес-процесів управління.

Видова класифікація за цією ознакою може суттєво деталізуватись за видами бізнес-процесів різних рівнів.

Варто зазначити, що економічна ефективність бізнес-процесів управління тісно пов’язана з поняттям економічної ефективності управління підприємством. Проте їх не можна вважати тотожними з огляду на складність і багатогранність самого поняття «управління».

Значна кількість науковців вважають за доцільне класифікувати види ефективності за умовами оцінювання, виокремлюючи реальну, розрахункову та умовну ефективність. Так, реальною ефективністю вважають фактичний рівень витрат та результатів за даними бухгалтерського обліку та звітності. Розрахункова – базується на проєктних або планових показниках, отриманих розрахунковим шляхом. Умовна ефективність використовується для оцінювання роботи структурних підрозділів підприємства [2].

Поширеною в літературі класифікаційною ознакою є поділ економічної ефективності за рівнями оцінювання. Якщо розглядати цей критерій поділу виключно на мікрорівні, то можна виділити економічну ефективність підприємства в цілому; економічну ефективність окремої бізнес-одиниці; економічну ефективність окремого структурного підрозділу [1, 2, 4, 5].

Окремі дослідники класифікують економічну ефективність за ступенем збільшення ефекту, пропонуючи розрізняти первісну та мультиплікаційну ефективність, пояснюючи необхідність такого поділу видів ефективності тим, що в результаті здійснення тих чи інших заходів може спостерігатися як одноразовий ефект, так і мультиплікаційний. Про мультиплікаційний ефект може йтися тоді, коли початковий ефект повторюється й примножується на різних рівнях цього підприємства, а також поширюється на інші підприємства та організації [1, 2, 4, 5].

Також у наявних наукових підходах зустрічається класифікація економічної ефективності за метою визначення, в межах якої розрізняють абсолютну та порівняльну ефективність. Абсолютна ефективність характеризує загальну або питому (в розрахунку на одиницю витрат чи ресурсів) її величину, яку отримує підприємство в результаті своєї діяльності за певний проміжок часу. Натомість порівняльна ефективність визначається шляхом порівняння можливих варіантів господарювання і вибору кращого з них, а її рівень показує переваги певного варіанта реалізації господарських рішень (напряму діяльності) порівняно з іншими варіантами [1, 2, 4].

Інакше пропонує класифікувати економічну ефективність Архіпов Н. М. – за стейкголдерами, виокремлюючи ефективність для власників, для кредиторів, для постачальників, для персоналу тощо [5]. Погоджуємося з доцільністю такого підходу, особливо в умовах актуальності запровадження стейкхолдерського підходу в практику корпоративного управління, який вважають умовою стійкого зростання. Також він пропонує класифікувати економічну ефективність за обраними критеріями оцінювання, поділяючи на максимальну, мінімальну та цільову (оптимальну) [5]. Зазначений підхід вважаємо доречним, він є важливою характеристикою в тому числі результату управлінської діяльності.

До зазначених вище ми пропонуємо додати класифікацію економічної ефективності за досягнутим рівнем та виокремлювати низьку, середню та високу економічну ефективність. Так, низька ефективність характеризується показниками ефективності на рівні нижчому за середньогалузевий; середня економічна ефективність – відповідає середньоринковим оцінкам, а висока – перевищує рівень середньоринкових показників. Зазначені види важливі для розуміння місця підприємства у конкурентному середовищі та розробленні заходів щодо підвищення його конкурентоспроможності.

Також, на нашу думку, доречно додати поділ економічної ефективності залежно від основних факторів-акселераторів, що її формують. За цією ознакою пропонуємо виокремлювати економічну ефективність, що формується переважно завдяки сприятливим можливостям зовнішнього середовища (як-от кон'юнктури товарного ринку, фінансового ринку тощо) та економічну ефективність, що формується переважно завдяки внутрішнім зусиллям підприємства. Остання характеризується зростанням її індикаторів за рахунок запровадження різноманітних управлінських, технологічних, товарних, продуктових інновацій тощо.

Отже, узагальнюючи наявні підходи, можна таким чином представити класифікацію видів економічної ефективності підприємства (табл. 1.8).

Таблиця 1.8

Види економічної ефективності підприємства

Класифікаційна ознака	Види ефективності
характер здійснюваних витрат	ресурсна, витратна
вид діяльності	операційна; інвестиційна; фінансова
вид бізнес-процесу (БП)	основний; допоміжний; обслуговуючий
рівень оцінювання	підприємства; бізнес-одиниці; структурного підрозділу
ступінь збільшення ефекту	первісна, мультиплікаційна
мета визначення	абсолютна; порівняльна
стейкголдер	власників; кредиторів; персоналу; постачальників; клієнтів
умови оцінювання	реальна, потенційна, розрахункова
критерій оцінювання	максимальна; мінімальна; цільова (оптимальна)
досягнутий рівень*	низький; середній; високий
основний фактор-акселератор формування*	досягнута за рахунок сприятливого зовнішнього середовища; за рахунок спрямованих управлінських дій

** Запропоновано автором*

Джерело: узагальнено та розвинено за [1–5]

Зазначена класифікація демонструє комплексність поняття «економічна ефективність», віддзеркалює її окремі аспекти та становить підґрунтя для дослідження сутності та видів економічної ефективності управління підприємством.

Ефективність управління підприємством давно перебуває в полі зору науковців, адже завжди актуальним лишається питання для власників, чи ефективно менеджмент компанії здійснює управління, для топменеджерів – чи ефективно здійснюють свої функції менеджери нижчих ланок, якими будуть фінансові результати діяльності та показники ефективності його функціонування, якщо підвищити рівень якості менеджменту?

Незважаючи на значну кількість публікацій, присвячених дослідженню цієї проблематики, на цей час немає одностайних підходів як до визначення змісту «економічної

ефективності управління», так і виокремлення її видів. Разом із тим збільшилася неоднозначність визначення ефективності управління та урізноманітнилися показники її оцінювання.

На сьогодні в науковій літературі простежується декілька підходів до розуміння та оцінювання економічної ефективності управління.

Так, перший підхід фактично ототожнює поняття ефективності функціонування підприємства та ефективності управління підприємством, посилаючись на суттєву залежність результатів діяльності підприємства від якості управлінських рішень [6].

Другий підхід трактує ефективність управління як відносну міру результативності управлінських витрат (витрат на управління) [7]. Зазначений підхід є дещо вужчим за попередній, але, на нашу думку, більш об'єктивно відображає зміст цього поняття, оскільки спрямований на розмежування термінів «ефективність функціонування підприємства» та «ефективність управління підприємством».

Третій підхід припускає, що ефективність управління потрібно розглядати як результативність діяльності конкретної системи управління, що відображається в різних показниках як стану об'єкта управління, так і власне управлінської діяльності. Саме ефективність управління розглядається як результативність діяльності конкретної системи управління, яка характеризується показниками, що належать до об'єкта управління у вигляді техніко-економічних результатів виробництва та до суб'єкта управління – це фінансові витрати на утримання керуючої системи, затрати часу на виконання певних операцій і всього процесу управління [8].

Четвертий підхід тлумачить ефективність управління як ступінь досягнення цілей управління діяльністю підприємства [8]. Погоджуючись з тим, що досягнення цілей є важливим завданням системи управління підприємством, вбачаємо, що зазначене трактування є ближчим до поняття «результативність управління», адже економічна ефектив-

ність передбачає розуміння того, наскільки витратним було досягнення цілей.

П’ятий підхід трактує ефективність управління як ефективність управлінських рішень, а тому її оцінювання має базуватися на чіткому визначенні цілей і виборі критеріїв. Так, за наявності кількох цілей Л. М. Христенко рекомендує привести різні цілі до єдиної оцінки та визначити ефективність кожного рішення за всіма цілями, обираючи при цьому найбільш ефективний варіант [9].

Шостий підхід інтерпретує ефективність управління як ефективність управлінської праці. Погоджуємося з думкою Р. З. Вечерковськи, що це поняття є більш вузьким, тому що охоплює тільки економію живої й упредметненої праці у сфері управління матеріальним виробництвом за рахунок оптимізації та раціоналізації управлінської діяльності [7].

Сьомий підхід розглядає економічну ефективність управління крізь призму відносної ефективності заходів та вдосконалення управління [8]. На нашу думку, визначення ефективності заходів щодо вдосконалення управління є важливим аспектом комплексної оцінки ефективності управління, але повною мірою не розкриває комплексності поняття «економічна ефективність управління підприємством».

Наявність такої значної кількості трактувань поняття «економічна ефективність управління підприємством» насамперед демонструє його комплексність та складність, що обумовлюється складністю самого поняття «управління підприємством». Не випадково вивченню його змісту й методологічних засад формування присвячено значний науковий доробок [1–8].

У сучасних дослідженнях описано різні аспекти цього поняття, зокрема:

1. Управління як мистецтво застосовувати накопичений досвід на практиці, спираючись на концепції, теорії, принципи, форми і методи, що лежать в його основі, для того, щоб члени колективу спрямовували свої зусилля на досягнення її цілей в умовах найбільш повного розкриття потенціалу колективу [10].

2. Управління як наука, яка має свій предмет вивчення, специфічні проблеми і підходи до їх вирішення. Зусилля науки спрямовані на пояснення природи управлінської праці, встановлення зв'язку між причиною і наслідком, виявлення факторів і умов, при яких спільна праця людей стає більш ефективним і корисним. Наука управління має свою теорію, змістом якої є закони і закономірності, принципи та функції, форми і методи цілеспрямованої діяльності людей у процесі управління [10].

3. Управління як процес, що відображає прагнення інтегрувати всі види діяльності за рішенням управлінських проблем в єдиний ланцюг. Управління при цьому представляється як пов'язані між собою управлінські функції, що динамічно змінюються у просторі та часі, метою яких є вирішення проблем і завдань навчального закладу [10].

4. Управління як функція, яка реалізується шляхом виконання ряду управлінських дій (функцій управління) – планування, організація, розпорядження, координування, контроль, мотивація, керування, комунікації, дослідження, оцінки, прийняття рішень, підбір кваліфікованих фахівців, представництво, ведення переговорів, укладання угод на освітні послуги [10].

5. Управління як вид практичної діяльності [11], який потребує спеціальної підготовки, набуття певних знань та компетентностей і передбачає виконання усіляких рутинних дій.

6. Управління як орган чи апарат [11], який формується з певних організаційних структур, персоналу, який займається управлінською діяльністю.

7. Управління як соціальний інститут сучасного суспільства, існування якого ґрунтується на людській взаємодії, комунікації та кооперації й спрямоване на задоволення важливих суспільних запитів [11]. Особливо ця функція управління посилюється в умовах відділення інституту власності від інституту управління.

Крім багатоаспектностні поняття управління підприємством, виокремлюють також різні підходи до його здійснення. Найбільш поширеними з них є ситуаційний, функціональний, системний та процесний.

Ситуаційний підхід – спосіб мислення стосовно організації, що розглядає конкретні ситуації, а саме: виділення факторів, що створили певну ситуацію і є найбільш впливовими, визначення недоліків і переваг, обмежень і наслідків ситуації, обрання специфічних прийомів і методів управління для конкретної ситуації. Використання цього підходу щодо управління сприяє більш ефективному досягненню мети, особливо на великих підприємствах із великою кількістю поставлених до вирішення завдань [12].

Таким чином, ситуаційний підхід – це застосування методів адаптації на зміну факторів внутрішнього та зовнішнього середовищ. В умовах високого рівня флуктуацій зовнішнього середовища ситуаційний підхід може бути досить ефективним за умови високої кваліфікації менеджерів та достатнього рівня децентралізації системи управління.

Ситуаційний підхід орієнтує менеджерів на використання можливостей прямого застосування науки до конкретних ситуацій та умов. Центральним моментом ситуаційного підходу є ситуація, тобто конкретний набір обставин, які впливають на підприємство в конкретний період часу. Через те, що в центрі уваги опиняється ситуація, ситуаційний підхід підкреслює значущість «ситуаційного мислення» [10].

Функціональний підхід до управління підприємством ґрунтується на вертикальній ієрархічній структурі, за якої окремі організаційні одиниці (підрозділи, цехи, відділи, департаменти тощо) виокремлюються за ознакою виконання ними певної функції: чим більшою є кількість та складність виконуваних на підприємстві завдань, тим більше рівнів та складових матиме його ієрархічна структура. За функціонального підходу управління підприємством здійснюється як єдиним цілим за допомогою розпоряджень, наказів та дозволів, при цьому чим вищим є рівень управління, тим відповідальніші рішення на ньому приймаються. Відповідно на нижні рівні ієрархії делегуються лише повноваження щодо прийняття найменш значущих рішень. Кожен структурний підрозділ за такої системи управління функціонує відокремлено, автономно від інших; рівень взаємодії між підрозділами визначається поділом праці та обміном матеріальними продуктами [13].

Процесний підхід, на відміну від попередніх, орієнтується насамперед на управління процесом створення цінності для споживача.

Процесний підхід веде до спрощення багаторівневих ієрархічних організаційних структур, що забезпечує більшу орієнтацію організації на споживача. За рахунок скорочення ієрархічних рівнів організаційної структури процесний підхід дозволяє спростити обмін інформацією між різними підрозділами. Перехід до процесного підходу дає змогу усунути відособленість підрозділів і посадових осіб, розглядати діяльність у системі менеджменту якості не в статиці, а в динаміці, коли діяльність в системі має постійно поліпшуватися на основі відповідних вимірювань і аналізу, акцентувати увагу менеджменту на взаємодії підрозділів і посадових осіб, що дає можливість усувати «нічийні поля», тобто ділянки діяльності, що випадають з-під впливу системи менеджменту якості [10].

Системний підхід, який розглядає підприємство як систему, елементи якої взаємозв’язані між собою, що дозволяє ефективно управляти всією системою на основі налагодженої роботи кожного з компонентів. Системний підхід в управлінні базується на загальній теорії систем [12].

Системний підхід у теорії менеджменту визначає організацію як сукупність взаємопов’язаних елементів, які орієнтовані на досягнення єдиної кінцевої мети в умовах зовнішнього середовища, що змінюється, і до яких відносять спільні цінності, стратегічну орієнтацію, структуру, стиль управління, склад співробітників, сукупність теоретичних знань та практичного досвіду. Сутність системного підходу до управління полягає в такому: формулювання цілей та встановлення їхньої ієрархії до початку будь-якої діяльності, пов’язаної з управлінням; отримання максимального ефекту, тобто досягнення поставлених цілей шляхом порівняльного аналізу альтернативних шляхів та методів досягнення цілей і здійснення вибору; кількісна оцінка цілей та засоби їх досягнення, заснована на всебічній оцінці всіх можливих і планованих результатів діяльності [14].

Отже, в найбільш узагальненому вигляді з позицій системного підходу управління підприємством розуміють як сукупність взаємопов'язаних і взаємозалежних частин – компонентів (підсистем): наукових знань і практичних навичок щодо керування різними об'єктами (людиною, процесом, організацією) для забезпечення їх конкурентоспроможності в ринкових умовах і всебічного задоволення потреб при оптимальному використанні ресурсів [15]. Системний підхід є найбільш комплексним, по суті об'єднує всі аспекти управління, які виокремлюються в інших підходах.

На підставі зазначених аспектів управління як явища та підходів до його здійснення його можна описати таким чином (рис. 1.15).

Рис. 1.15. Характеристики управління підприємством

Джерело: складено автором

Так, управління підприємством ґрунтується на певній організаційній структурі, яка передбачає виокремлення функціональних підрозділів. Раціональність цієї структури, її відповідність особливостям підприємства, стану зовнішнього середовища є важливим чинником ефективності рішень, рівня управлінських витрат тощо. Тому сукупність таких підрозділів є важливою характеристикою управління підприємством.

Водночас управління – це послідовний процес реалізації окремих функцій: обліку, планування, стимулювання, координації, контролю. Раціональність їх організації є важливою детермінантою як ефективності функціонування підприємства в цілому, так і управління зокрема.

Організаційна структура підприємства – це не лише сукупність підрозділів, а й персоналу, який працює в них. Таким чином, управління можна охарактеризувати як сукупність управлінського персоналу різних ланок: вищої, середньої, нижчої.

З огляду на те, що результатом управлінської діяльності є управлінське рішення, управління можна розглядати як сукупність таких рішень як ситуативних, так і заздалегідь сформованих з різною відповідністю часовому горизонту: стратегічних, тактичних, оперативних.

З розвитком та популяризацією системи контролінгу поширеним явищем стало виокремлення на підприємствах центрів відповідальності, які можуть певним чином «накладатися» на функціональну структуру підприємства, тому управління можна також характеризувати як сукупність центрів відповідальності. Зазвичай дослідники виокремлюють центри доходів, витрат, прибутку, розвитку. Ми пропонуємо додати до цього переліку центр безпеки, зважаючи на постійне збільшення загроз інтересам підприємства, високий рівень флуктуацій зовнішнього середовища.

Таким чином, виходячи з позицій системного підходу, **економічну ефективність управління підприємством можна розглядати як інтегровану характеристику ефективності (міри отриманого ефекту до ресурсів / понесених витрат) функціонування всіх його підсистем: функціональних підрозділів, центрів відповідальності, процесів, управлінських рішень, управлінського персоналу, яка суттєво детермінує ефективність функціонування підприємства.**

З огляду на зазначене можна виокремити такі види економічної ефективності управління підприємством: **ефективність структурних підрозділів управління; ефективність процесів управління; ефективність центрів відповідальності; ефективність управлінського персоналу; ефективність управлінських рішень** та деталізувати їх (табл. 1.9).

Таблиця 1.9

Класифікація видів економічної ефективності управління підприємством

Класифікаційна ознака	Види економічної ефективності
За структурними підрозділами	– відділу постачання; – відділу маркетингу; – комерційного відділу; – виробничого відділу; – фінансового відділу; – юридичного відділу та ін.
За процесами	– обліку; – ЕЕ планування; – координації; – мотивації; – контролю
За центрами фінансової відповідальності	– центру витрат; – центру доходів; – центру прибутку; – центру розвитку; – центру безпеки
За управлінськими рішеннями	– стратегічних управлінських рішень; – тактичних управлінських рішень; – ЕЕ оперативних управлінських рішень
За категоріями управлінського персоналу	– вищої ланки управління; – середньої ланки управління; – нижчої ланки управління
За метою визначення	– абсолютна; – порівняльна
За досягнутим рівнем	– висока – середня; – низька

Джерело: складено автором

Окрім зазначених вище видів економічної ефективності управління підприємством за його елементами пропонуємо додати ще види ефективності за метою визначення та досягнутим рівнем, які пропонувались у видовій класифікації

економічної ефективності функціонування підприємства, адже саме ці види ефективності дозволяють, з одного боку, ідентифікувати достатність зусиль у вдосконаленні системи управління та з іншого – здійснювати їх порівняльне оцінювання.

Також окремі види ефективності можна деталізувати на більш локальні (прості) види. Зокрема, економічну ефективність окремих структурних підрозділів можна класифікувати за видами ефективності окремих функціональних завдань, що розв'язуються управлінським персоналом у межах кожного з них.

Зважаючи на обрану тему наукового дослідження, пропонуємо таку деталізацію видів економічної ефективності, що може виокремлюватися в межах діяльності служби безпеки (рис. 1.10).

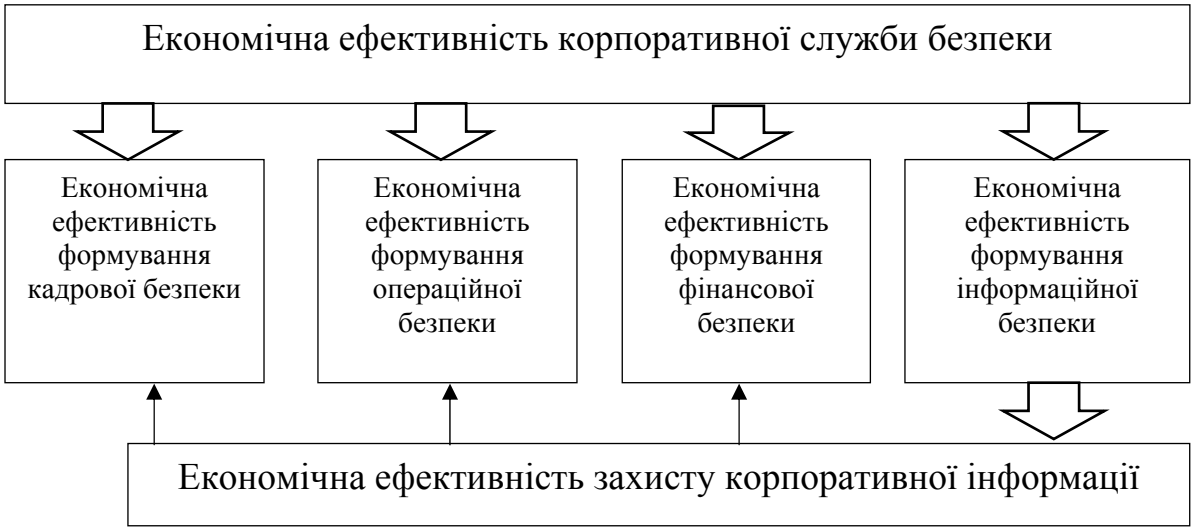


Рис. 1.10. Види економічної ефективності корпоративної служби безпеки

Джерело: складено автором

Так, на основі логічного зв'язку між захистом корпоративної інформації та формуванням інформаційної безпеки, її впливу на досягнення та збереження економічної безпеки (що розглянуто в п. 1.3), можна констатувати особливе місце економічної ефективності захисту корпоративної інформації у формуванні економічної ефективності інформаційної безпеки та її інших видів, які повинні забезпечуватись корпоративною службою безпеки, що суттєво впливає на ефективність формування

кадрової, операційної, фінансової безпеки, адже в корпоративному інформаційному просторі зберігається та передається інформація з різних предметних сфер.

На сьогодні у спеціалізованій літературі відсутнє визначення поняття «економічна ефективність захисту корпоративної інформації». Виходячи з нашого розуміння змісту понять «захист корпоративної інформації» (що розкривається у п. 1.3) та «економічна ефективність управління підприємством» пропонуємо таке його тлумачення.

Економічна ефективність захисту корпоративної інформації – це міра економічного ефекту витрачених ресурсів на реалізацію системи заходів з ідентифікації, аналізу, нейтралізації загроз порушення функціонування корпоративного інформаційного поля та запобігання їм.

З огляду на це економічна ефективність захисту корпоративної інформації зводиться до визначення основних параметрів: економічного ефекту та витрат.

В умовах цифровізації економіки основний акцент у захисті корпоративної інформації зміщується саме на цифровий контент, бо саме він є найбільш вразливим для сучасних загроз.

Відповідно до загальноприйнятої точки зору, характерною для більшості фахівців у сфері інформаційної безпеки (далі – ІБ), сформувалася думка, що інвестування в ІБ та її концепція для конкретного об’єкта інформатизації (далі – ОБІ) будуть ефективними, якщо забезпечити виконання вимог державних нормативних документів і стандартів. Така думка виникла на основі єдиної загальновизнаної методики оцінки економічного ефекту від інвестування в ІБ ОБІ [16, 17]. Зауважимо, що в цьому контексті проблематики оцінювання ефективності інвестування в ІБ ОБІ розуміється перевищення вартісної оцінки кінцевого результату відповідних заходів над сумарними розмірами інвестицій, тобто сукупними витратами фінансових ресурсів на ІБ ОБІ в перебігу фіксованого періоду часу [18].

Складність оцінювання реального ефекту від інвестування в захист корпоративної інформації (далі – ЗКІ) обумовлюється досить великим переліком специфічних для сектора захисту інформації та кібернетичної безпеки чинників. Загалом відзначимо лише істотний вплив на ефективність інвестування в ЗКІ таких факторів як 1) постійно мінливий контекст кіберзагроз; 2) різноваріантність стратегії і тактики атакуючої сторони (комп'ютерних зловмисників); 3) швидкий розвиток технічних засобів ЗКІ і кібербезпеки (далі – КБ) та ін. У свою чергу, відповідно до базових постулатів теорії оцінки ефективності систем відомо, що якість засобів ЗКІ (далі – ЗЗКІ), може проявлятися лише під час реального цільового застосування на об'єкт інформатизації. Саме ця обставина дає можливість об'єктивно оцінювати ефективність їх застосування, а отже, і результативність інвестицій в ЗЗКІ на ОБІ [19, 20].

Додаткова складність при оцінюванні ефективності інвестування в ЗКІ ОБІ пов'язана з невизначеністю результатів функціонування засобів ЗКІ. На етапі проєктування ЗЗКІ фактори невизначеності. Наприклад, пов'язані з тим, що може скластися така ситуація, за якої сторона захисту ОБІ витратить сотні тисяч грошових одиниць або навіть мільйони на захист від складних спрямованих кібератак, а атакуючій стороні часто досить вдатися до невеликих за витратами методів соціальної інженерії («інвестицій в кібератаку»). Така тактика застосування методів соціальної інженерії в деяких випадках допомагала обходити найсучасніші ЗЗКІ [21]. Таким чином, під час реалізації проєктів у сфері ЗКІ рівень функціональності ЗЗКІ може знизитися. Отже, з точки зору методології моделювання ефективності інвестування в ЗКІ ряд функціональних метрик ЗЗКІ не може бути тотожним виражений і описаний детермінованими показниками.

Зауважимо, що в ході багатокритеріальної оптимізації ЗЗІ також виконується оцінювання рівня гарантій ІБ залежно від особливостей ОБІ (наприклад, банк, промислове підприємство, сфера торгівлі або освіти та ін.). Цей рівень досить значною мірою залежить від розміру потенційного запобі-

гання шкоді для інформаційних масивів ОБІ. У такому разі, виникає нове завдання, пов'язане з отриманням чисельної оцінки ризику для ОБІ. Тобто стороні захисту необхідно володіти уявленням про розподіл випадкових величин збитку в разі атаки. У такій ситуації традиційно застосовують методи імітаційного моделювання. Як альтернативний підхід також використовують результати активного аудиту інформаційної безпеки (або ЗЗКІ) для аналізованого ОБІ.

Справжня вартість захисту корпоративної інформації складається з витрат на запобігання кібератакам (програмне забезпечення; навчання цифровій грамотності працівників; на організацію системи безпеки, мотиваційної політики та корпоративної культури) і на ліквідацію наслідків від кібератак (викуп, відновлення операційних процесів, репутації).

Втрати підприємства у разі успішної кібератаки:

1. По-перше, це грошові втрати, пов'язані з уповільненням темпів зростання виручки від реалізації і, як наслідок, недоотримання доходів і прибутку у найближчій та середньостроковій перспективі.

2. По-друге, якщо кібератака зловмисників мала успіх, то найчастіше це призводить до втрати репутації. Найбільш критично це для відомих брендів, які мають певну репутацію, яка створювалася роками, їм довіряють клієнти і працівники. При порушені ж ІБ конфіденційні дані потрапляють до зловмисників, що руйнує довіру. І навіть швидка реакція з боку компанії – своєчасний викуп або дешифрування даних, стрімке відновлення основних процесів – не повертає клієнтам комфорту і відчуття впевненості. Втрата довіри призводить до скорочення обсягів покупок в очікуванні розвитку подій, часткової втрати постійних клієнтів, стає значною перешкодою для залучення нових. Це, в свою чергу, веде до зниження конкурентоспроможності підприємства.

3. По-третє, незалежно від того, яке рішення приймають керівники компаній – задоволення вимог зловмисників або самостійне вирішення проблем – ці процеси супроводжуються втратою часу, який є дедалі ціннішим ресурсом будь-якого

бізнесу в умовах прискорення розвитку інформаційного суспільства. Відволікання грошових коштів, втрата фінансових можливостей, як наслідок – втрата мобільності при змінному попиті суттєво знижують конкурентні можливості підприємства.

4. По-четверте, викрадення бази даних зловмисниками може бути пов'язане не тільки з особистими даними клієнтів, а й з конфіденційною інформацією підприємства. Оприлюднення цих даних спричинить втрату конкурентних переваг компанії. Конфіденційна інформація контрагентів також опиняється під загрозою оприлюднення, що, в свою чергу, призведе до штрафів, санкцій, судових витрат.

5. По-п'яте, викрадення, шифрування даних призводить до порушення бізнес-процесів підприємства. Але не менш важливим є втручання і пошкодження в закупівельні, збутові та інші бази за видами діяльності підприємства, що може супроводжуватися іншою формою кіберзагрози, наприклад, вірусною атакою. Тимчасова втрата доступу до платіжної системи банку, бухгалтерських, кур'єрських програм та іншого зумовлює тимчасову дезорієнтацію та уповільнення основних бізнес-процесів, а відтак – зниження обсягу виручки від реалізації та інших ключових показників діяльності підприємства.

6. По-шосте, стосунки з інвесторами. Як правило, великі підприємства, особливо міжнародного рівня, при ліквідації наслідків кібератаки не втрачають своїх інвесторів або акціонерів – це пов'язано з достатньою кількістю фінансових ресурсів і наявністю потужної системи інформаційної безпеки. Але якщо йдеться про середні підприємства, в яких недосконала система безпеки і які потребують додаткових вкладень з боку інвесторів (акціонерів) для подальшого розвитку, то після успішної кібератаки є висока ймовірність втрати довіри інвестора (акціонера) такими підприємствами та/або обмеження можливостей залучення інших інвесторів (акціонерів) для подальшого розвитку.

Економічний ефект захисту корпоративної інформації сучасні автори розраховують через темп зміни доходу (прибутку), відвернений збиток. Розрахунок обох показників є складним.

Методику розрахунку темпів зміни доходу (прибутку) можна поділити на 2 підходи шляхом обчислення: по-перше, приросту доходу (прибутку); по-друге, недоотриманої суми доходу (прибутку).

Розрахунок приросту доходу (прибутку) залежить від наявності достатнього рівня інформаційної безпеки і ускладнений тим, що фактично система ІБ є не центром формування прибутку, а допоміжною в загальній системі підприємства. Крім того, достатній (належний) рівень як критерій ІБ підприємства потребує своєї системи оцінки. Розрахунок недоотриманої суми доходу (прибутку) можна здійснювати через імовірність настання кібератаки або як результат фактичної кібератаки. Перший ускладнений тим, що кібератаки не мають певної системи. Фактичні додаткові витрати підприємства для викупу інформації, відновлення бізнес-процесів після кібератаки і порівняння фактичних значень доходу (прибутку) із запланованими є основними показниками для розрахунку економічної ефективності у випадку успішної кібератаки.

Методика розрахунку економічного ефекту внаслідок відверненого збитку передбачає аналіз всіх інформаційних загроз, яким піддавалося підприємство протягом певного часу, де враховується можлива вартість викупу на відновлення бізнес-процесів. У цьому разі економічна ефективність розраховується як співставлення суми відверненого збитку з витратами підприємства на організацію належного рівня ІБ.

Можливості сучасних методик, які використовуються для оцінки економічної ефективності, представлено у табл. 1.10, дані якої відображають можливість кожного з методів визначати складові економічної ефективності захисту корпоративної інформації.

Таблиця 1.10

Методики оцінки економічної ефективності захисту корпоративної інформації

Назва методики	Оптимізація витрат	Визначення результату	Максимізація результату	Оцінка ризиків	Розроблення ймовірних сценаріїв
Прикладний інформаційний аналіз (*Applied Information Economics, AIE*)	+	+	–	+	+
Споживчий індекс (*Customer Index, CI*)	–	+	–	–	–
Додана економічна вартість (*Economic Value Added, EVA*)	–	+	–	–	–
Вихідна економічна вартість (*Economic Value Sourced, EVS*)	–	+	+	+	+
Управління портфелем активів (*Portfolio Management, PM*)	+	+	+	+	+
Оцінка дійсних можливостей (*Real Option Valuation, ROV*)	+	+	+	+	+
Метод життєвого циклу штучних систем (*System Life Cycle Analysis, SLCA*)	–	+	–	+	+
Система збалансованих показників (*Balanced Scorecard, BSC*)	+	+	+	–	–
Сукупна вартість володіння (*Total Cost of Ownership, TCO*)	+	–	–	–	–
Функціонально-вартісний аналіз (*Activity Based Costing, ABC*)	+	–	–	–	+
Метод експертних оцінок	–	+	–	+	–
Метод дисконтованого грошового потоку (*DCF*)	+	+	+	+/–	+/–
Метод індексу дохідності (*PI)*	–	+	+	–	-
Метод чистої приведеної вартості (*NPV*)	+	+	+	+/–	+
Метод імітаційного моделювання	-	+	+	+	+
Метод генетичних алгоритмів	+	+	+	+	+

Джерело: систематизовано автором за [16–24]

З огляду на сутність економічної ефективності передусім необхідно звернути увагу на методики, які дозволяють оптимізувати (мінімізувати) витрати на ІБ. *AIE* передбачає оцінку ефективності інвестицій у технології безпеки з використанням експортних оцінок якісних показників. У цьому разі важливу роль відіграють особисті якості експертів (знання, досвід).

Використання *AIE* доволі складне і потребує звернення до компанії-консультанта. Застосування методики *PM* дає змогу оптимізувати витрати у режимі реального часу, але оцінка і прийняття рішень покладені на керівника і залежать від його особистих якостей. Метод *ROV* є трудомісткім і обмеженим у використанні, застосовується на стадії проєктування. Застосування *BSC* передбачає розроблення унікальних критеріїв: в залежності від стратегії підприємства, показників оцінки задаються планові значення показників. Через те, що ІБ є допоміжною системою, виникає чимало проблем у побудові збалансованої моделі. Стратегічні показники підприємства, пов’язані з основною діяльністю, необхідно узгодити з показниками інформаційної безпеки. *ABC*-метод є орієнтованим на виробничу і логістичну систему підприємства й співвідноситься з визначенням і розподілом витрат.

Аналіз можливостей розглянутих методів визначення розміру витрат і результату, оцінки економічної ефективності дає змогу зробити такі висновки:

– застосування деяких методів є неможливим для малих підприємств, що пов’язано з їх значною трудомісткістю, відсутністю експертів тощо;

– метод *Customer Index* найповніше відображає специфіку діяльності підприємств торгівлі і дає можливість оцінити вплив інвестицій в ІБ на динаміку кількості споживачів;

– використання методу *Total Cost of Ownership* надає найбільше можливостей для аналізу і мінімізації витрат на підприємстві, але для визначення результату необхідно застосовувати принаймні ще одну методику;

– метод *DCF* ґрунтується на комплексному підході при оцінюванні інвестиційних витрат, враховує всі етапи життєвого циклу компонентів ЗЗКІ та бізнес-процесів компанії. Проте в моделі складно врахувати всі ризики порушення інформаційної безпеки;

– модель *PI* максимально узгоджена з типовими показниками та формами бухгалтерського обліку, характеризується простотою, але суттєво обмежена щодо оцінювання ризиків;

– методика *NPV* орієнтована на врахування інтересів інвесторів, повною мірою дає змогу оцінювати витрати та ефект;

– методи імітаційного моделювання та генетичного алгоритму максимально гнучкі та спрямовані на врахування ризиків при визначенні витрат та ефекту, вони базуються на аналізі даних попередніх періодів (сталого розвитку) і під впливом пандемії *COVID-19* та пов'язаних з цим карантинних обмежень, тож прогнозні дані виявилися помилковими.

Таким чином, очевидною є неусталеність методологічних засад та підходів до оцінювання економічної ефективності захисту корпоративної інформації в системі інформаційної безпеки, обмеженість окремих методик, що обумовлюється насамперед складністю досліджуваної проблематики.

Проте важливість збереження інформаційної безпеки в умовах розвитку інформаційної економіки та її стрімкої цифровізації потребує обґрунтування концептуальних засад її формування на підприємстві, методологічних засад забезпечення ефективності функціонування та систематизації показників оцінювання її економічної ефективності, що і буде предметом розгляду наступного розділу дослідження.

Список бібліографічних посилань

1. Лобов С. П. Сучасні концепції економічної ефективності діяльності та ефективності управління підприємством. *Ефективна економіка*. № 4. 2015. URL : http://www.economy.nayka.com.ua/?op=1&z=4011 (дата звернення: 15.06.2022).

2. Братанич М. В., Полозова Т. В. Визначення сутності економічної ефективності та класифікація її видів. *Економіка промисловості*. 2010. № 4. С. 153–155. URL : http://nbuv.gov.ua/UJRN/econpr_2010_4_26 (дата звернення: 15.06.2022).

3. Говорушко Т. А. Ефективність як економічна категорія // Наукові праці НУХТ. 2007. № 20. С. 74–76.

4. Економіка підприємства : підручник / за заг. ред. С. Ф. Покропивного. 2-ге вид., перероб. та допов. Київ : КНЕУ, 2005. 528 с.

5. Архіпов Н. М. Види ефективності операційної діяльності підприємства торгівлі // Науковий вісник Ужгородського національного ун-ту. Серія «Міжнародні економічні відносини та світове господарство». Вип. 18. Ч. 1. 2018. С. 21–25.

6. Синицына Т. А. Оценка эффективности системы управления промышленным предприятием: целевой подход : дис. ... канд. екон. наук : спец. 08.06.01 «Экономика, организация и управление предприятиями». Одеса : ОДЕУ, 2004. 187 с.

7. Вечерковски Р. З. Управление знаниями при формировании конкурентных преимуществ предприятия : дис. ... канд. экон. наук : спец. 08.06.01 «Экономика, организация и управление предприятиями». Луганск : ВНУ им. В. Даля, 2004. 216 с.

8. Щеглова О. Ю., Судакова О. І., Лаже М. В. Ефективність управління підприємством та підходи до її визначення // Науковий вісник Ужгородського національного ун-ту. Вип. 12. Ч. 2. 2017. С. 186–189.

9. Христенко Л. М. Удосконалення оцінки управління ефективністю підприємства : дис. ... канд. екон. наук : спец. 08.06.04 «Економіка та управління підприємствами (підприємства машинобудівної та металургійної галузей)». Луганськ : ВНУ ім. В. Даля, 2007. 192 с.

10. Кононова І. В. Аналіз підходів до управління підприємством у сучасних умовах. *Прометей*. № 1 (40). 2013. С. 146–151.

11. Поканевич Ю. В. Управління як складна багатовимірна категорія // Вісник ЖДТУ. № 1 (47). 2009. URL : http:// nbuv.gov.ua/portal/Soc_gum/Vzhdtu_econ/2009?1/44.pdf (дата звернення: 15.06.2022).

12. Харченко В. А. Системний підхід до стратегічного управління підприємством // Економічний вісник Донбасу. 2013. № 1. С. 157–160.

13. Порівняльний аналіз можливості застосування функціонального та процесного підходів до управління установою / Б. Й. Семон, В. Л. Шевченко, І. В. Подобєдов, Я. О. Радченко. URL : http://nbuv.gov.ua/portal/soc_gum/Znpcvsd/2009_1/1.pdf (дата звернення: 15.06.2022).

14. Дідур К. М. Системний підхід до управління підприємством та персоналом підприємства. *Ефективна економіка*. 2012. № 4. URL : http://www.economy.nayka.com.ua/?op=1&z= 1079 (дата звернення: 15.06.2022).

15. Устенко А. О. Система управління підприємством // Вісник Прикарпатського ун-ту. Економіка. Випуск X. 2014. С. 96–103.

16. Pieters W., Probst C. W., Lukszo Z. & Montoya L. Cost-effectiveness of security measures: A model-based framework. In Approaches and processes for managing the economics of information systems // IGI global. 2014. P. 139–156.

17. Brangetto P. & Aubyn M. K.-S. Economic aspects of national cyber security strategies // Economic Aspects of National Cyber Security Strategies: project report. 2015. Annex, 1 (9–16), P. 86.

18. Boiko A., Shendryk V. & Boiko O. Information systems for supply chain management: uncertainties, risks and cyber security // Procedia computer science, 2019. № 149, P. 65–70.

19. Chronopoulos M., Panaousis E. & Grossklags J. An options approach to cybersecurity investment // IEEE Access, 2017. № 6, P. 12175–12186.

20. Hallman R. A., Major M., Romero-Mariona J., Phipps R., Romero E., Slayback S. M. & San Miguel J. M. Determining a Return on Investment for Cybersecurity Technologies in Networked Critical Infrastructures // International Journal of Organizational and Collective Intelligence (IJOCI), 2021. № 11 (2), P. 91–112.

21. Nagurney A. & Shukla S. Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability // European Journal of Operational Research, 2017. № 260 (2), P. 588–600.

22. Frolick M. N., Ariyachandra T. R. Business Performance Management: One Truth // Information Systems Management. 2006. № 23 (1). P. 41–48.

23. An Overview of Applied Information Economics. URL : https://hubbardresearch.com/about/applied-information-economics/ (дата звернення: 16.06.2022).

24. Customer intelligence URL : https://searchcustomerexperience-techtarget-com.translate.goog/definition/customer-intelligence-CI?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=uk&_x_tr_pto= op,sc (дата звернення: 16.06.2022).

Розділ 2

КОРПОРАТИВНА ІНФОРМАЦІЙНА БЕЗПЕКА: ВІД КОНЦЕПЦІЇ ДО ПРАГМАТИЧНОЇ ОЦІНКИ

2.1. Формування корпоративної інформаційної безпеки

Актуальність та нагальна необхідність ефективного захисту корпоративної інформації, що було доведено в попередньому розділі дослідження, потребують запровадження дієвих механізмів та організації процесу такого захисту в межах підприємства. З огляду на це власники та топменеджери повинні володіти відповідною концепцією, тобто певним баченням формування корпоративної інформаційної безпеки.

У найбільш загальному розумінні концепцію визначають як систему поглядів, те чи інше розуміння явищ і процесів; єдиний, визначальний задум [1].

Оскільки концепція, на думку дослідників, істотно відрізняється від теорії не тільки своєю незавершеністю, а й недостатньою верифікованістю, розглядається як сурогатна форма теорії, головне призначення якої полягає в інтеграції певного масиву знання, то єдиного чіткого бачення стосовно структурних елементів концепції не окреслили й до цього часу.

Так, у загальнонауковому плані здебільшого вважається, що концепція містить методологію, методи та принципи [2].

Наприклад, проєкт Концепції інформаційної безпеки України зосереджується на висвітленні мети, основних термінів, правових основ інформаційної безпеки, базового підходу до забезпечення інформаційної безпеки, принципів та основ державної політики в сфері інформаційної безпеки, суб'єктів і механізмів забезпечення інформаційної безпеки, громадського контролю та державно-громадського партнерства в сфері реалізації державної інформаційної політики [3].

Зокрема, відповідно до цього документа, «Концепція інформаційної безпеки України (далі – Концепція) спрямована на створення передумов для розвитку такого потенціалу інформаційної сфери України, за якого забезпечується її випереджальний розвиток, а зовнішні негативні впливи не створюють реальних небезпек національній інформаційній безпеці держави. Ключове завдання системи інформаційної безпеки – забезпечити сталість такого розвитку, не допускаючи негативних впливів з боку сторонніх суб'єктів.

Реалізація на практиці такого підходу до інформаційної безпеки держави може здійснюватися виключно за участі всіх внутрішніх суб'єктів інформаційних відносин та за умов ефективної взаємодії держави з громадянським суспільством, приватним сектором та окремими громадянами в інтересах ефективного розвитку інформаційної сфери і спільного захисту такого розвитку від зовнішніх загроз» [3].

Корпоративний рівень організації захисту інформації, безумовно, має свої особливості, що відповідним чином має позначатись і на концепції корпоративної інформаційної безпеки.

Вагомий внесок у дослідження проблематики інформаційної безпеки зробили такі вітчизняні і зарубіжні науковці: Н. С. Безугла, О. Р. Бойкевич, Т. Г. Васильців, Г. Б. Веретенникова, О. А. Грунін, С. О. Грунін, Я. А. Жаліло, А. В. Іванов, Г. Б. Клейнер, Г. В. Козаченко, Т. Б. Кузенко, В. А. Ліпкан, В. Я. Пригунов, А. С. Соснін, А. Г. Шаваєв, В. В. Шликов, В. І. Ярочкін, В. М. Ячменьова та ін. [4–7]. Аналіз праць зазначених авторів свідчить як про відсутність єдиного підходу до побудови концепції корпоративної інформаційної безпеки зокрема, так і безпеки підприємства загалом, а також єдиного бачення компонентної структури концепції.

Так, М. І. Камлик до логічної структури концепції економічної безпеки сільськогосподарських підприємств включає: роль і завдання, об'єкт, предмет, умови реалізації, заходи та шляхи реалізації, критерії успішності [8].

На нашу думку, такий підхід до структуризації концепції дещо змішує поняття «концепція» та «механізм», включаючи

їх окремі елементи, проте не містить базових компонентів, якими характеризується концепція в класичному загальнонауковому розумінні цього поняття.

На переконання В. Г. Кононовича та М. Ф. Тардаскіна, концепція інформаційної безпеки викладає систему поглядів, основних принципів, розкриває визначальні напрями забезпечення безпеки інформації та інформаційних ресурсів [9]. Вважаємо, що такий підхід є більш строгим з точки зору загальнонаукового трактування терміна «концепція», проте містить певну тавтологію, адже концепція за своєю суттю є системою поглядів. Натомість логічна структура концепції має розкривати те, крізь призму яких структурних елементів транслюються ці погляди. На нашу думку, найкращим чином така трансляція відбувається шляхом окреслення обраних методологічних підходів, які покладаються в основу концепції, що відповідає загальнонауковій трактуванні цього терміну.

З погляду Ю. В. Борсуковського базовими вимогами до структури концепції інформаційної безпеки в умовах гібридних загроз є терміни та визначення, загальні положення, нормативні посилання, опис об'єкта захисту, основні фактори, що впливають на інформаційну безпеку організації, основні принципи забезпечення інформаційної безпеки, організаційна структура служби інформаційної безпеки, організація робіт із захисту інформації, заходи управління інформаційною безпекою, розподіл відповідальності і порядок взаємодії, порядок класифікації інформації, що підлягає захисту, модель порушника безпеки, модель загроз безпеки, вимоги щодо забезпечення інформаційної безпеки ІАСУ, технічні вимоги до суміжних підсистем, відповідальність співробітників за порушення вимог щодо забезпечення інформаційної безпеки, аудит і звітність, механізм реалізації концепції, історія змін [10]. Зазначений підхід характеризується прагматизмом, що є його позитивною рисою, проте деталізація компонентів концепції, на нашу думку, є надмірною та переобтяженою, містить елементи, які не відображають концептуальні положення формування інформаційної безпеки, а відповідають тактичному та оперативному рівням її реалізації.

Аналіз та розвиток наявного доробку дозволив нам визначити сутність концепції формування корпоративної інформаційної безпеки як систему поглядів на організацію та забезпечення такої безпеки, що відображається в обраній методології формування, окреслених принципах та розробленому механізмі забезпечення. Таким чином, концепція формування корпоративної інформаційної безпеки містить три принципові структурні компоненти: методологічну основу, принципи, механізми, які перебувають у логічному зв'язку та підпорядкуванні (рис. 2.1).

Так, на нашу думку, базовим елементом концепції є саме її методологічна основа, яка індивідуалізує концепції корпоративної інформаційної безпеки на різних підприємствах та у наукових дослідженнях. Адже саме обрана методологічна база обумовлює принципи та механізм формування корпоративної інформаційної безпеки. Виходячи з того, що забезпечення інформаційної корпоративної безпеки, з одного боку, має ґрунтуватись на чітко окреслених наукових засадах, а з іншого – мати суто прагматичний характер, вважаємо за потрібне в межах компоненту «методологічна база» виокремити два підрівні: «метаметодологію» та «підходи до управління».

Метаметодологія визначає загальні філософські основи пізнання світу та окремих явищ і процесів. Так, серед наявних загальнонаукових та філософських концепцій пізнання світу, яка останнім часом стала мейнстрімом в економічній методології, в тому числі є позитивізм, що пройшов вже певну еволюцію (від власне позитивізму до постпозитивізму). Позитивізм – філософія позитивного знання, що відкидає теоретичні спекуляції й умогляди як засоби одержання знання. Позитивізм почав спробу осмислення істини на основі точного експериментального знання. Ідея: знати, щоб передбачити, передбачати – щоб мати силу.

Позитивізм знайшов широку популярність у соціології, політиці, праві та економічній теорії [11]. Позитивістська філософська основа пройшла три стадії розвитку: позитивізм, неопозитивізм та постпозитивізм.

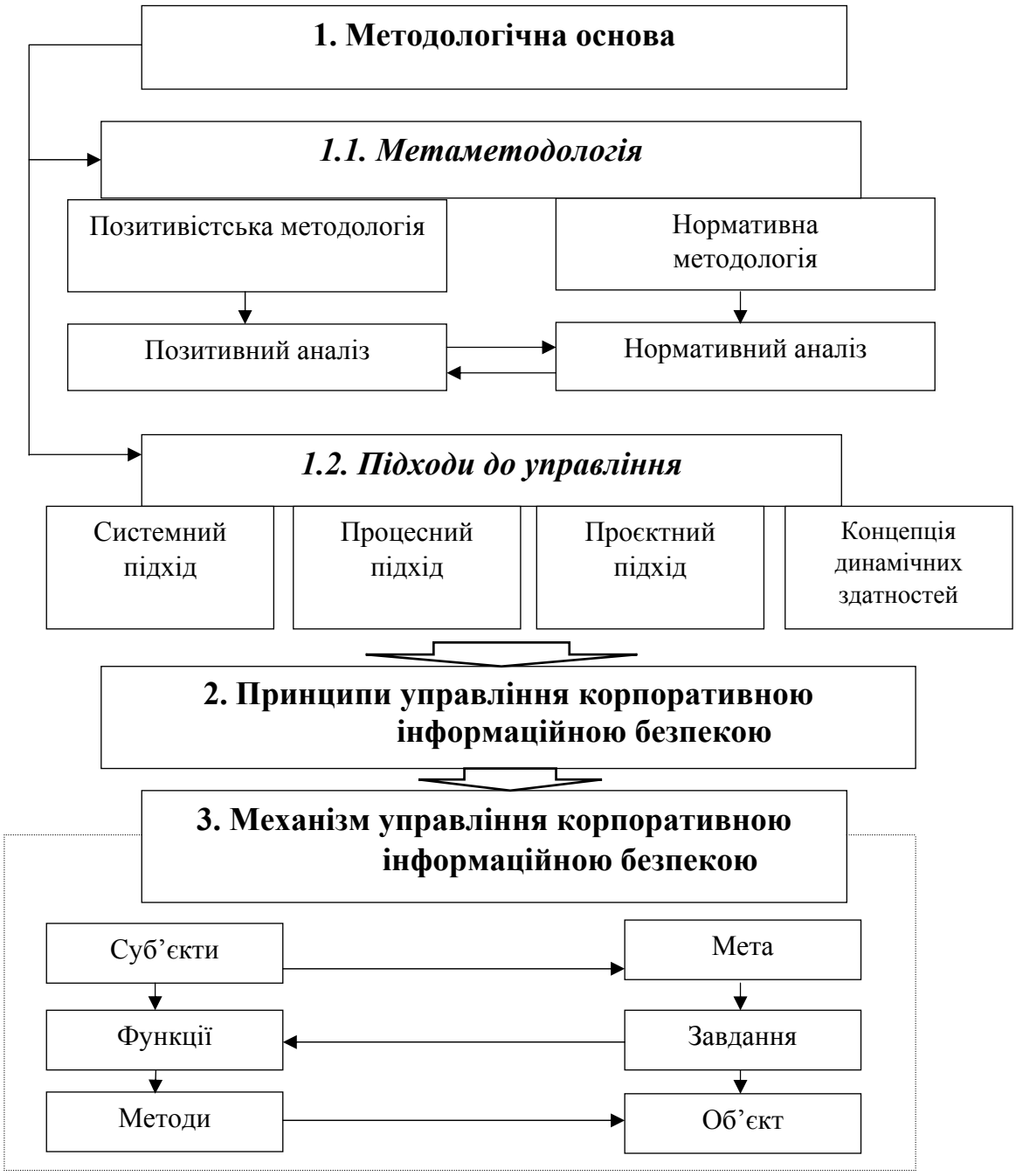


Рис. 2.1. Елементи концепції формування корпоративної інформаційної безпеки

Джерело: розроблено автором

Таким чином, позитивізм в економічній теорії ґрунтується на філософії позитивізму, що визнає як джерело знання практику і конкретні науки, які не потребують власного методологічного обґрунтування. Прихильники цього підходу вважають неправильною і позбавленою практичної значущості будь-яку теоретичну систему, засновану на нереальних постулатах і непідтверджених фактах господарського життя. Характерними рисами позитивізму є феноменталізм (відображення конкретних факторів як феномена); верифікація (безпосереднє зведення наукових знань до конкретних знань); прагматизм (значимість знання залежно від вузькопрактичних наслідків).

Зазначена методологія найкращим чином, на нашу думку, може бути основою формування концепції корпоративної інформаційної безпеки, захист якої потребує повсякчасного аналізу стану інформаційної системи, загроз, що виникають тощо, а розроблені моделі захисту корпоративної інформації потребують постійної верифікації та вдосконалення. Важливою складовою цієї методології є позитивний аналіз, тобто аналіз «як є», який власне і спрямовує підприємство на постійний моніторинг та оцінку стану об'єкта, засобів впливу на нього.

Другою важливою складовою метаметодології є нормативна методологія. Так, С. В. Мочерний визначає нормативну економічну теорію як теорію, в якій аналіз окремих економічних явищ або процесів, національної економіки загалом дається на основі оцінок вченого з погляду інтересів окремих соціальних верств, груп, населення країни або загальнолюдських інтересів з урахуванням їх справедливого або несправедливого характеру [12].

Словник економічних термінів нормативну економічну теорію тлумачить як теорію, яка здатна не тільки пояснити економічні явища і події, а й покликана передусім сприяти виробленню економічної політики, необхідного способу дій, прийняттю раціональних рішень. Нормативна теорія повинна давати конкретні рекомендації уряду, керівникам підприємств, фірм, як необхідно діяти в певній економічній ситуації [13]. При цьому оцінки та рекомендації даються на основі ціннісних орієнтацій, суджень та думки окремого науковця, чи фахівця.

Таким чином, на противагу позитивній економічній теорії нормативна теорія описує «як має бути» та яким чином досягати цього стану. Важливою складовою цієї методології є нормативний аналіз, який і описує бажаний (ідеальний) стан об'єкта.

У межах обґрунтування концепції формування корпоративної інформаційної безпеки нормативна методологія є основою для подальшого цілевизначення та розроблення заходів у сфері захисту корпоративної інформації.

Інший підрівень методології – підходи до управління – спрямований на конкретизацію метаметодології й окреслює підходи до управління інформаційною безпекою, що покладаються в основу вибору засобів впливу на об'єкт управління, оцінювання тощо.

Відповідно до сучасних умов господарювання та розвитку теорії менеджменту ми пропонуємо покласти в основу побудови системи забезпечення інформаційної безпеки інтеграцію системного, процесного, проєктного підходів та концепції динамічних здатностей.

Так, системний підхід в управлінні передбачає насамперед врахування найбільш істотних рис системи, якими, на думку Б. І. Холод, є:

а) наявність різних елементів, складових системи;

б) наявність взаємозв'язку елементів системи;

в) наявність мети, що є початком системи, котра пов'язує і визначає взаємодію елементів.

Таким чином, систему автор визначає як сукупність взаємно пов'язаних і в той же час різних елементів, створену для досягнення певної мети [14].

Системний підхід передбачає дотримання основних законів системи, а саме:

1. Композиції, тобто узгодження спільної і приватної мети.

2. Пропорційності. Внутрішня пропорційність повинна поєднуватись із зовнішньою пропорційністю, тобто відповідним рівнем розвитку елементів зовнішнього середовища.

3. Зважання на «вузьке місце», де особлива увага приділяється найбільш слабкому елементу системи.

4. Онтогенезу, що враховує послідовність стадій життєвого циклу підприємства (товару).

5. Інтеграції, що спрямовує систему на високий рівень організації і дає змогу одержати синергетичний ефект.

6. Інформованості, що виділяє інформаційне забезпечення як головну умову конкурентоспроможності.

7. Стійкості, що висуває вимоги до побудови системи (статичний стан) і до її функціонування (динамічний стан) [15].

Таким чином, уже в своїй основі системний підхід відводить важливе значення інформації в системі ресурсного потенціалу підприємства, забезпеченні його функціонування та необхідності захисту інформації з метою підтримання статичної та динамічної стійкості підприємства в умовах мінливого зовнішнього середовища. Системний підхід передбачає як структуризацію корпоративного інформаційного поля, так і структуризацію елементів системи управління та захисту корпоративного інформаційного поля.

Важливе значення в сучасних умовах для забезпечення ефективного управління підприємством відводиться постійному вдосконаленню бізнес-процесів, у тому числі процесам захисту корпоративної інформації. Саме постійний аналіз, оцінювання бізнес-процесів дозволяють оптимізувати їх вартість, якісні параметри, адаптуватись до змін зовнішнього середовища, забезпечуючи стійкість системи та її фінансових результатів. Фокусування уваги на бізнес-процесах підприємства пов’язаний з процесним підходом.

Наприклад, М. Х. Мескон визначає процесний підхід як такий, що базується на концепції, згідно з якою управління є безперервною серією взаємопов’язаних дій або функцій [16]. Дослідження та оцінка серії таких дій справді дає змогу вдосконалювати бізнес-модель підприємства, шукати слабкі місця у забезпеченні захисту корпоративної інформації. Останнім часом актуальність застосування процесного підходу лише посилюється з огляду на пандемії, воєнний стан. Ці події змушують підприємства кардинально змінювати бізнес-процеси з метою адаптації до абсолютно нових умов

функціонування. А в умовах інформатизації та цифровізації бізнесу потреба в постійному вдосконаленні процесів захисту інформації є перманентною з огляду на постійне нарощення та модифікацію загроз корпоративному інформаційному простору.

Важливим елементом процесного управління є регламентація і чіткий опис процесів, що також надзвичайно важливо в системі захисту корпоративного інформаційного поля та формування корпоративної інформаційної безпеки. Методологія процесного підходу покладена і в основу міжнародних стандартів якості із забезпечення корпоративної інформаційної безпеки. Так, у стандарті ISO/IEC 17799:2000 «Інформаційні технології – практичні правила управління інформаційною безпекою» зазначається, що «цей Міжнародний стандарт сприяє утвердженню процесного підходу до створення, впровадження, експлуатації, моніторингу, аналізу, супроводу та вдосконаленню системи управління інформаційною безпекою організації».

Реалізація окремих заходів щодо вдосконалення бізнес-процесів захисту корпоративної інформації часто потребує серйозних фінансових витрат, має інноваційний характер і втілюється як інвестиційні проєкти, які спрямовані на модернізацію інформаційної інфраструктури тощо. Проєктний підхід до управління є також, на нашу думку, важливим елементом методологічної основи концепції інформаційної безпеки підприємства. У класичному розумінні проєкт можна розглядати як підбір і об'єднання бізнес-процесів, що забезпечують виконання рішення унікального завдання в заданий термін з заданими ресурсами. Основними особливостями проєктного управління є: розгляд проєкту як унікальної комбінації процесів; зосередження прав і відповідальності за досягнення результатів у керівника проєкту і проєктної групи; виділення бюджету проєкту; застосування спеціальної проєктної організаційної структури та проєктної мотивації його учасників; розроблення і застосування спеціальних стандартів реалізації складових процесів проєкту [17].

У разі декомпозиції проєкт може розбиватися на субпроєкти, а ті, у свою чергу, – на процеси. Процеси можуть розбиватися на підпроцеси або функції. У підсумку виникає детальний багаторівневий опис порядку виконання проєкту: проєкт – субпроєкти – процеси – функції. На наступному етапі сфери проєкту можуть закріплюватися за виконавцями (організаційними ланками), і таким чином формується проєктна модель відповідальності [17].

В умовах зростаючої конкуренції та ролі нематеріальних чинників в економіці суттєво актуалізується питання пошуку стійких конкурентних переваг. Відповіддю на цей запит став розвиток ресурсної концепції фірми, яка пройшла шлях від класичної ресурсної концепції в середині XX сторіччя до концепцій ключових компетентностей, динамічних здібностей (1990-ті роки) та концепції ресурсних переваг, (2000-ті роки). Концепція динамічних здібностей, яка поступово трансформується в концепцію ресурсних переваг стала відповіддю на гуманізацію ресурсів та зростання ролі знань в отриманні стійких конкурентних переваг.

Погоджуємось з тезою про те, що сучасний етап гуманізації сутності ресурсів підприємства в економічній теорії позначився відділенням нематеріальної складової ресурсу від її носія (людини) в самостійну категорію, а синонім нематеріальних ресурсів – інформацію, що деякі науковці пропонують вважати ще одним фактором виробництва. Більше того, із поширенням використання інформаційних технологій у діяльності соціально-економічних систем інформацію починають розглядати як основу для отримання ресурсів вищого порядку – знань. Знання є невіддільними від людини і визначають можливості використання будь-яких матеріальних та нематеріальних ресурсів з метою розвитку бізнесу. Жоден матеріальний ресурс не є ресурсом, поки не існує знань (не визначено можливостей) його продуктивного використання. Розуміння ресурсів як можливостей піднімає управління ними на рівень стратегії підприємства [18].

В основі динамічних здатностей лежать пошукові (дослідницькі) рутини, які забезпечують проактивність і креативність стратегічного процесу.

Вихідний базис для тлумачення динамічних здатностей розроблено Д. Дж. Тісом, Г. Пізано та А. Шуєн та ін. [19–22], які визначали їх як уміння підприємства інтегрувати, створювати та реконфігурувати внутрішні й зовнішні компетенції у відповідь на швидкі зміни зовнішнього середовища. «Ми називаємо цей потенціал досягнення нових форм конкурентної переваги «динамічними здатностями», маючи на увазі акцентування двох ключових аспектів, які не перебували раніше у центрі уваги попередніх концепцій стратегічного управління.

Термін «динамічні» означає можливість оновлення компетенцій з метою досягнення узгодженості зі змінним бізнес-середовищем. Термін «здатності» підкреслює ключову роль стратегічного управління у належній адаптації, інтеграції та реконфігурації внутрішніх і зовнішніх організаційних навиків, ресурсів та функціональних компетенцій з метою відповідності вимогам бізнес-середовища» [23]. При цьому конкурентні переваги, на думку авторів концепції, реалізуються у наявних відмітних процесах, сформованих внаслідок існування на підприємстві специфічних активів і траєкторії еволюційного розвитку, яку воно набуло або успадкувало.

Незважаючи на відмінності у визначеннях і незалежно від галузевих, функціональних і технологічних особливостей організаційних здатностей, у сучасній літературі є консенсус щодо їх загальних характеристик, якими прийнято вважати:

– по-перше, здатності, як правило, мають цінність для діяльності організації зі створення різних продуктів і на різних ринках;

– по-друге, здатності є вбудованими в організаційні рутини і тому можуть зберігати своє значення, якщо окремі працівники залишать організацію;

– по-третє, за суттю здатності є неявними, тобто їх важко викласти у вигляді алгоритмів поведінки або операційних процедур [18].

У новітньому трактуванні Д. Дж. Тіса динамічні здатності організації містять чотири організаційні вміння:

– рутинізовані процеси управління інноваціями та змінами;

– бізнес-інтуїцію і бачення, необхідне для створення бізнес- моделей;

– механізми ухвалення правильних економічних рішень (що дозволяють визначити нові ринки й технології; обмежити невизначеність; передбачливо здійснювати ризиковані інвестиції в нові технології; забезпечувати ефективний зв'язок коспеціалізованих активів);

– компетенції «оркестрування» й управління трансакціями (наприклад, ухвалення рішення про аутсорсинг і вибір партнерів у цій сфері).

На думку авторів концепції, динамічні здатності можна звести у три категорії: процеси, позиції за активами та траєкторії розвитку. Свою тезу вони пояснюють тим, що компетенції та здатності вбудовано в організаційні процеси певного роду. Одначе зміст цих процесів і можливостей, що надаються ними для створення конкурентної переваги в будь-який момент, значною мірою зумовлюється особливостями активів, якими володіє фірма, та траєкторією розвитку, котру вона сприйняла або успадкувала.

У контексті забезпечення корпоративної інформаційної безпеки концепція динамічних здатностей проявляє себе в тому, що процеси захисту інформації, позиція підприємства за активами (нематеріальними та матеріальними, які обумовлюють спроможності підприємства до організації інформаційних потоків, зберігання інформації та захисту), обрані стратегії захисту обумовлюють не лише захищеність підприємства та відсутність фінансових втрат від порушення цілісності, конфеденційності інформації, а в цілому посилюють позицію підприємства за всіма видами активів.

Отже, в узагальненому вигляді взаємопов'язаність та взаємообумовленість підходів до управління, що обрано та покладено в основу концепції формування корпоративної інформаційної безпеки, можна представити за допомогою рис. 2.2.

Рис. 2.2. Інтеграція підходів до управління, що покладена в основу концепції формування корпоративної інформаційної безпеки

Джерело: розроблено автором

Наступною компонентою концепції корпоративної інформаційної безпеки є принципи її забезпечення.

Так, концепція інформаційної безпеки України визначає такі принципи її забезпечення: верховенство права; пріоритетність захисту прав і свобод людини і громадянина в інформаційній сфері; своєчасність та адекватність заходів щодо захисту життєво важливих національних інтересів України від реальних і потенційних загроз інформаційній безпеці; захист інформаційного суверенітету України; свобода думки і слова та вільне вираження своїх поглядів і переконань; свобода на право збирати, зберігати, використовувати та поширювати інформацію; захищеність особи від втручання в її особисте та сімейне життя; обмеження доступу до інформації виключно на підставі закону; гармонізація особистих, суспільних і державних інтересів, відповідальність всього українського народу за забезпечення інформаційної безпеки; розмежування повноважень, взаємодія та відповідальність державних і недержавних суб'єктів забезпечення інформаційної безпеки; пріоритетність розвитку та поширення національних інформаційних технологій, ресурсів, продукції та послуг, а також політика постійного поліпшення кількості та технічної якості каналів передавання інформації; можливість задіяння в інтересах забезпечення інформаційної безпеки України систем і механізмів міжнародної та колективної безпеки; гармонізація інформаційного законодавства з нормами міжнародного права і правовими актами Європейського Союзу; захист інформаційного суверенітету, державного суверенітету, конституційного ладу і територіальної цілісності України; формування в інформаційному просторі української ідентичності як невід'ємної складової сталого суспільно-політичного дискурсу; формування дуальної системи суспільного та комерційного мовлення; сприяння розвитку в національному інформаційному просторі контенту, який підтримує збереження і захист загальнолюдських цінностей, інтелектуальний, духовний і культурний розвиток українського народу [3].

Формування корпоративної інформаційної безпеки насамперед не повинно порушувати зазначені принципи та сприяти формуванню національної інформаційної безпеки.

На сьогодні в наукових дослідженнях немає єдиного підходу до визначення принципів формування корпоративної інформаційної безпеки.

Так, І. А. Маркіна пропонує дотримуватись таких принципів формування корпоративної інформаційної безпеки: законність, дотримання балансу інтересів особи, суспільства й держави; системність; плановість; комплексність; безперервність; взаємна відповідальність суб'єктів забезпечення інформаційної безпеки, їх взаємодія; спадкоємність і безперервність вдосконалення; розумна достатність; персональна мінімізація повноважень; наукова обґрунтованість і технічна реалізація; обов'язковість контролю; превентивний характер проведення заходів з інформаційної безпеки щодо заходів інших видів безпеки [24].

Варто зазначити, що автором представлений досить вичерпний перелік принципів, а щодо значної їх частини є консенсус серед інших дослідників [25–37].

На нашу думку, зазначені принципи варто доповнити такими:

Принцип креативності та інноваційності, який полягає у необхідності розроблення креативних та інноваційних підходів до захисту інформації та організації інформаційних потоків на підприємстві, які діють на випередження. Реалізація такого принципу дозволить отримувати підприємству унікальні конкурентні переваги в царині інформаційної безпеки, що сприятиме в цілому більш конкурентоздатній позиції по активах.

Принцип економічної ефективності, який передбачає забезпечення порівнянності витрачання ресурсів на формування інформаційної безпеки та можливих потенційних втрат від реалізації загроз інформаційній безпеці.

Принцип ситуаційності та адаптивності, який передбачає швидке коригування стратегій захисту інформації залежно від ситуації.

Принцип інтегрованості в загальну систему управління. З огляду на те, що інформація є особливим видом ресурсів, який сприяє підвищенню ефективності використання інших ресурсів, корпоративна інформаційна безпека має формуватися з урахуванням її впливу на стан інших видів безпеки, а процеси ідентифікації, аналізу, нейтралізації інформаційних загроз розглядатися в комплексі з іншими видами ресурсів.

Принцип ризик-орієнтованості, який передбачає дослідження інформаційних загроз у контексті вивчення ризиків підприємства.

З огляду на викладене вище в узагальненому вигляді принципи формування корпоративної інформаційної безпеки можна представити за допомогою табл. 2.1.

Таблиця 2.1

Принципи формування корпоративної інформаційної безпеки

Принцип	Стисла характеристика
Законність	Заходи з підтримання інформаційної безпеки мають лежати в межах чинного правового поля
Дотримання балансу інтересів особи, суспільства й держави	Заходи з убезпечення інформації повинні відповідати принципам національної інформаційної безпеки, не порушувати прав та інтересів окремих осіб (працівників, клієнтів тощо) та максимально захищати корпоративний інформаційний простір
Системність	Заходи з убезпечення інформації мають узгоджуватись та оцінюватись з позицій впливу та можливих наслідків на всі підсистеми підприємства
Плановість	Підприємство повинно мати чітку стратегію та оперативно-тактичний план з розроблення та реалізації заходів щодо убезпечення інформації

Закінчення табл. 2.1

Принцип	Стисла характеристика
Комплексність	Заходи з убезпечення мають охоплювати всі елементи корпоративного інформаційного поля
Безперервність	Заходи з убезпечення інформації повинні відбуватися на постійній основі
Взаємна відповідальність суб'єктів забезпечення інформаційної безпеки, їх взаємодія	Всі суб'єкти з забезпечення корпоративної інформаційної безпеки мають діяти узгоджено та відповідально, дотримуватися встановлених регламентів та нести відповідальність за якість і результати своїх рішень
Розумна достатність	Заходи з убезпечення повинні відповідати ресурсним можливостям підприємства та потенційним загрозам інформаційній безпеці
Персональна мінімізація повноважень	Дотримання балансу повноважень, що забезпечує можливість реалізації процесу з захисту інформації в умовах звільнення відповідального працівника та уникнення персональних ризиків
Обов'язковість контролю	Постійний моніторинг і контролювання інформаційного поля та заходів з його убезпечення
Превентивний характер проведення заходів інформаційної безпеки щодо заходів інших видів безпеки	Заходи з інформаційної безпеки мають бути переважно попереджувального характеру
Креативність та інноваційність*	Розроблення креативних та інноваційних підходів до захисту інформації та організації інформаційних потоків на підприємстві, які діють на випередження
Економічна ефективність*	Забезпечення порівнянності витрачання ресурсів на формування інформаційної безпеки та можливих потенційних втрат від реалізації загроз інформаційній безпеці
Ситуативність та адаптивність*	Швидке коригування стратегій захисту інформації залежно від ситуації
Інтегрованість*	Управління корпоративною інформаційною безпекою має інтегруватися в загальну систему управління
Ризик-орієнтованість*	Управління корпоративною інформаційною безпекою повинно бути повністю узгоджене та гармонізоване з системою ризик-менеджменту на підприємстві

** Запропоновано автором*

Джерело: узагальнено та розвинено автором на основі [24–35]

Ще одним структурним елементом концепції корпоративної інформаційної безпеки є механізм її формування.

«Механізм» у загальному розумінні – це система, простір, спосіб, що визначає порядок будь-якої діяльності, системи взаємодії певних ланок та елементів або внутрішню будову, систему, сукупність станів та процесів, з яких складається певне явище [38]. Прорив у теорії механізмів в економіці був створений Л. Гурвіцем, Р. Майєрсоном та Е. Маскіном, за що у 2007 році вони отримали нобелівську премію з економіки за «видатний внесок у теорію економічних механізмів». На думку Л. Гурвіца, механізм – це взаємодія між суб'єктами і центром, яка складається з трьох стадій: суб'єкти надсилають інформацію у центр; центр отримує всю інформацію й розраховує майбутній результат; центр оголошує результат. Таким чином, було доведено можливість і необхідність механістичного підходу до управління економічними системами.

Словник-довідник під редакцією С. В. Мочерного дає визначення механізму управління як свідомо організованого, цілеспрямованого та активного впливу різних суб'єктів управління на процес розвитку та функціонування суспільного способу виробництва, окремих його ланок [39].

Дослідник В. А. Герцик визначає механізм управління як систему елементів управління, до яких належать цілі, функції, методи, структури, суб'єкти та об'єкти управління. У цій системі в результаті впливу елементів управління змінюється стан об'єктів управління [40]. Натомість В. С. Пономаренко, О. М. Ястремська, В. М. Луцковський та ін. визначають його як сукупність форм, структур, методів та засобів управління, котрі об'єднані спільністю мети, за допомогою яких здійснюється узгодження суспільних, групових та особистих інтересів, забезпечується функціонування і розвиток підприємства як соціально-економічної системи [41].

Схожі підходи до визначення та структуризації економічного механізму підприємства зустрічаються і в інших дослідженнях [42, 43].

Отже, спостерігаємо консенсус серед науковців щодо структуризації економічного механізму. В загальному вигляді в структуру економічного механізму підприємства завжди включають об'єкт, суб'єкти управління, мету, завдання, функції, засоби (методи, інструменти) впливу на об'єкт.

Зважаючи на те, що корпоративна інформаційна безпека спрямована на забезпечення стійких фінансових результатів та стійкого розвитку підприємства, нарощення його вартості (тобто підпорядкована основній меті та завданням його економічної діяльності) процес її формування ґрунтується на теорії економічних механізмів та має бути інтегрованим у механізм управління підприємством і відповідно включати не лише економічні важелі, а й економічні методи. Водночас широке застосування спеціалізованих інформаційних технологій потребує включення до складу такого механізму низки технічних методів.

Критичний аналіз, узагальнення та розвиток сучасних наукових підходів до формування механізму економічної безпеки підприємства та її інформаційної складової зокрема [38–43] дав змогу нам таким чином відобразити механізм формування корпоративної інформаційної безпеки (табл. 2.3).

Таблиця 2.3

Елементи механізму формування корпоративної інформаційної безпеки

Елементи	Стисла характеристика
Об'єкти	Структурні елементи корпоративного інформаційного простору: інформаційне поле; віртуальна реальність; інформаційний процес; інформаційна культура; технічні та технологічні засоби; регламенти та норми
Суб'єкти	Служба безпеки; IT-служба; юридична служба; топменеджери; відповідальні за процеси та центри фінансової відповідальності; окремі особи, що мають доступ до конфіденційної інформації

Продовження табл. 2.3

Елементи	Стисла характеристика
Мета	Забезпечення реалізації економічних інтересів підприємства шляхом захисту корпоративної інформації
Завдання	Забезпечення цілісності, конфеденційності та доступності інформації
Функції	– ідентифікація загроз інформаційній безпеці; – формування організаційної структури служби безпеки; – оцінювання та аналіз загроз інформаційній безпеці; – розроблення стратегії захисту та планів захисту корпоративної інформації; – координація роботи служби безпеки з іншими службами підприємства; – нейтралізація загроз інформаційній безпеці; – контролювання корпоративного інформаційного простору та реалізації заходів із захисту корпоративної інформації
Методи впливу	***Економічні***: – аналіз бізнес-процесів; – система збалансованих показників; – стратегічні карти; – карта ризиків; – методи інтегрального аналізу; – прикладний інформаційний аналіз; – споживчий індекс; – додана економічна вартість; – вихідна економічна вартість; – управління портфелем активів; – оцінка дійсних можливостей; – метод життєвого циклу штучних систем; – сукупна вартість володіння; – функціонально-вартісний аналіз; – метод експертних оцінок; – метод дисконтованого грошового потоку; – метод індексу дохідності; – метод чистої приведеної вартості; – сценарний підхід; – метод імітаційного моделювання; – метод нечітких множин

Закінчення табл. 2.3

Елементи	Стисла характеристика
	– метод Ісікави; – метод генетичних алгоритмів
	Організаційно-правові: – моделювання бізнес-процесів; – комплаєнс; – формування регламентів та положень
	Технічні *методи моделювання інормаційної безпеки:* – модель Bell-LaPadula (BLP); – модель Biba; – модель Clark-Wilson (CW); – дискреційна (матрична) модель; – модель Адепт-50
	– модель MITER ATT & CK TM»; – «модель алмазу» «Diamond Model»; – «піраміди болю» («The Pyramid of Pain») Модель «глибинного захисту» *– автоматизовані системи управління інформаційними ризиками:* CRAMM, CORAS, OCTAVE, Risk Watch, Oracle Crystal Ball

Джерело: розроблено автором

Варто зазначити, що представлений перелік методів впливу на стан інформаційної безпеки, з одного боку, є далеко невичерпним, а з іншого – досить варіативним. Підприємство обирає методи управління інформаційною безпекою залежно від особливостей внутрішнього і зовнішнього середовища, обраної стратегії захисту тощо.

Зміст окремих економічних методів широко висвітлюється в літературі, окреслимо лише можливу сферу їх застосування в процесі управління корпоративною інформаційною безпекою залежно від контексту реалізації основних функцій (табл. 2.4).

Таблиця 2.4

Економічні методи управління корпоративною інформаційною безпекою

Назва методики	Ідентифікація загроз	Аналіз	Планування
Прикладний інформаційний аналіз (Applied Information Economics, AIE)	+	+	+
Споживчий індекс (Customer Index, CI)	–	+	–
Додана економічна вартість (Economic Value Added, EVA)	–	+	–
Вихідна економічна вартість (Economic Value Sourced, EVS)	+	+	+
Управління портфелем активів (Portfolio Management, PM)	+	+	+
Оцінка дійсних можливостей (Real Option Valuation, ROV)	+	+	+
Метод життєвого циклу штучних систем (System Life Cycle Analysis, SLCA)	+	+	+
Система збалансованих показників (Balanced Scorecard, BSC)	-	+	+
Сукупна вартість володіння (Total Cost of Ownership, TCO)	-	+	–
Функціонально-вартісний аналіз (Activity Based Costing, ABC)	-	+	+
Метод експертних оцінок	+	+	+
Метод дисконтованого грошового потоку (DCF)	+-	+	-
Метод індексу дохідності (PI)	-	+	-
Метод чистої приведеної вартості (NPV)	+-	+	-
Метод імітаційного моделювання	+	+	+

Закінчення табл. 2.4

Назва методики	Ідентифікація загроз	Аналіз	Планування
Метод генетичних алгоритмів	+	+	+
Аналіз бізнес-процесів	+	+	-
Стратегічні карти	-	-	+
Карта ризиків	+	+	-
Методи інтегрального аналізу	+-	+	-
Сценарний підхід	+	-	+
Метод нечітких множин	+	-	+
Метод Ісікави	+	+	-

Джерело: розроблено автором

Організаційно-правові методи включають моделювання бізнес-процесів, в тому числі процесів захисту корпоративної інформації, комплаєнс та розроблення регламентних документів.

Так, для моделювання бізнес-процесів у сучасній практиці використовується декілька різних методів, в основі яких лежить як структурний, так і об'єктно -орієнтований підходи до моделювання. Погоджуємося з думкою про те, що класифікація самих методів на структурні та об'єктні є доволі умовною, оскільки найбільш розвинуті методи використовують елементи обох підходів [44]. Серед найбільш поширених методів моделювання бізнес-процесів можна виокремити такі: метод функціонального моделювання SADT (IDEF0); метод моделювання процесів IDEF3; моделювання потоків даних DFD; метод ARIS; метод Ericsson-Penker; метод технології Rational Unified Process (див. табл. 2.5).

Таблиця 2.5

Найбільш поширені методи моделювання бізнес-процесів підприємства

Методи	Коротка характеристика
SADT (Structured Analysis and Design Technique)	Вважається класичним методом підходу до управління на основі процесів, базовим принципом якого є структуризація діяльності організації у відповідності з її бізнес-процесами; використовується для моделювання штучних систем середньої складності
IDEF3	Частина сімейства стандартів IDEF; застосовується для моделювання послідовності виконання дій і їх взаємозалежностей в межах процесу. Метод отримав визнання серед системних аналітиків як доповнення до методу функціонального моделювання IDEF0. Основою моделі IDEF3 служить сценарій процесу, який відокремлює послідовність дій і підпроцесів системи. Як і в методі IDEF0, основною одиницею моделі є діаграма. Іншим важливим компонентом є дія або «одиниця роботи» (Unit of Work), взаємодія яких зображається за допомогою зв'язків
DFD (Data Flow Diagrams)	Ієрархія функціональних процесів, що пов'язані потоками даних. Мета такого представлення полягає у демонстрації того, як кожен процес перетворює свої вхідні дані на вихідні і виявлення зв'язків між цими процесами
ARIS (Architecture of Integrated Information System)	Комплекс засобів аналізу і моделювання діяльності підприємства. Його методичну основу становить сукупність різноманітних методів моделювання, що відображають різні погляди на системи. ARIS підтримує чотири типи моделей, які віддзеркалюють різні аспекти системи, що досліджується. Для побудови зазначених типів моделей використовуються як власні методи моделювання ARIS, так і різні відомі методи та мови моделювання, зокрема UML
Ericsson-Penker	Автори цього методу створили свій профіль UML для моделювання бізнес-процесів – Ericsson-Penker Business Extensions, ввівши набір стереотипів, які описують основні категорії бізнес-моделі: процеси, ресурси, правила і цілі діяльності підприємства

Закінчення табл. 2.5

Методи	Коротка характеристика
Rational Unified Process	Метод спрямовано насамперед на створення основи для формування вимог до ПЗ. Передбачає побудову двох базових моделей – моделі бізнес-процесів (Business Use Case Model) та моделі бізнес-аналізу (Business Analysis Model) Модель бізнес-процесів становить собою розширення моделі варіантів використання (Use Case) UML шляхом введення набору стереотипів – Business Actor (стереотип діючої особи) та Business Use Case (стереотип варіанту використання). Діючими особами можуть бути акціонери, замовники, постачальники, партнери, потенційні клієнти, місцеві органи влади, зовнішні системи, співробітники тих підрозділів організації, діяльність яких не враховується у моделі, тощо. Business Use Case визначається як опис послідовності дій (потоку) у межах певного бізнес-процесу, що дає результат для певної діючої особи

Джерело: систематизовано автором за [44–57]

Моделювання бізнес-процесів є основою для їх оптимізації, оцінювання вартості, вдосконалення бізнес-моделі, в тому числі стосовно формування корпоративної інформаційної безпеки.

Важливе місце в системі захисту корпоративної інформації посідає розроблення та запровадження різноманітних внутрішніх стандартів і регламентів роботи з інформацією. Насамперед варто зазначити, що політика підприємства в сфері інформаційної безпеки має відповідати чинній національній законодавчій базі, серед яких варто виокремити Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.», Концепцію інформаційної безпеки України (проєкт), Доктрину інформаційної безпеки України (Указ Президента України від 25.02.2017 № 47/2017), Стратегію національної безпеки і оборони України. Таким чином, внутрішні регламенти та стандарти не повинні суперечити чинним нормам зазначених нормативних актів.

Крім цього, серед зовнішніх регламентуючих документів варто наголосити на доцільності застосування стандартів якості в сфері захисту інформації, які мають рекомендаційний характер, проте можуть бути досить корисними в розробленні й реалізації політики інформаційної безпеки підприємства, зокрема: ISO 27001:2005 Сертифікація систем менеджменту; ISO/IEC 17799:2005: Міжнародний стандарт «Інформаційні технології – практичні правила управління інформаційною безпекою», а також документи, на який посилається ISO/IEC 17799:2005.

Спираючись на зазначені стандарти, власні цілі, потреби та особливості функціонування бізнесу в цілому й інформаційної системи зокрема, підприємство має обґрунтовувати власні внутрішні стандарти та регламенти, серед яких можуть бути такі: положення про комерційну таємницю та конфіденційну інформацію; посадові інструкції окремих фахівців, які працюють з інформацією; положення про службу безпеки тощо. Перелік таких документів може суттєво коливатися залежно від особливостей підприємства.

Наступним елементом організаційно-правових методів є комплаєнс, який можливий для впровадження саме завдяки реалізації попередніх заходів управління цього тематичного спрямування.

Термін «комплаєнс» – порівняно новий у діловому середовищі України і в цей час використовується в основному в фінансово-банківській сфері. У 2005 р. Базельським комітетом з банківського нагляду був опублікований документ «Дотримання законів, правил і рішень регулюючих органів і організація цієї діяльності в банках» (Compliance and the compliance function in banks) [58], на підставі якого в Україні обов'язковість застосування комплаєнс-політики регламентовано Методичними рекомендаціями щодо організації корпоративного управління в банках України [59]. Згідно із зазначеними документами, комплаєнс-ризик – це ризик юридичних санкцій, фінансових збитків або втрати репутації

внаслідок невиконання банком вимог законодавства, нормативно-правових актів, внутрішніх положень та правил, а також стандартів саморегулюючих організацій, що застосовуються до його діяльності. Станом на сьогодні практичне застосування функцій комплаєнс в Україні обмежується відсутністю правової визначеності, що є фундаментальною проблемою для ведення бізнесу: з одного боку, існує законодавство, що регулює бізнес (у тому числі в сфері бухгалтерського обліку та аудиту), а з іншого – закони України не вимагають від підприємств створювати внутрішні системи контролю і програми виконання встановлених правил, а тому запровадження комплаєнсу зазвичай є ініціативою самого підприємства. Його наявність у компанії завжди є свідченням високої корпоративної культури, прозорості та інноваційності в системі запровадження інструментів та технологій управління. Водночас варто зазначити, що в сучасній практиці комплаєнс упроваджують не лише кредитно-фінансові установи, а й підприємства інших секторів економіки, і ця тенденція посилюється [60–70].

У широкому сенсі комплаєнс – це частина системи управління / контролю в організації, пов’язана з ризиками невідповідності, недотримання вимог законодавства, нормативних документів, правил і стандартів наглядових органів, галузевих асоціацій та саморегулюючих організацій, кодексів поведінки і т.д. Такі ризики невідповідності в кінцевому підсумку можуть виявлятися у формі застосування юридичних санкцій або санкцій регулюючих органів, фінансових або репутаційних (іміджевих) втрат як результат невідповідності законам, загальноприйнятим правилам і стандартам [71].

Здебільшого комплаєнс фокусується на дотриманні належних стандартів поведінки на ринку, управління конфліктами інтересів, справедливого ставлення до клієнтів і забезпечення сумлінного підходу при консультуванні клієнтів. Проте в сучасній практиці до сфери комплаєнс належать також специфічні царини, серед яких чільне місце посідає

захист інформаційних потоків. У системі корпоративної інформаційної безпеки комплаєнс має орієнтуватися саме на уникнення ризиків умисного витоку конфіденційної інформації від персоналу підприємства, неумисного витоку інформації шляхом порушення встановлених внутрішніх стандартів та регламентів зберігання й передавання інформації, порушення національного законодавства в сфері інформації, що може призводити до іміджевих та фінансових втрат.

У банківській сфері, де запровадження комплаєнсу регламентується відповідним законодавством, виокремлюють два принципові підходи до його організації.

1. «Rule based approach», заснований на дотриманні норми, який передбачає мінімальний рівень організації комплаєнсу в банку – виконується тільки те, що імперативно вимагає закон.

2. «Risk based approach», що ґрунтується на аналізі ризиків. Саме такий підхід рекомендується іноземним банкам як національними регуляторами, так і міжнародними структурами (Вольфсбергська група, Базельський комітет з банківського нагляду), є домінуючим в Європі. В Україні він також рекомендований для впровадження центральним банком, однак, на жаль, у національній банківській практиці є менш поширеним, ніж підхід, заснований на нормі.

Якщо розглядати комплаєнс як інструмент формування корпоративної інформаційної безпеки, то, безумовно, його доцільно запроваджувати у формі «Risk based approach», що узгоджується з іншими інструментами формування корпоративної інформаційної безпеки.

Третьою групою методів формування інформаційної безпеки є технічні, в межах яких варто виокремити методи моделювання корпоративної безпеки та автоматизовані системи управління інформаційними ризиками. Стисла характеристика цих методів наводиться в табл. 2.6 та 2.7.

Таблиця 2.6

Характеристика методів моделювання корпоративної інформаційної безпеки

Методи	Коротка характеристика
Модель Bell-LaPadula (BLP)	Базується на політиці конфіденційності і визначає поняття захищеного стану; повністю математично формалізована
Модель Biba	Інтегрована модель; наявність рівнів інтеграції та додаткової властивості – виклику, що відповідає за можливість суб'єкта надсилати сервісні запити; пов'язана з рівнем інтеграції, на якому перебувають об'єкт і суб'єкт
Модель Clark-Wilson (CW)	Повною мірою забезпечує безпеку та підзвітність переходів у системі за рахунок вибору необхідного для такої ситуації режиму роботи з даними; передбачає поділ процедур з перевірки цілісності та процедур зміни, що дає змогу запобігти або виправити більшість нелегальних дій, які здійснюються всередині організації
Дискреційна (матрична) модель	Має більш практичне спрямування, оскільки стан системи захисту можна описати тріадою (на основі термінів матричної моделі): безліч суб'єктів доступу, безліч об'єктів доступу, матриця доступу; наочність і гнучкість налаштувань політики доступу до ресурсів; зайвий деталізований рівень опису відносин суб'єктів та об'єктів. Він призводить до підвищення складності адміністрування системи захисту під час задання параметрів і їх підтримки в актуальному стані при включенні до схеми розмежування доступу нових елементів (об'єктів чи суб'єктів або ж і тих, і інших одночасно), через що виникає ризик до-пустити багато помилок при адмініструванні
Модель Адепт-50	Модель, яка розглядає 4 групи об'єктів безпеки: користувачі, завдання, термінали та файли. Кожен об'єкт безпеки описується вектором (A, C, F, M), що включає різні параметри безпеки
Модель MITER ATT & CK TM	База знань про тактики та методи формування інформаційної політики, базовані на реальних спостереженнях; використовується як основа для розроблення конкретних моделей та методологій загроз, для приватного сектора користувачів та уряду; передбачає використання матриці, яка формується на основі використання таких показників: ступінь доступу, система реалізації програмних додатків, наполегливість, ескалація привілеїв, ухилення від захисту, доступ до довірених даних, відкриття, додатків дії, збирання, управління та адміністрування, ексфільтрація, вплив

Закінчення табл. 2.6

Методи	Коротка характеристика
«Модель алмазу» («Diamond Model»)	Визначає політику інформаційної безпеки об'єкта на основі аналізу чотирьох ознак: зловмисника (супротивника), інформаційної інфраструктури, можливостей (здатностей персоналу) та об'єкта впливу (жертви). Зазначені елементи розташовані у формі ромба, що і визначає назву моделі, а також додаткові метафункції для підтримки таких конструкцій вищого рівня, як пов'язання подій разом у потоки діяльності та подальше злиття подій потоків у групи інформаційної активності. Ця модель встановлює формальний метод, який застосовує наукові принципи аналізу вторгнень або загроз, методів їх вимірювання, встановлення достовірності та повторюваності, забезпечуючи комплексний метод синтезу та кореляції діяльності відносно забезпечення інформаційної безпеки об'єкта
«Піраміда болю» («The Pyramid of Pain»)	Вибір політики інформаційної безпеки ґрунтується на градуюванні загроз від слабких до критичних
Модель «глибинного захисту»	Передбачає розшарування механізмів інформаційної безпеки і тим самим підвищує безпеку системи в цілому. Якщо атака спричиняє збій одного механізму захисту, то інші механізми все ще можуть забезпечити необхідний рівень безпечності для захисту системи. Включає безліч елементів: персонал (людей), технологію, операційну систему, моніторинг та різні аспекти захисту як ключові компоненти забезпечення інформаційного захисту. Ці організаційні компоненти важко перевести в конкретні технологічні компоненти захисту, тому вони залишають такі сфери, як моніторинг безпеки та показники

Джерело: систематизовано автором за [72–82]

Компанія в ході формування політики управління корпоративною інформаційною безпекою може обирати за основу певний з варіантів описаних підходів, розробляти власний підхід, комбінувати елементи окремих технологій тощо.

Таблиця 2.7

Характеристика автоматизованих методів управління інформаційними ризиками

Методи	Стисла характеристика	Переваги	Недоліки
CRAMM	Британський метод, що має відомий підхід до кількісного і якісного розрахунку ір. Його основними цілями є: автоматизація управління ризиками, оптимізація фінансових витрат на управління, оптимізація часу на супровід систем безпеки компанії, підтримка безперервності бізнесу	Використовує комплексний підхід до оцінювання ризиків державних і комерційних організацій, застосовує технології оцінювання загроз і вразливостей за непрямими факторами з можливістю верифікації результатів, має широку базу знань про контрзаходи і володіє універсальністю і адаптованістю під профілі різних організацій. Розроблено програмні продукти, що реалізують цю методику	Потребує спеціальної підготовки і високої кваліфікації аудитора, процес є досить трудомістким і може обраховуватись місяцями безперервної роботи аудитора, не дає змоги створювати власні шаблони звітів або модифікувати наявні; припускає використання лише методів зниження рівня ризиків іб, такі способи управління ризиками, як «уникнення» або «прийняття», не розглядаються. Програмне забезпечення існує тільки англійською мовою
CORAS	Інструмент, що дає змогу документувати, створювати звіти про результати аналізу шляхом моделювання ризику. У цій методології інформаційні системи	Програмний продукт, що реалізує цю методологію, є безкоштовним і не потребує значних ресурсів для встановлення; методика проста у використанні і не потребує спеціальних знань	Не передбачена періодичність проведення оцінювання ризиків і оновлення їх величин; не дає змоги оцінити ефективність інвестицій, вкладених у впровадження заходів безпеки, та не дає можливості знайти

Продовження табл. 2.7

Методи	Стисла характеристика	Переваги	Недоліки
	представлені як складний комплекс з урахуванням людського фактора, а не тільки на основі використовуваних технологій		необхідний баланс між заходами, спрямованими на виявлення, виправлення або відновлення інформаційних активів та запобігання їм
Risk Watch	Сімейство програмних продуктів, побудованих на загальному програмному ядрі, які призначені для управління різними видами ризиків та підтримки великого різновиду стандартів	Як критерії для оцінювання та управління ризиками використовуються «очікувані річні втрати» та оцінка «повернення інвестицій»; орієнтована на точне кількісне оцінювання співвідношення втрат від загроз безпеці і затрат на створення системи захисту	Отримані оцінки ризиків (математичне очікування втрат) далеко не вичерпують розуміння ризику з системних позицій – метод не враховує комплексний підхід до інформаційної безпеки
OCTAVE	Метод оперативного оцінювання критичних загроз, активів і вразливостей, який вказує на те, що персонал несе відповідальність за встановлення стратегії безпеки організації	Простота у використанні і наочність вихідних даних; швидке впровадження і використання в організаціях і установах різного профілю; регулярне проведення оцінювання ризиків та оновлення їх величин як частини процесу оцінювання ризиків. Існує програмний продукт, що реалізує положення цієї методики	Не використовується такий спосіб управління ризиками як обхід (виключення); не дає кількісного оцінювання ризиків інформаційній безпеці, проте якісне оцінювання може бути використане у визначенні кількісної шкали їх ранжування

Закінчення табл. 2.7

Методи	Стисла характеристика	Переваги	Недоліки
Oracle Crystal Ball	Додаток до ms excel для моделювання бізнес-процесів, оцінювання ризиків, прогнозування невизначених даних і оптимізації результатів. Моделювання за методом монте карло дає додаткові можливості оптимізації. Забезпечує моделювання та імітацію для здійснення «what-if» аналізу	Простота у використанні і наочність вихідних даних	

Джерело: систематизовано автором за [83–88]

Описані автоматизовані системи спрямовані на проведення оцінювання ризиків інформаційної безпеки, що дає можливість сконцентрувати увагу на найбільш актуальних проблемах та запобігти завданню шкоди підприємству шляхом порушення корпоративної інформаційної безпеки.

Список бібліографічних посилань

1. Сурмін Ю. П. Майстерня вченого : підручник для науковця. Київ : навч.-метод. центр «Консорціум з удосконалення менеджмент-освіти в Україні», 2006. С. 38.

2. Концепція / В. Лук’янець. Концепції науки. С. 301 // Філософський енциклопедичний словник / В. І. Шинкарук (гол. редкол.) та ін. Київ : Інститут філософії імені Григорія Сковороди НАН України : Абрис, 2002. 742 с.

3. Концепція інформаційної безпеки України : проєкт. URL : https://www.osce.org/files/f/documents/0/2/175056.pdf (дата звернення: 14.06.2022).

4. Кавун С. В. Економічна безпека підприємства: інформаційний аспект. Харків, 2014. 312 с.

5. Ковтун О. І. Стратегія підприємства : навч. посіб. Київ, 2014. 680 с.

6. Судакова О. І., Щеглова О. Ю., Гасенко О. О. Головна характеристика механізму управління економічною безпекою розвитку підприємства // Науковий вісник Міжн. гуманітарного ун-ту. Серія «Економіка і менеджмент». 2017. № 24. С. 11–14.

7. Чумак О. В., Андрющенко І. С. Управління витратами в інформаційно-аналітичній системі підприємств ресторанного господарства : монографія. Харків, 2016. 268 с.

8. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект : навч. посіб. / Київ : Атіка, 2005. 432 с.

9. Кононович В. Г., Тардаскін М. Ф. Основні положення концепції інформаційної безпеки телекомунікаційних мереж загального користування. *Захист інформації*. 2006. № 8.1 (28). С. 18–30.

10. Борсуковський Ю. В. Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Частина 1. *Кібербезпека: освіта, наука, техніка*. 2019. № 1(5). С. 61–72.

11. Позитивізм як найбільш впливовий рух західної філософії другої половини XIX. URL : https://osvita.ua/vnz/reports/ philosophy/13067 (дата звернення: 14.06.2022).

12. Економічна енциклопедія : у 3 т. / за ред. С. В. Мочерного. Київ : видавнич. центр «Академія», 2000. Т. 1. 864 с.

13. Словник економічних термінів. URL : http://epi.cc.ua/-slovar-ekonomicheskih-terminov247.html (дата звернення: 14.06.2022).

14. Холод Б. І., Зборовська О. М. Системний підхід – основа сучасного управління діяльністю промислових підприємств. Академічний огляд. 2010. № 1 (32). С. 48–54.

15. Єфімова О. Системний підхід – основа управління діяльністю підприємств. Персонал. 2007. № 2. С. 67–72.

16. Мескон М., Альберт М., Хедоури М. Основы менеджмента : пер с англ. М. : Дело, 1997. 495 с.

17. Сутність проектного підходу до управління організацією. URL : https://pidru4niki.com/1580042053533/menedzhment/upravlinnya_proektami (дата звернення: 14.06.2022).

18. Управління ресурсами підприємства : монографія / за заг. ред. канд. екон. наук, проф. Г. О. Швиданенко. Київ : КНЕУ, 2014. 418 с.

19. Tis D. Dzh., Pizano G., Shuen E. Dynamic capabilities and strategic management of the company// Strategic Management Journal. 1997. Vol. 18, № 7. P. 509–533.

20. Семенчук А. О. Концепція динамічних здатностей конкурентоспроможного підприємства // *Ефективна економіка*. № 5. 2014. URL : http://www.economy.nayka.com.ua/?op=1&z=2987 (дата звернення: 14.06.2022).

21. Collis D. J. Research note: how valuable are organizational capabilities? // Strategic Management Journal. 1994. Vol. 15. № 8. P. 143–152.

22. Amit R., Schoemaker P. J. H. Strategic assets and organizational rent // Strategic Management Journal. 1993. Vol. 14, № 1. P. 33–46.

23. Teece D. J. Dynamic Capabilities and Strategic Management / Oxford University Press, 2009.

24. Маркіна І. А., Гарічев Ю. М. Інформаційна безпека підприємства та організаційні заходи її забезпечення. Український журнал прикладної економіки. 2019. Том 4. № 4. С. 209–215.

25. Барановський О. І. Фінансова безпека. Київ : Фенікс, 1999. 338 с.

26. Богуш В., Юдін О. Інформаційна безпека держави. Київ : МК-Прес, 2005. 432 с.

27. Економічна безпека підприємств, організацій та установ : навч. посіб. / В. Л. Ортинський, І. С. Керницький, З. Б. Живко та ін. Київ : Правова єдність, 2009. 544 с.

28. Жарков Я. М., Бєсєдіна Л. М. Напрямки зовнішнього інформаційно-психологічного впливу на Україну // Збірник наукових праць Військового ін-ту Київського Нац. ун-ту ім. Т. Шевченка. 2009. № 19. С. 15–19.

29. Захаркін О. О., Абрамчук М. Ю., Деркач М. А. Інформаційні системи та технології у фінансових установах. Суми : Вид-во СумДУ, 2007. 80 с.

30. Інформаційна безпека. Економічний енциклопедичний словник. URL : http://zalik.org.ua/index.php?newsid=25011 (дата звернення: 14.06.2022).

31. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. ... докт. юрид. наук : спец. 12.00.07. М-во освіти і науки України, Нац. ун-т внутр. справ. Харків. ХНУВС, 2004. 42 с.

32. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. Київ : КНТ, 2006. 280 с.

33. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. Державна безпека України. 2011. № 21. С. 92–95.

34. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи Юридичний журнал. 2009. № 5. С. 122–134.

35. Питання концепції реформування інформаційного законодавства України / Р. Калюжний, В. Говловський, В. Цимбалюк, М. Гузалюк. Київ : НТУУ «КПІ», Міністерство освіти і науки України, 2000. С. 17–21.

36. Амитан В. М. Економічна безпека: концепція й моделі. Економічна кібернетика. 2009. № 3. С. 13–20.

37. Васильців Т. Г. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення : монографія / Т. Г. Васильців, В. І. Волошин, О. Р. Бойкевич, В. В Каркавчук. Львів, 2012. 386 с.

38. Літвінов О. С., Капталан С. М. Сутність та види механізмів в економіці. Східна Європа: економіка, бізнес та управління. 2017. № 6 (11). С. 146–147.

39. Економічна енциклопедія : у 3 т. / За ред. С. В. Мочерного. Київ : видавнич. центр «Академія», 2000. Т. 2. 848 с.

40. Герцик В. А. Ієрархічна структура організаційно-економічного механізму управління розподілом підприємства. Культура народов Причерноморья. 2009. № 172. С. 22–24.

41. Пономаренко В. С., Ястремская Е. Н., Луцковский В. М. Механизм управления предприятием: стратегический аспект : монографія. Харків : вид. ХДУ, 2002. 252 с.

42. Саблук П. Т., Малік М. Й., Валентинов В. А. Формування міжгалузевих відносин: проблеми теорії і методології. Київ : ІАЕ, 2002. 294 с.

43. Полтавський Ю. А., Супрун О. М. Ринковий механізм як система забезпечення ефективної діяльності аграрних підприємств // Вісник Харківського національного технічного ун-ту сільського господарства: економічні науки. Ринкова трансформація економіки АПК. 2004. Вип. 31. с. 375–380.

44. Методи моделювання бізнес-процесів. URL : https://pidru4niki.com/12710107/informatika/tehnologiyi_modelyuvannya_biznes-protsesiv_mova_uml (дата звернення: 14.06.2022).

45. Aho A., Ullman J. D. Data Structures and Algorithms. Amsterdam : Addison Wesbley, 1982. 448 p.

46. Бабенко Л. П., Лаврищева К. М. Основи програмної інженерії. Київ : Знання, 2001. 269 с.

47. Booch G., Jacobson I., Rumbaugt J. UML Distilled: A Brief Guide to the Standard Object Modeling Language. Amsterdam : Addison-Wesley Longman, 2000. 457 p.

48. Вербіцький О. Вступ до криптології. Львів : вид-во наук.-техн. літ-ри, 1998. 247 с.

49. Goodliff P. Programmer's craft. Practice writing good code / 1st edition. No Starch Press, 2006. 624 p.

50. Гундарь К. Ю., Гундарь А. Ю., Янишевский Д. А. Защита информации в компьютерных системах. Київ : Корнейчук, 2000. 152 с.

51. Жуков І. А., Дрововозов В. І., Махновський Б. Г. Експлуатація комп'ютерних систем та мереж : навч. посіб. Київ : НАУ, 2007. 361 с.

52. Катренко А. Дослідження операцій : підручник. Львів : Магнолія 2006, 2009. 350 с.

53. Малайчук В. П., Рожковський В. Ф. Основи теорії кодування й декодування. Дніпро : Дніпропетр. держ. ун-т, 2000. 204 с.

54. Taha H. Operations Research. An Introduction. Pearson Higher Education. 2017. 813 p.

55. Томашевський В. М. Моделювання систем. Київ : видавнича група BHV, 2005. 400 с.

56. Цегелик Г. Чисельні методи. Львів : Вид. центр ЛНУ ім. Івана Франка, 2004. 408 с.

57. Young B. Object-Oriented Analysis and Design with Sample Applications / 3rd Edition. Amsterdam : Addison-Wesley Longman, 1993. 589 p.

58. Basel Committee on Banking Supervision: Compliance and the compliance function in banks, april 2005. URL : http://www.bis.org/publ/bcbs113.htm (дата звернення: 14.06.2022).

59. Методичні рекомендації щодо організації корпоративного управління в банках України : схвал. рішенням Правління Національного банку України від 03.12.2018 № 814-рш. Дата оновлення: 28.11.2019. URL : https://zakon.rada. gov.ua/ laws/show/vr814500-18#Text (дата звернення: 14.06.2022).

60. Kocziszky G., Veres M. Somosi, Pererva P. G. Anti-corruption compliance in the enterprise's program // Стратегічні перспективи розвитку економічних суб'єктів в нестабільному економічному середовищі : зб. тез наук. робіт 2-ї Всеукр. наук.-практ. інтернет-конф. з міжнар. участю, 28–30 листопада 2017 р. Кременч. нац. ун-т ім. Михайла Остроградського. Кременчук, 2017. С. 164–167. URL : https:// drive. google.com/file/d/1r-6uz8h9jl-bCWwpPrY7esG925mrQudP/view (дата звернення: 14.06.2022).

61. Kocziszky G., Veres M. Somosi, Kobielieva T. O. Compliance risk in the enterprise // Стратегії інноваційного розвитку економіки України: проблеми, перспективи, ефективність «Форвард-2017» : тр. 8-ї Міжнар. наук.-практ. інтернет-конф. студ. та молодих вчених, 27 грудня 2017 р. / ред.: П. Г. Перерва, Є. М. Строков, О. М. Гуцан. Харків : НТУ «ХПІ», 2017. С. 54–57.

62. Kocziszky G., Veres M. Somosi, Kobielieva T. O. Reputational compliance // Дослідження та оптимізація економічних процесів «Оптимум-2017» : тр. 13-ї Міжнар. наук.-практ. конф., 6-8 грудня 2017 р. / ред.: О. В. Манойленко, Є. М. Строков. Харків : НТУ «ХПІ», 2017. С. 140–143.

63. Nagy S., Sikorska M., Pererva P. Current evaluation of the patent with regarding the index of its questionnaire // Сучасні підходи до креативного управління економічними процесами : матеріали 9-ї Всеукр. наук.-практ. конф., 19 квітня 2018 р. Київ : НАУ, 2018. С. 21–22.

64. Sikorska M., Kocziszky G., Pererva P. Compliance service at guest services enterprises // Менеджмент розвитку соціально-економічних систем у новій економіці : матеріали Міжнар. наук.-практ. інтернет-конф., 19 жовтня 2017 р. Полтава : ПУЕТ, 2017. С. 389–391.

65. Бондаренко Ю. Эффективное управление compliance-рисками: системный подход и критический анализ // Корпоративный юрист. № 6. 2008. С. 31–34.

66. Бортников Г. Комплайенс-риск (риск несоблюдения): международные стандарты и их применимость для банков в странах СНГ. URL : http://www.iiru.ru/inner_auditor/publication/foreignmass_media_articles/bortnikov (дата звернення: 14.06.2022).

67. Климко Т. Ю., Мельник Е. А. Корпоративний комплаєнс як превентивний захід боротьби з шахрайством. Економіка і фінанси. 2015. № 6–7. С. 25.

68. Козлов Д. Н., Юденков Ю. Н. Контроль регуляторных рисков. URL : http://futurebanking.ru/reglamentbank/article/2092 (дата звернення: 14.06.2022).

69. Козырева Н. А. Внутренний контроль и комплаенс // Внутренний контроль в кредитной организации. 2015. № 1. С. 65.

70. Кобєлєва Т. О. Сутність та визначення комплаєнс-ризику // Вісник Національного технічного ун-ту «ХПІ». Економічні науки = Bulletin of the National Technical University «KhPI». Economic sciences : зб. наук. пр. Харків : НТУ «ХПІ», 2020. № 1 (3). С. 116–121.

71. Комплаєнс як фактор інноваційного розвитку підприємства. URL : http://repository. kpi.kharkov. ua/bitstream/KhPI-Press/39628/1/Pererva_Komplaiens_iak_faktor_2018.pdf (дата звернення: 14.06.2022).

72. Богомолов С. А. Модели типовых политик безопасности. 2016. URL : https://infourok.ru/lekciya-po-zaschite-informacii-modeli-bezopasnosti-927637.html (дата звернення: 14.06.2022).

73. Мельник М. О., Нікітин Г. Д., Мезенцева К. О. Аналіз побудови моделі політики інформаційної безпеки підприємства // Системи обробки інформації. 2017. Вип. 2 (148). С. 126–128.

74. Модели в информационной безопасности. URL : https:// habr.com/ru/post/467269/ (дата звернення: 14.06.2022).

75. Spillman R. et al, Use of Genetic Algorithms in Cryptanalysis of Simple Substitution Ciphers // Cryptologia. 1993. Vol. 17 (1). P. 31–44.

76. Ревнивых А. В., Федотов А. М. Обзор политик информационной безопасности // Вестник НГУ. Серия «Информационные технологии». 2012. № 3. URL : https:// cyberleninka.ru/ article/n/obzor-politik-informatsionnoy-bezopasnosti (дата звернення: 14.06.2022).

77. Степанов В. Ю. Інформаційна безпека як складова державної інформаційної політики // Державне будівництво. 2016. № 2. URL : http://www.kbuapa.kharkov.ua/e-book/db/2016-2/doc/1/02.pdf (дата звернення: 14.06.2022).

78. Чуруброва С. М. Політика інформаційної безпеки в системах інформаційно-аналітичного забезпечення підтримки прийняття організаційних рішень // Проблеми програмування. 2016. № 4. С. 97–103.

79. Домарев В. В. Безопасность информационных технологий. Системный подход. Київ : ООО «ТИД», 2004. 912 с.

80. Caballero A. Information security essentials for it managers: protecting mission-critical systems. URL : samplechapters/ 9781597495332/02~Chapter_1.pdf https://booksite. elsevier. com/ (дата звернення: 14.06.2022).

81. Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments. National Security Agency, Information Assurance Solutions Group. STE 6737.

82. Дячков Д. В. Формування моделі політики інформаційної безпеки на основі концепції «глибинного захисту». Підприємництво і торгівля. 2019. № 25. С. 116–121.

83. Замула А. А., Северинов А. В., Корниенко М. А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации // Наука і техніка Повітряних Сил Збройних Сил України. 2014. № 2 (15). С. 133–138.

84. Гарасим Ю. Р., Ромака В. А., Рибій М. М. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем // Вісник Нац. ун-ту «Львівська політехніка». Серія «Автоматика, вимірювання та керування». 2013. № 753. С. 90–99.

85. Левченко М. О. Використання інформаційних технологій в управлінні ризиками машинобудівних підприємств. Актуальні проблеми економіки. 2012. № 4. С. 305–311.

86. Мельник Г. Модель оценивания уровня информационных рисков в корпоративных системах // Вісник Київського Нац. ун-ту імені Тараса Шевченка. Серія «Економіка». 2015. № 6 (171). С. 48–54.

87. Гловацький В. В. Методи оцінювання стану безпеки та загроз інформаційних ресурсів. Зв'язок. 2016. № 5. С. 13–16.

88. Савельева Т. В., Панаско О. М., Пригодюк О. М. Аналіз методів і засобів для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства // Вісник Черкаського державного технологічного ун-ту. Серія «Технічні науки». 2018. № 1. С. 81–88.

2.2. Методологічні засади формування корпоративної політики інформаційної безпеки

У сучасних умовах розвитку корпорацій коло питань щодо забезпечення інформаційної безпеки корпорацій перемістилося з вузькоспрямованого технічного до стратегічного пріоритетного завдання бізнесу. Головною метою корпоративної політики інформаційної безпеки є забезпечення безперервності бізнесу та зменшення збитків шляхом мінімізації наслідків інцидентів безпеки та запобігання їм.

Отже, сьогодні виникає об'єктивна необхідність створення системи захисту корпоративних інформаційних систем та зміцнення національної безпеки країни шляхом включення інформаційної безпеки корпоративного сектора до системи корпоративного управління. Визначаючи інформаційну безпеку однією з основних вимог системи корпоративного управління, необхідно зазначити, що вона є корпоративним інструментом забезпечення стійкого, динамічного та збалансованого розвитку вітчизняних корпорацій.

Політика інформаційної безпеки корпорацій є елементом корпоративного управління і випливає зі стратегічних вимог до управління ризиками та корпоративного управління. Інформаційна безпека корпорацій має бути реалізована відповідно до бізнес-цілей, які характеризуються високим рівнем динамічності за умов необхідності безперервного послідовного узгодження між політикою безпеки та іншими напрямами корпоративної бізнес-політики та стратегіями. Послідовне узгодження політики інформаційної безпеки може бути досягнене шляхом конвергенції корпоративної політики інформаційної безпеки з іншими бізнес-політиками політики організації у межах циклу стратегічного управління.

Питання формування ефективної корпоративної політики інформаційної безпеки в різних її аспектах досліджували багато вітчизняних та зарубіжних науковців. Однак незважаючи на значну кількість праць, потрібно констатувати факт відсутності уніфікованого термінологічного узагальнення політики інформаційної безпеки та механізмів її реалізації, що активізує дискусії вчених стосовно систематизації політики інформаційної безпеки та методичного інструментарію її впровадження як на рівні держави, так і на рівні корпорацій.

Стаття 17 Конституції України регламентує захист інформаційної безпеки, нарівні із захистом суверенітету та територіальної цілісності України, є найважливішою функцією держави та справою всього українського народу [1].

Відповідно до Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» поняття «інформаційна безпека» має таке визначення: «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації» [1]. Оскільки саме інформаційна система синтезує дані про стан та тенденції розвитку всіх інших систем діяльності корпорацій, вона одночасно функціонує

як відокремлена складова, так і у взаємодії з іншими елементами корпоративної системи, створюючи єдиний інформаційний корпоративний простір.

Аналізуючи сутність корпоративної політики інформаційної безпеки, треба зазначити, що більшість науковців розглядають її тільки через склад її компонентів, без виділення в окрему категорію цього терміна.

Так, В. В. Домарєв та О. В. Гордієнко характеризують політику інформаційної безпеки як набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок оброблення інформації і спрямовані на захист інформації від певних загроз [3]. І. В. Анікін, В. І. Глова та А. Н. Нігматулліна визначають політику інформаційної безпеки як набір норм, правил і практичних рекомендацій, що регламентують процес оброблення інформації, виконання яких забезпечує захист від заданої множини загроз [4].

На думку А. Я Страхарчука і В. П. Страхарчука, політика інформаційної безпеки – це набір законів, правил і практичних рекомендацій, на базі яких здійснюється керування, захист і розподіл критичної інформації в системі [4].

Натомість Є. М. Бодюл пропонує політику інформаційної безпеки розуміти як науково обґрунтовану систему поглядів на визначення основних напрямів, умов і порядку практичного вирішення завдань інформаційного захисту організацій та установ від протиправних дій [6].

За визначенням Ю. Хохлачової, політика інформаційної безпеки – це сукупність керівних принципів, правил, процедур фактичних прийомів, якими об’єкт керується в своїй діяльності [7].

М. Бондаренко, О. Потій, І. Горбенко та інші характеризують політику інформаційної безпеки як сукупність правових і морально-етичних норм, правил, адміністративних, організаційних заходів і технічних, програмних і криптографічних засобів, спрямованих на захист інформаційної інфраструктури організації від випадкового і навмисного втручання в процес її функціонування [8].

На думку А. Нашинець-Наумової, політика інформаційної безпеки – це сукупність нормативних документів, які встановлюють порядок забезпечення безпеки інформації на конкретному підприємстві, а також висувають вимоги щодо підтримання цього порядку [9].

Варто зазначити, що більшість вітчизняних науковців доводять необхідність застосування комплексної системи захисту інформації корпоративного простору при впровадженні корпоративної політики інформаційної безпеки.

Так, З. Валіулліна та О. Черевко визначають, що в умовах сучасних глобалізаційних процесів інформаційна безпека корпорацій є пріоритетним напрямом соціально-економічного розвитку держави. Ці автори обґрунтовують необхідність впровадження в діяльність корпорацій заходів законодавчого, економічного, програмно-технічного та адміністративно-управлінського характеру, комплексний влив яких дозволить створити інформаційно безпечний корпоративний простір [10]. При цьому формування системи комплексного захисту інформаційних ресурсів повинно бути забезпечене перш за все за рахунок системи створення механізмів власного забезпечення, здатних реалізувати її функціонування не тільки в повсякденних умовах, а й у критичних ситуаціях [11].

Погоджуючись з зазначеними вище думками, А. Нашинець-Наумова визначає необхідність застосування комплексу відповідних заходів також для проведення систематичного моніторингу стану інформаційної безпеки корпорацій та розроблення оптимальної моделі функціонування системи її забезпечення шляхом створення необхідних організаційно-економічних та правових механізмів формування розвитку і забезпечення ефективного використання інформаційних ресурсів корпорації [9, с. 60].

О. Й. Жабинець при розробленні політики інформаційної безпеки визначає доцільність прийняття відповідних заходів, спрямованих на захист активів компаній від будь-якої зміни, розкриття чи знищення, а також з метою забезпечення конфіденційності, цілісності та доступності інформації. [12].

Акцентують увагу на необхідності впровадження в діяльність корпорацій комплексу заходів та засобів контролю, які б дозволили здійснювати систематичне управління безпекою та ризиками М. Шилов та І. Жевелєва [13].

Дослідники В. Бакай та В. Зима обґрунтовують думку про те, що в умовах глобалізації саме ефективна політика інформаційної безпеки є пріоритетним механізмом забезпечення системи економічної безпеки підприємства й економічної безпеки держави загалом. Водночас, автори наголошують на тому, що саме політика забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку корпорацій, доводячи, що «в нових реаліях, без належного захисту інформаційного середовища підприємства неможливо забезпечити його економічну безпеку» [14].

Наведені вище підходи до визначення корпоративної політики інформаційної безпеки відображають погляди багатьох вітчизняних дослідників, але не враховують стратегічний підхід до феномену цього поняття.

Необхідність врахування саме стратегічного підходу до формування корпоративної політики інформаційної безпеки обґрунтовується тим, що сьогодні інформаційні технології відіграють особливу пріоритетну роль у розвитку бізнесу, забезпечуючи гнучку адаптацію бізнес-структур до впровадження інновацій та формування потенціалу і розвитку їх конкурентних переваг.

Тому зміна парадигми корпоративної політики інформаційної безпеки для зміни її вектору від внутрішньо орієнтованого захисту інформації до стратегічного погляду, який враховує міжорганізаційний рівень, є об’єктивно необхідним та доцільним. Модифікація парадигми корпоративної політики шляхом визначення стратегічного підходу дозволить визначати акценти та сфокусуватися саме на впровадженні в діяльність корпорацій механізмів щодо захисту інформаційних ресурсів на користь тих стейкголдерів, які приймають рішення та відповідальні за забезпечення ефективної політики інформаційної безпеки організації на стратегічному рівні.

У працях багатьох зарубіжних дослідників визначається, що збереження конфіденційності, цілісності та доступності інформаційних ресурсів є важливою вимогою для організації, як і потреба в життєздатній стратегії інформаційної безпеки в організаціях для полегшення передавання інформації на міжорганізаційному рівні [15].

На думку Н. Бибе і В. Рао, стратегічна політика інформаційної безпеки визначається як «шаблон або план, який об'єднує основні цілі, політику та послідовність дій організації щодо інформаційної безпеки в єдине ціле» [16]. Автори наголошують на необхідності узгодження оцінки зовнішніх інформаційних загроз із фінансово обґрунтованим комплексом внутрішніх контрзаходів, включаючи необхідні допоміжні політики та процедури, тобто політика інформаційної безпеки розглядається ними як ключовий інструмент впливу на зовнішнє бізнес-середовище організації шляхом ретельного відбору засобів внутрішнього контролю.

С. Парк і Т. Руіджхавер визначають корпоративну політику інформаційної безпеки як «мистецтво вирішувати, як найкращим чином використовувати відповідні технології та заходи оборонної інформаційної безпеки, а також скоординовано розгортати та застосовувати їх до інформаційної інфраструктури корпорації проти внутрішніх та зовнішніх загроз, пропонуючи конфіденційність, цілісність та доступність за рахунок найменших зусиль і витрат» [17]. Дослідження корпоративної політики інформаційної безпеки цими авторами доводить її міцний зв'язок з організаційним стратегічним планом корпорацій, яким саме стратегічна політика інформаційної безпеки дозволить запобігти наявним та потенційним загрозам інформаційним ресурсам у час, просторі і в процесі прийняття управлінських рішень.

Саме врахування стратегічного підходу, як стверджують К. С. Хонг та ін., до формування корпоративної політики інформаційної безпеки дає змогу розширити її функціонал та зорієнтуватися на управлінні ризиками та надзвичайними ситуаціями [18].

У. Флорес та інші зарубіжні вчені розглядають корпоративну політику інформаційної безпеки як динамічний процес забезпечення захисту корпоративної інформації, який реалізується зацікавленими особами [19].

Отже, корпоративна інформаційна політика інформаційної безпеки є ключовим елементом загальної бізнес-стратегії корпорації, що включає адекватну підтримку її стратегічного розвитку, згуртованість інформаційних систем і бізнесу та координацію зусиль з інформаційної безпеки.

Функціонування сучасних корпоративних структур в умовах динамічного бізнес-середовища змушує перманентно враховувати та приймати нові технології. Саме технологічний вплив обумовлює необхідність формування стратегічного вектору розвитку корпорацій з урахуванням ключових викликів, що обумовлюють необхідність змін напрямів їх діяльності (табл. 2.8).

Корпоративні структури швидко впроваджують цифрові бізнес-стратегії, які характеризуються високим рівнем технологічного розгортання. Наприклад, корпоративне використання хмарних сервісів, блокчейну, штучного інтелекту, інтернету речей, великих даних, мобільних і соціальних мереж [20]. Така тенденція, по-перше, призвела до всебічного вбудовування інформаційних технологій у бізнес корпорацій. Об’єктивно сформований поточний технологічний бізнес-клімат повністю нівелював дистанцію між традиційним фізичним і новим цифровим світом, створив єдиний простір інформаційних технологій та бізнесу, перетворив безпеку з ізольованої проблеми на стратегічний напрям корпоративної політики інформаційної безпеки, який потребує розроблення та впровадження відповідних регулюючих механізмів.

Таблиця 2.8

Стратегічні напрями діяльності корпорацій

Напрями діяльності, що потребують стратегічних змін	Ключові виклики
Цифрові бізнес-стратегії	Впровадження інформаційної безпеки в бізнес
	Відсутність розриву між фізичним і цифровим світом
	Безпека – це пріоритетний стратегічний напрям комплексного вирішення питань бізнесу
Стратегії мінімізації інцидентів з інформаційною безпекою	Залучення керівництва до перманентного вирішення питань щодо мінімізації інцидентів з безпекою
	Зростання безпосереднього впливу кібератак на бізнес, що потребує постійного пошуку альтернативних механізмів управління інформаційною безпекою
Стратегії організаційно-управлінського забезпечення перспектив інформаційної безпеки	Кібератаки обмежують інноваційні можливості та продуктивність корпорації, зменшуючи їх конкурентні переваги
	Перехід від внутрішньої до міжорганізаційної взаємодії
	Транскордонні ризики безпеки
	Збільшення довіри до діяльності корпорацій шляхом підвищення рівня безпеки та конфіденційності

Джерело: укладено автором

По-друге, через всебічне впровадження інформаційних технологій у бізнес інциденти з інформаційною безпекою, що викликають порушення стійкості функціонування корпорацій, безпосередньо впливають на прогресивність розвитку їхнього бізнесу [21]. Кібератаки обмежують перш за все продуктивність діяльності корпорацій, їх інноваційні можливості та обмежують конкурентні переваги. Це призводить до зменшення кола бізнес-партнерів, фінансових та репутаційних збитків [22].

Крім того, зарубіжні науковці виявили кореляцію між інцидентами інформаційної безпеки та ефективністю діяльності корпорацій [23]. Факт виникнення порушення інформаційної безпеки негативно впливає на ринкову вартість, коливається від 1 до 2,1 відсотка [24]. Зростання впливу кібератак на безпеку та ринкову вартість корпорацій змушують керівників корпорацій здійснювати постійний пошук альтернативних механізмів їх мінімізації.

По-третє, цифровізація потребує від організацій перейти на стратегічні міжорганізаційні перспективи забезпечення безпеки бізнесу корпорацій. Постійні порушення інформаційної безпеки підвищують розумні очікування клієнтів корпорацій щодо розроблення та впровадження заходів для захисту їхньої безпеки та конфіденційності [25]. Запорукою збереження та відтворення потенціалу цільової аудиторії корпорацій є формування нормативно-правової бази, що регламентує та забезпечує права всіх стейкголдерів бізнесу, таким чином, ще більше стимулюють ці очікування. Крім цього, необхідно зазначити, що в умовах сучасного цифрового середовища корпорації функціонують як цифровий ланцюг поставок, а не як окремі бізнес-одиниці [26]. Такий механізм їх функціонування обумовлює виникнення ризиків інформаційної безпеки за межами корпорацій, розширюючи завдання з розроблення відповідного методичного інструментарію формування ефективної корпоративної політики інформаційної безпеки, яка має бути зосереджена на створені прозорого міжорганізаційного захисту інтересів всіх зацікавлених осіб.

Стратегічні зміни, зумовлені впровадженням інформаційних технологій та формуванням єдиного цифрового корпоративного бізнесу-простору, виявили потребу в оновленому підході до розроблення методичних засад систематизації видів корпоративних політик інформаційної безпеки, які б враховували динаміку стратегічних змін напрямів діяльності корпорацій відповідно до ключових викликів сучасності.

Корпоративні структури – це динамічні системи зі складною внутрішньою структурою та різнобічними зв'язками між елементами, які цілеспрямовано забезпечують своє функціонування та взаємодію із зовнішнім середовищем.

В основі корпоративних структур лежить системний підхід. Методологія системного підходу полягає у виявленні тих аспектів предметів чи подій, які випливають із загальних властивостей системи. Дослідження ступеня розвитку систем та механізмів їх функціонування в умовах економічного середовища, що змінюється, становить основу дослідження корпоративних структур, їх властивостей, структури, організованості та функціонування з урахуванням взаємодії із зовнішнім економічним середовищем [27].

Корпоративні структури мають певні властивості, які забезпечують їх раціональне функціонування, зокрема:

– цілісність: структурні підрозділи корпорацій утворюють єдине ціле з якісно новими властивостями;

– зв'язність усіх структурних підрозділів корпорацій, як-от економічна, механічна, енергетична, інформаційна залежність між ними;

– структурність: якісно визначена та порівняно стійка впорядкованість між підрозділами та відносинами корпорацій;

– взаємодія між елементами всередині корпоративної системи та з зовнішнім середовищем;

– безперервність розвитку: зростання попиту, необхідність підвищення ефективності виробництва та науково-технічного прогресу;

– складність, що виявляється у взаємному неоднозначному впливі різноманітних факторів.

Корпоративні структури складаються з сукупності елементів, між якими існують певні зв'язки (структура внутрішніх відносин), і включають функціональні зв'язки із зовнішнім економічним середовищем. Характеристика елементів корпоративних структур та їх призначення представлені у табл. 2.9.

Таблиця 2.9

Характеристика елементів корпоративних структур

Елементи корпоративних структур	Призначення
Технічні ресурси	Забезпечення максимально можливої відповідності технічного рівня корпоративних структур сучасним вимогам
Технологічні ресурси	Забезпечення відповідності технологічних ресурсів цілям корпоративних структур
Кадрові ресурси	Забезпечення постійної відповідності кадрових ресурсів вимогам гнучкого реагування корпоративних структур на зміни потреб суспільства
Інформаційні ресурси	Забезпечення відповідності інформаційних ресурсів вимогам щодо прийняття оптимальних управлінських рішень з метою ефективного функціонування корпоративних структур
Організаційно-економічні ресурси	Забезпечення відповідності організаційно-економічних ресурсів вимогам безперервного підвищення ефективності використання трудових, матеріальних, інформаційних та фінансових ресурсів корпоративних структур

Джерело: укладено автором

Різноманітність властивостей, елементів корпоративних структур, їх призначення та зв'язки дозволяють зробити висновок, що вони належать до класу складних динамічних систем.

Отже, на цей час важливим для корпоративних структур є розроблення такої стратегії інформаційної безпеки, яка б забезпечувала гнучкість корпоративних структур в умовах економіч-

ної, соціальної та політичної динаміки і сприяла можливості прийняття ефективних рішень на основі адаптивних підходів в управлінні корпоративними структурами.

З огляду на зазначене обов'язковою умовою забезпечення ефективної та рентабельної діяльності корпоративних структур є підвищення ролі корпоративної політики інформаційної безпеки в управлінні їх розвитком. Забезпечення інформаційної безпеки стало стратегічним завданням для корпорацій через збільшення частоти, впливу, наслідків та складності інцидентів кібербезпеки [28].

Тепер корпораціям доводиться не лише боротися з бізнес-середовищем, яке характеризується конкуренцією, динамічністю за своєю природою та економічними проблемами; вони також повинні боротися з системою інформаційних небезпек, що є дуже складною і стрімко змінюється [29].

Сталий корпоративний розвиток може бути досягнутий лише за допомогою прагматичної стратегії, яка включає стійкість у своїй основі разом зі стійкими бізнес-моделями, а для збереження конкурентоспроможності динамічні можливості є ключовими факторами, що сприяють підтримці конкурентних переваг у бізнес-середовищі, що постійно змінюється [30].

Теорія динамічних можливостей, висунута D. J. Teece [31], є інструментальною, але вона не розширює взаємозв'язок динамічних можливостей з корпоративною стійкістю.

Корпоративна політика інформаційної безпеки, в основі якої лежать переважно соціально-економічні стимули розвитку корпорацій, сприяє істотному розширенню їх самостійності. Вона проявляється як у виборі цілей розвитку, так і у виборі засобів досягнення цих цілей.

Можливість варіювання цілей та маневрування ресурсами, що виникає під впливом корпоративної політики інфор-

маційної безпеки, позначається на прогресивності динамічного розвитку корпорацій.

Так, корпоративна політика інформаційної безпеки з переважанням командно-адміністративних стимулів сприяє формуванню корпоративних структур, прогресивність розвитку яких орієнтована на високий рівень централізації функцій управління: як функції цілепокладання, так і функції розподілу ресурсів.

Корпоративна політика інформаційної безпеки, в основі якої переважають соціально-економічні стимули, більшою мірою сприяє формуванню корпорацій з такою прогресивністю, що дає змогу гнучко реагувати на зміну потреб корпорацій.

Головним джерелом потенційного ефекту гнучкості корпоративних структур є сфера споживання її продукції, де саме й виникає обумовлена гнучкістю можливість своєчасного та якісного задоволення змін потреб суспільства. Ефект, що досягається у сфері споживання, у багато разів перевершує ефект автоматизації виробництва всередині самих гнучких корпоративних структур (вивільнення працівників, засобів виробництва, предметів праці). Не всі складові ефекту можуть бути визначені у вигляді економії витрат праці за допомогою діючих методик. До цих складових належать всі доданки соціально-економічного ефекту у сфері виробництва та споживання продукції гнучких корпоративних структур, хоча саме ці доданки найбільш інтенсивно впливають на підвищення соціально-економічної ефективності діяльності корпорацій. Своєчасне та якісне задоволення потреб суспільства часом настільки важливе з погляду необхідності вирішення суспільно-політичних завдань, що саме ці причини спонукають до прискореного впровадження у промисловість гнучких корпоративних структур. Задоволення таких потреб, безумовно, у переважній більшості випадків принесе і економічний ефект, але непрямий, розрахувати який за допомогою наявних методик виявляється інколи неможливим.

Ефект гнучких корпоративних систем, що включає всі елементи, варто визначити як «стратегічний» ефект гнучкого

реагування корпоративної політики інформаційної безпеки на зміну потреб суспільства.

Необхідність досягнення такого стратегічного ефекту висуває вимоги повноти обліку витрат на створення та функціонування політики інформаційної безпеки корпоративної структури, яка була б здатна такий ефект створити. Це становище випливає з відомого закону необхідної різноманітності, коли потрібно враховувати принаймні дві найважливіші обставини.

По-перше, щодо величини витрат, пов'язаних зі створенням і реалізацією корпоративної політики інформаційної безпеки, необхідно вибрати як об'єкт економічного аналізу таку сукупність технічних, технологічних, трудових, інформаційних, просторових і структурних ресурсів, яка була б здатна функціонувати автономно.

По-друге, гнучка політика інформаційної безпеки корпоративних структур, що створюється, повинна бути настільки значущою з точки зору кінцевого результату діяльності корпорацій, частиною якої вона є, щоб забезпечити можливість отримання всіх або принаймні найбільш значущих складових стратегічного ефекту.

Такий об'єкт, що відповідає вимогам автономності та значущості, назвемо первинним модулем гнучкої корпоративної політики інформаційної безпеки, витрати на створення та функціонування якого можуть створити передумови для отримання стратегічного ефекту гнучкого реагування на зміну цілей корпоративної структури. При визначенні складу корпоративної політики інформаційної безпеки необхідно враховувати також ефект цілісності (принцип емерджентності), що виражає таку важливу властивість системи: чим більша система і чим більша різниця в розмірах між частиною та цілим, тим частішою є ймовірність того, що властивості цілого можуть сильно відрізнятиметься від властивостей частин [32].

Це означає, що чим менший об'єкт прийнятий як модуль гнучкої корпоративної політики інформаційної безпеки, тим

менш імовірним є досягнення за допомогою цього об'єкта в повному обсязі стратегічного ефекту гнучкого реагування на зміну потреб суспільства. Нехтування цим принципом призводить до того, що на підприємствах створюються дрібні гнучкі об'єкти для забезпечення їхньої інформаційної безпеки, лінії та інші підрозділи, які не можуть забезпечити виникнення передумов для отримання ефекту, достатнього для окупності капітальних вкладень. З цього робиться висновок (іноді необґрунтований) про потенційну неможливість створення високоефективних гнучких інструментів реалізації корпоративної політики інформаційної безпеки або необхідність розроблення спеціальних методик визначення їхньої економічної ефективності, покликаних штучно підвищити ефект у сфері функціонування корпорацій.

Вибір модуля корпоративної політики інформаційної безпеки пов'язаний також із відомою закономірністю інтегративності системи, що передбачає наявність факторів, які забезпечують її збереження, тобто системоутворювальних та системозберігаючих. Стосовно гнучкої корпоративної політики інформаційної безпеки подібним системоутворювальним чинником є значимість елементів системи з погляду їхнього впливу на ступінь гнучкості всієї системи.

У кожній корпоративній системі можуть бути знайдені провідні елементи, від яких визначальною мірою залежить здатність системи досягати заданих цілей. Інакше якщо елемент системи має надмірну жорсткість, що не дозволяє всій системі ефективно, своєчасно та якісно переходити від виготовлення однієї продукції до іншої, то він має стати насамперед основою для створення модуля гнучкої корпоративної політики інформаційної безпеки. Якщо таких елементів системи кілька, то як основа модуля гнучкої корпоративної політики інформаційної безпеки повинна бути прийнята сукупність цих елементів системи. Ігнорування цього положення не дозволить досягти очікуваного ефекту, а вкладені кошти виявляться «умертвленими».

Таким чином, для кожного модуля гнучкої корпоративної політики інформаційної безпеки або їх сукупності повинно бути визначено оптимальне з точки зору співвідношення витрат та потенційного стратегічного ефекту прогресивність корпоративної системи, що забезпечує високий рівень ефективності задоволення потреб суспільства.

Зміна потреб суспільства позначається на прогресивності корпоративної політики інформаційної безпеки. У міру збільшення темпів зміни потреб, що виражаються у зростанні темпів оновлення продукції, прогресивність корпоративної політики інформаційної безпеки має посилюватись. Інакше корпорація перебуватиме у стані постійного переозброєння чи реконструкції. Посилення прогресивності неминуче пов'язане зі зростанням ступеня виробничої різноманітності продукції, що випускається корпорацією [33].

Отже, кількісною характеристикою зміни потреб суспільства за той чи інший період може стати індекс зміни за цей період ступеня розмаїття заходів корпоративної політики інформаційної безпеки: $I_p(t_h, t_k)$ де t_h, t_k – відповідно початок і кінець аналізованого періоду. Економічною характеристикою задоволення потреб, що змінюються, за той же період може бути прийнятий індекс зміни витрат, пов'язаних з функціонуванням корпоративної політики інформаційної безпеки $I_n(t_h, t_k)$. Тоді кількісною характеристикою гнучкості корпоративної політики інформаційної безпеки може бути показник:

$$G(t_h, t_k) = I_{np}(t_h, t_k), \qquad (2.1)$$

де G – індекс гнучкості корпоративної політики інформаційної безпеки.

У міру збільшення ступеня гнучкості системи за аналізований період все більше відрізнятиметься від одиниці (у більшу сторону). Це означає, що чим вищі темпи зміни ступеня різноманітності заходів корпоративної політики інформаційної безпеки порівняно з темпами зміни витрат, пов'язаних зі створенням та функціонуванням системи, тим інформаційна безпека має більший рівень гнучкості.

Якщо $G(t_h, t_k) < 1$, то створена система інформаційної безпеки корпорації повинна бути віднесена до категорії жорстких систем, при $G(t_h, t_k) = 1$ система адаптивна, якщо ж $G(t_h, t_k) > 1$ – система гнучка.

Дуже важливим при розрахунку показника $G(t_h, t_k)$ є визначення вимірювачів ступеня різноманіття напрямів корпоративної політики інформаційної безпеки, пов'язаних із створенням та функціонуванням корпоративних структур.

Як вимірник ступеня різноманіття напрямів корпоративної політики інформаційної безпеки у найпростішому випадку, як було показано вище, може бути використаний коефіцієнт асоціації. Тоді значення $I_{np}(t_h, t_k)$ визначають за формулою:

$$I_{np}(t_h, t_k) = [1 - S(t_h, t_k)]/[1 - S(t_h)], \qquad (2.2)$$

де $S(t_h, t_k)$, $S(t_h)$ – коефіцієнти асоціації відповідно за весь період та на початок періоду.

Як вимірник витрат, пов'язаних зі створенням та реалізацією, можуть бути прийняті витрати за період (t_h, t_k). Однак при цьому треба ретельно обґрунтувати їхній склад. Це зумовлено важливими положеннями визначення потенційного стратегічного ефекту гнучкого реагування на зміну потреб суспільства, викладеними вище.

Оскільки потенційний стратегічний ефект гнучкого реагування може бути забезпечений в результаті взаємодії всіх складових корпоративної політики інформаційної безпеки, то забезпечити передумови досягнення зазначеного ефекту можуть капітальні вкладення і поточні витрати, пов'язані зі створенням і функціонуванням цих складових.

У табл. 2.9 було розглянуто характеристику елементів корпоративних структур як сукупності певним чином технічних, технологічних, кадрових, інформаційних та організаційно-економічних ресурсів. Виходячи з цього, а також

зважаючи на склад потенційного стратегічного ефекту гнучкого реагування, визначимо узагальнений склад витрат, здатних зумовити виникнення потенційного стратегічного ефекту гнучкого реагування на зміну потреб суспільства (табл. 2.10).

Дані, наведені у табл. 2.10, можуть бути деталізовані з необхідним для тих чи інших цілей аналізу ступенем конкретизації. Для розрахунку кожної зі складових одноразових чи поточних витрат розробляються відповідні моделі.

Таблиця 2.10

Склад витрат, що створюють передумови для ефективного функціонування корпоративної політики інформаційної безпеки

Напрями витрат	
Разові	Поточні
Формування технічних ресурсів корпоративної політики інформаційної безпеки – K_1	Підтримання технічних ресурсів корпоративної політики інформаційної безпеки в актуальному стані – C^1
Формування технологічних ресурсів корпоративної політики інформаційної безпеки – K_2	Підтримання технологічних ресурсів корпоративної політики інформаційної безпеки в актуальному стані – C^2
Формування кадрового потенціалу корпоративної політики інформаційної безпеки – K_3	Підтримання в актуальному стані кадрового потенціалу корпоративної політики інформаційної безпеки – C^3
Формування інформаційних ресурсів корпоративної політики інформаційної безпеки – K_4	Підтримання в актуальному стані інформаційних ресурсів корпоративної політики інформаційної безпеки – C^4
Формування організаційно-економічних ресурсів корпоративної політики інформаційної безпеки – K_5	Підтримка в актуальному стані організаційно-економічних ресурсів корпоративної політики інформаційної безпеки – C^5

Джерело: укладено автором

Результати цих розрахунків виводяться за допомогою такого виразу:

$$Z(t_h, t_k) = \sum_{t=t_h}^{t=t_k}[(\sum_{i=1}^{i=h} C_{it} + \sum_{i=1}^{i=5} K_{it})(1 + E_h^z)^{t_k - t}], \quad (2.3)$$

де C_{it} – поточні витрати на підтримку в актуальному стані i-ої умови функціонування корпоративної політики інформаційної безпеки у році t, $t \in (t_h, t_k)$;

K_{it} – одноразові витрати на формування i-ої умови функціонування корпоративної політики інформаційної безпеки на рік t, $t \in (t_h, t_k)$;

E_h^z – коефіцієнт дисконтування різночасних витрат;

$Z(t_h, t_k)$ – витрати на створення та підтримання в актуальному стані умов функціонування корпоративної політики інформаційної безпеки у період (t_h, t_k).

Тоді:

$$I_n(t_h, t_k) = Z(t_h, t_k) / Z(t_h), \quad (2.4)$$

де $Z(t_h)$ – витрати на створення та підтримання в актуальному стані умов функціонування корпоративної політики у першому році аналізованого періоду.

Підставивши значення $I_{np}(t_h, t_k)$ у формулу (2.3), отримаємо кількісну характеристику гнучкості корпоративної політики інформаційної безпеки:

$$G(t_h, t_k) = \frac{[1 - S(t_h, t_k)](\sum_{i=1}^{5} C_{it_h} + \sum_{i=1}^{5} K_{it_h})(1 + E_h^z)^{t_k - 1}}{[1 - S(t_h)] \sum_{t=t_h}^{t_k} [(\sum_{i=1}^{5} C_{it} + \sum_{i=1}^{5} K_{it})(1 + E_h^z)^{t_k - t}]}. \quad (2.5)$$

Таким чином, здатність корпоративної політики інформаційної безпеки до гнучкого реагування на зміни потреб суспільства визначається співвідношенням темпів зміни ступеня напрямів корпоративної політики інформаційної безпеки та темпів зміни витрат, що забезпечують її ефективне функціонування протягом певного періоду.

Інакше кажучи, здатність корпоративної політики інформаційної безпеки змінювати свою прогресивність без істотного збільшення сукупних витрат, які забезпечують її ефективне функціонування, має кваліфікуватися як гнучкість цієї системи.

Отже, ефективність корпоративної політики інформаційної безпеки потрібно розуміти як досягнення заданих системі цілей з мінімальними витратами та одночасним покращенням (в ідеальному випадку) або (принаймні) не заподіянням шкоди соціальній та екологічній системам.

В умовах високих темпів науково-технічного прогресу корпоративна політика інформаційної безпеки може успішно виконувати своє головне призначення, якщо вона спочатку має можливість протягом тривалого часу ефективно, своєчасно і якісно задовольняти потреби корпорації, що змінюються. Однак ступінь різноманітності потреб, які задовольняються, має бути визначена в певних межах, тоді як основний чинник прогресивності – корпоративну політику інформаційної безпеки – треба розглядати як сталість і повторюваність ступеня розмаїття її напрямів та інструментів.

Таким чином, прогресивність корпоративної політики інформаційної безпеки варто трактувати її пристосованість до ефективного, своєчасного та якісного досягнення цілей і завдань функціонування корпорацій, що володіє певним і постійно повторюваним ступенем різноманітності напрямів.

Вихідним моментом процесу формування прогресивності корпоративної політики інформаційної безпеки є визначення завдань економічного та соціального розвитку суспільства на найближчу перспективу. Потреба вирішення цих завдань, їх характер і значущість визначають специфіку потреб суспільства, яка, своєю чергою, формулює вимоги до результативності діяльності корпорації, покликаної задовольняти ці потреби суспільства.

Специфіка потреб суспільства, що розглядаються у динаміці, диктує необхідність використання тих чи інших видів відтворюваних та не відтворюваних ресурсів, залучення у діяльність корпорацій нових ресурсів. З іншого боку, обмеженість ресурсів, можливості їх поповнення та регенерації коригують потреби суспільства, що впливають на обсяг цих потреб. Врахування зазначених факторів дає змогу формувати потенційні обсяги виробництва продукції корпорації, які в сукупності з вимогами природоохоронних обмежень та особливостями діяльності корпорації зумовлюють виникнення тих чи інших варіантів технології функціонування корпорації.

У різноманітті споживчих та виробничих властивостей діяльності та продукції корпоративних структур, обсягів потреби в ній та можливих обсягів, засобів та методів її виробництва об'єктивно проявляється процес поділу праці, який визначає галузеву, виробничу та організаційно-управлінську структуру діяльності корпорацій. Розширення потреб і напрямів діяльності корпоративних структур створюють передумови для їх галузевої діяльності, а різноманіття технологій, обумовлене науково-технічним прогресом, є основою розвитку різних видів і напрямів спеціалізації діяльності корпорацій.

У процесі взаємодії всіх цих факторів формується прогресивність корпоративної політики інформаційної безпеки, тобто склад та структура сукупності складових її ресурсів. Особливості прогресивності корпоративної політики інформаційної безпеки формують зворотні зв'язки з суспільними потребами та завданнями соціально-економічного розвитку країни. Ці зв'язки стимулюють чи, навпаки, стримують розвиток певних потреб. Незначна прогресивність корпоративної політики інформаційної безпеки має консервативність по відношенню до процесу оновлення діяльності корпорацій. У той самий час прогресивність корпоративної політики інформаційної безпеки стимулює прискорений розвиток потреб суспільства, створює сприятливі передумови для підвищення ефективності задоволення нових потреб економіки та населення.

Таким чином, у процесі дослідження виникає проблема пошуку кращої прогресивності корпоративної політики

інформаційної безпеки, тобто пошуку параметрів сфери ефективного функціонування системи.

Інформаційна безпека може бути представлена сукупністю певним чином організованих та спільно використовуваних ресурсів. До них треба віднести технічні, технологічні, кадрові, інформаційні й навіть організаційно-економічні ресурси. Загальний обсяг та структура цих ресурсів, система їх взаємодії дають змогу відповісти на питання про здатність виробничої системи до досягнення тих чи інших цілей, тобто визначити її прогресивність.

Принципово важливими етапами вибору кращої прогресивності корпоративної політики інформаційної безпеки варто вважати:

1. Формування безлічі технічно та організаційно здійсненних варіантів структури елементів системи.

2. Аналіз соціально-екологічних, тимчасових та якісних характеристик кожного варіанту з множини та формування підмножини допустимих варіантів.

3. Визначення з підмножини варіанта, що дає змогу системі досягти заданих цілей з максимальним ефектом в умовах обмежень засобів розширення сукупності ресурсів, які становлять виробничу систему.

Завдання першого етапу може бути вирішене на основі морфологічного аналізу структури елементів системи або за допомогою імітаційного динамічного моделювання чи інших відомих методів системного аналізу.

Завдання другого етапу – формування підмножини допустимих варіантів – здійснюється шляхом відбору тих з них, реалізація яких не викликає виникнення потенційно неприпустимих з точки зору встановлених суспільством нормативів негативних соціально-екологічних наслідків та забезпечує якісне й своєчасне задоволення потреб суспільства.

Завдання третього етапу можна вирішити з урахуванням економіко-математичного моделювання максимізації ефекту функціонування корпоративної політики інформаційної безпеки з урахуванням відповідних обмежень.

На рис. 2.3 представлено схему оптимізації прогресивності корпоративної політики інформаційної безпеки.

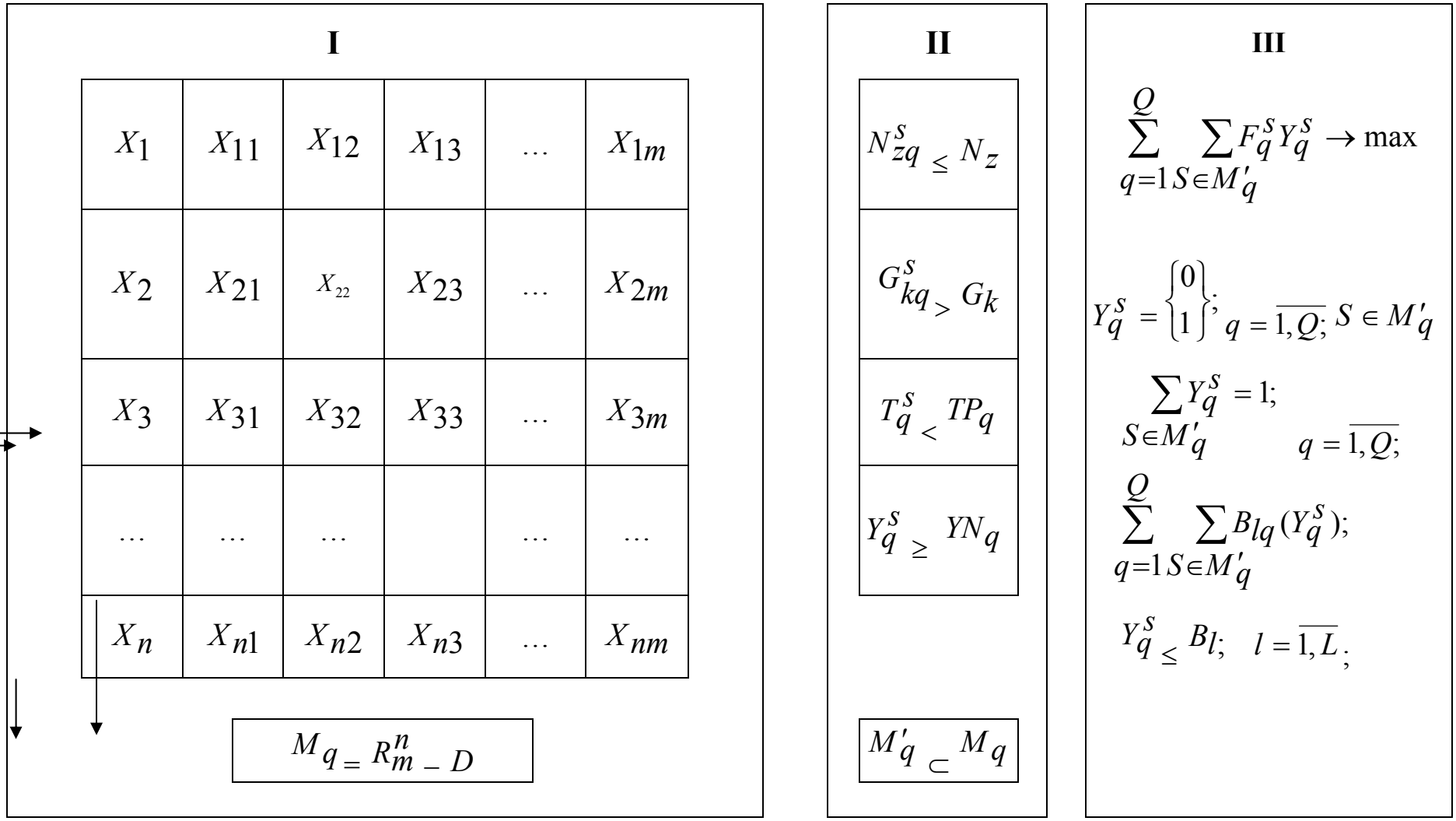


Рис. 2.3. Схема оптимізації прогресивності корпоративної політики інформаційної безпеки

Джерело: укладено автором

При цьому використані такі умовні позначення:

I – етап формування множини технічно та організаційно здійсненних варіантів структури корпоративної політики інформаційної безпеки;

II – етап аналізу соціально-економічних, тимчасових та якісних характеристик варіантів і формування підмножини допустимих варіантів структури корпоративної політики інформаційної безпеки;

III – етап визначення кращого варіанта структури корпоративної політики інформаційної безпеки;

X_i – параметр, що характеризує елемент корпоративної політики інформаційної безпеки;

X_{ij} – можливі значення елемента за варіантом i по варіанту j $j = \overline{1,m}$;

S – варіант структури корпоративної політики інформаційної безпеки;

R_m^n – число можливих варіантів структури корпоративної політики інформаційної безпеки;

Mq – безліч технічно та організаційно здійсненних варіантів корпоративної політики інформаційної безпеки, призначеної для задоволення потреби q;

D – число технічно та організаційно не здійсненних варіантів структури корпоративної політики інформаційної безпеки;

N_{zq}^s – інтенсивність виникнення негативного соціально-екологічного наслідку z у разі задоволення потреби q за допомогою варіанта системи s;

Nz – нормативна інтенсивність виникнення негативного соціально-екологічного наслідку z;

G_{kq}^s – інтенсивність виникнення позитивного соціально-екологічного наслідку у разі задоволення потреби q за допомогою варіанта системи s;

G_k – нормативна інтенсивність виникнення позитивного соціально-екологічного наслідку k;

T_q^s – тривалість періоду, протягом якого може бути задоволена потреба q у разі використання варіанта системи s;

TP_q – планова тривалість періоду, протягом якого може бути задоволена потреба q;

Y_q^s – показник, що характеризує якість задоволення потреби q за допомогою варіанта системи s;

YN_q – нормативний (плановий) показник якості задоволення потреби q;

$M'q$ – підмножина допустимих варіантів системи, призначеної для задоволення потреби q;

F_q^s – ефект задоволення потреб q за допомогою варіанта системи s;

Y_q^s – булева змінна, що показує, чи застосовується для задоволення потреби q варіант системи s;

Q – число потреб, що задовольняються корпоративною політикою інформаційної безпеки;

$B_{lq}(Y_q^s)$ – потреба у засобах розширення ресурсів виду l для задоволення потреб виду q умовах Y_q^s;

B_l – загальний обсяг засобів розширення ресурсів виду l;

L – число видів засобів розширення ресурсів корпоративної політики інформаційної безпеки.

Отриманий варіант прогресивності корпоративної політики інформаційної безпеки відповідає такому критерію, завдяки якому корпоративна структура має можливість забезпечити своєчасне та якісне задоволення потреб суспільства, що розвивається, з мінімальними сукупними витратами живої та уречевленої праці при обов'язковому дотриманні соціальних умов, вимог до стану довкілля та обмежень засобів розширення ресурсів корпорації.

Розглянута схема пошуку кращої прогресивності корпоративної політики інформаційної безпеки виходить із можливості формування множини. З цього випливає, що саме це завдання є найскладнішим. Складність полягає не так у тому, щоб знайти вид параметрів і значень, які адекватно відображають стан того чи іншого елемента корпоративної політики інформаційної безпеки, як у можливості пов'язання цих параметрів та їх поєднань з факторами, що характеризують вплив на них системи вищого порядку, частиною якої є сама корпоративна структура.

У зв'язку з цим формування прогресивності корпоративної політики інформаційної безпеки перетворюється на процес приведення у відповідність ступеня розмаїття напрямів та інструментів реалізації корпоративної політики інформаційної безпеки та оптимальної гнучкості її елементів. Створення таких систем можливе лише на основі:

– дослідження динаміки цілей корпоративної політики інформаційної безпеки на перспективу, обумовлених необхідністю найбільш повного, своєчасного та якісного задоволення постійно змінюваних потреб ринку;

– прогнозування можливостей оснащення процесу реалізації корпоративної політики інформаційної безпеки технічно та програмно сумісними засобами виробництва й забезпечення їх відповідними матеріальними, інформаційними, технологічними та трудовими ресурсами;

– моделювання оптимальної структури напрямів та інструментів корпоративної політики інформаційної безпеки, що забезпечує досягнення максимально можливого потенційного стратегічного ефекту гнучкого реагування на зміну цілей діяльності корпоративних структур в умовах обмежень засобів розширення ресурсів системи та всебічного обліку впливу на прогресивність корпоративної політики інформаційної безпеки зовнішнього середовища.

Список бібліографічних посилань

1. Конституція України : Основний Закон України від 28.06.1996 № 254к/96-ВР. Дата оновлення: 01.01.2020. URL : http://zakon3.rada.gov.ua/laws/show/254 %D0 %BA/96-%D0%B2 %D1%80 (дата звернення: 17.06.2022).

2. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 № 537-V. Дата оновлення: 06.02.2007. URL : https: //zakon. rada. gov.ua/laws/show/537-16#Text (дата звернення: 13.06.2022).

3. Домарєв В. В. Обґрунтування основних функцій системи управління інформаційною безпекою // Вісник Державного ун-ту інформаційно-комунікаційних технологій. 2012. Т. 10, № 2. С. 102–104.

4. Антонюк В. В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України : дис. канд. наук з держ. управл.: 25.00.02 ; Національна академія державного управління при президентові України. Київ, 2017. С. 57–59.

5. Страхарчук А. Я., Страхарчук В. П. Інформаційні системи і технології в банках : навч. посіб. Київ : УБС НБУ : Знання, 2010. 515 с.

6. Бодюл Є. М. Інформаційна безпека банку // Протидія злочинам, які вчиняються з використанням комп'ютерних мереж : тези доповідей Міжн. науково-практ. конференції (м. Севастополь, 1–2 жов. 2010 р.) / Державний вищий навч. заклад «Українська академія банківської справи Національного банку України». Суми : ДВНЗ «УАБС НБУ», 2010.

7. Хохлачова Ю. Політика інформаційної безпеки об'єкта // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2012. Вип. 2 (24).

8. Визначення та обґрунтування суті політики інформаційної безпеки / М. Ф. Бондаренко, О. В. Потій, Ю. І. Горбенко та ін. // Радіотехніка. 2003. № 134. С. 9–25.

9. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання. Київ : ВД «Гельветика», 2017. 168 с.

10. Валіулліна З. В. Інформаційна безпека корпоративної економіки в умовах глобалізаційних процесів // Вісник Дніпропетровського ун-ту. Серія «Менеджмент інновацій». 2016. Вип. 6. С. 34–41.

11. Черевко О. В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту. *Ефективна економіка*. 2014. № 5. URL : http:// nbuv. gov.ua/UJRN/efek_2014_5_103 (дата звернення: 17.06.2022).

12. Жабинець О. Й. Політика інформаційної безпеки страхових компаній: українські реалії та досвід США. *Проблеми економіки*. 2014. № 4. С. 22–27.

13. Шилов М. С. Жевелєва І. С. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. допов. наук.-практ. конф. (Київ, 26 березня 2021 р.). Київ : НА СБУ, 2021. С. 325.

14. Бакай В. Й., Зима В. М. Нові виклики та особливості створення системи інформаційної безпеки підприємства // Вісник Хмельницького Нац. ун-ту. 2020. № 5. С. 19–22.

15. Kim S. H., Wang Q.-H., Ullrich J. B.. A Comparative Study of Cyberattacks // Communications of the ACM. 2012. № 55:3. P. 66.

16. Beebe N. L., Rao V. S. Improving Organizational Information Security Strategy Via MesoLevel Application of Situational Crime Prevention to the Risk Management Process // Communications of the Association for Information Systems. 2010. № 26:17. P. 329–358.

17. Park S., Ruighaver T. Strategic Approach to Information Security in Organizations // ICISS. International Conference on Information Science and Security. IEEE, 2008. P. 26–31.

18. Hong K.-S., Chi Y.-P., Chao L., Tang J.-H. An Integrated System Theory of Information Security Management // Information Management & Computer Security. 2003. № 11:5. P. 243–248.

19. Flores W. R., Antonsen E., Ekstedt, M. Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture // Computers & Security. 2014. № 43. P. 90–110.

20. Carcary M., Renaud K., McLaughlin S., O'Brien C. A framework for information security governance and management // IT Professional. 2016. Vol. 18. № 2. P. 22–30.

21. Soomro Z. A., Shah M. H. Ahmed J. Information security management needs more holistic approach: a literature review // International Journal of Information Management. 2016. Vol. 36. № 2. P. 215–225.

22. Hasbini M. A., Eldabi T., Aldallal, A. Investigating the information security management role in smart city organisations // World Journal of Entrepreneurship, Management and Sustainable Development. 2018. Vol. 14. № 1. P. 86–98.

23. Georg L. Information security governance: pending legal responsibilities of non-executive boards // Journal of Management and Governance. 2017. Vol. 21. № 4. P. 793–814.

24. Goel S., Shawky H. A. Estimating the market impact of security breach announcements on firm values // Information and Management. 2009. Vol. 46. № 7. P. 404–410.

25. Gillon K., Branz L., Culnan M.J., Dhillon G., Hodgkinson R., MacWillson A. Information security and privacy-rethinking governance models // Communications of the Association for Information Systems. 2011. Vol. 28. P. 33.

26. Вьуькцzkan G., Gцзer F. Digital supply chain: literature review and a proposed framework for future research // Computers in Industry. 2018. Vol. 97. P. 157–177.

27. Rothrock R. A., Kaplan J., Van D. O. The board's role in managing cybersecurity risks // MIT Sloan Management Review. 2018. Vol. 59. № 2. P. 12–15.

28. Ahmad A., Maynard S. B., Shanks G. A Case Analysis of Information Systems and Security Incident Responses // International Journal of Information Management. 2015. № 35:6. P. 717–723.

29. Desouza K. C., Ahmad A., Naseer H., Sharma M. Weaponizing Information Systems for Political Disruption: The Actor, Lever, Effects, and Response Taxonomy (Alert) // Computers & Security. 2020. P. 101606.

30. Oertwig N., Galeitzke M., Schmieg H.G., Kohl H., Jochem R., Orth R.; Knothe T. Integration of Sustainability into the Corporate Strategy. In Sustainable Manufacturing, Challenges, Solutions and Implementation Perspectives. Berlin, Heidelberg : Springer, 2017. P. 175–200.

31. Teece D.J. Business models and dynamic capabilities // Long Range Plan. 2018. № 51. P. 40–49.

32. Bouncken R. B., Gast J., Kraus S., Bogers M. () Coopetition: a systematic review, synthesis, and future research directions // RMS. 2015. № 9(3). P. 577–601.

33. ClauЯ T., Bouncken R.B., Laudien S., Kraus S. Business model reconfiguration and innovation in SMEs: a mixed-method analysis from the electronics industry // Int J Innov Manag. 2019. https://doi.org/10.1142/S1363919620500152.

2.3. Економічна ефективність управління корпоративною інформаційною безпекою: критерії та показники

Управління корпоративною інформаційною безпекою є надзвичайно складним процесом з кількох 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, а точніше, наявним бюджетом. Тому що, як би гостро не стояло питання захисту інформації, підприємство не може витрачати необмежені фінансові ресурси на його організацію, а важливим принципом (виокремленим нами раніше) є забезпечення економічної ефективності корпоративної інформаційної безпеки. У зв'язку з цим постає актуальне питання, яким чином вимірювати економічну ефективність управління корпоративною інформаційною безпекою.

Процес вимірювання економічної ефективності управління корпоративною інформаційною безпекою стикається з низкою методологічних перешкод:

1) отриманий дохід, або прибуток, який оцінюється як непонесений (відвернений) збиток, завжди є складно і неточно детермінованим показником;

2) витрати на забезпечення інформаційної безпеки є різнорідними та з погляду бухгалтерського обліку належать до різних періодів: частина цих витрат носить капітальний, тобто інвестиційний характер, а частина – поточний;

3) окремий ефект у захисті корпоративної інформації може досягатись за рахунок еволюційних змін процесів, які не мають 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. Часто це потребує специфічних налаштувань у системі збирання інформації та введення додаткових звітів в системі управлінського обліку.

Незважаючи на ці перешкоди, науковці не припиняють спроб сформулювати підходи до оцінювання такої ефективності. Зазначеній проблемі присвячено багато праць [1–26]. Вивчення джерел з відповідної тематики дозволило нам виокремити **три** принципові підходи до обґрунтування показників оцінювання економічної ефективності управління корпоративною інформаційною безпекою підприємства:

– перший – спрямований на оцінювання одного показника ефективності корпоративної інформаційної безпеки;

– другий ґрунтується на оцінюванні ефективності інвестицій у забезпечення корпоративної інформаційної безпеки;

– третій підхід передбачає оцінювання низки показників ефективності, які характеризують різні аспекти корпоративної інформаційної безпеки.

Перший підхід, на наш погляд, найбільш послідовно представлений у працях А. В. Бєгуна [1–4].

Так, автор економічну ефективність безпеки розуміє як відношення відвернутого збитку до витрат на її забезпечення [4]. Але, на його думку, відвернутий збиток – це не єдиний результат діяльності системи безпеки, з огляду на те, що 100 % захисту неможливо досягти, а отже, існує залишковий ризик реалізації загрози, який прогнозує можливість збитку – від'ємного результату. Таким чином, ефектом дій із забезпечення ІБ, на думку А. В. Бєгуна, є відвернутий та понесений збиток у вартісному вигляді. З огляду на це автор пропонує таку формулу оцінювання ефекту від інформаційної безпеки (2.6):

$$E = (U_1 - U_2) / Z_0, \qquad (2.6)$$

де U_1 – відвернутий збиток, тобто можливий збиток у результаті атаки на інформаційну систему;

U_2 – збиток від реалізації атаки на інформаційну систему;

Z_0 – витрати на забезпечення інформаційної безпеки.

Враховуючи формулу $U_2 = U_{2.1} + U_{2.2}$ ($U_{2.1}$ – прямі збитки, $U_{2.2}$ – непрямі збитки), розрахунок E має такий вигляд:

$$E = (U_1 - U_2) / (Z_1 + Z_2 + Z_3), \qquad (2.7)$$

де Z_1 – витрати на формування політики інформаційної безпеки;

Z_2 – витрати на коригування та вдосконалення політики інформаційної безпеки;

Z_3 – витрати, які пов'язані з наслідками порушення політики інформаційної безпеки.

Науковець пропонує враховувати страхування залишкового інформаційного ризику: величина страхового внеску (s) збільшить величину витрат (Z_0), а страхові виплати у разі настання страхової події (S) зменшать розмір збитку(U_2):

$$E = (U_1 - U_2 + \mathrm{S}) / (Z_0 + s). \qquad (2.8)$$

Оптимізація загального економічного ефекту від інформаційної безпеки, на думку автора, досягається за таких умов:

$$\begin{cases} U_1 \rightarrow \max \\ U_2 \rightarrow \min \\ Z_0 \rightarrow \min. \end{cases} \quad (2.9)$$

При цьому А. В. Бєгун слушно зазначає, що максимізація відвернутого та мінімізація понесеного (залишкового) ризику мають відбуватися в комплексі, а мінімізація витрат на підтримку інформаційної безпеки бути розумною.

Окрім абсолютного економічного ефекту, автор пропонує оцінювати вартість збереженого та збільшеного інформаційного ресурсу (C) та співвідносити його з витратами на забезпечення інформаційної безпеки. Для цього пропонується така формула:

$$E^* = C / Z_0. \quad (2.10)$$

Зазначимо, що дослідник чітко не визначає сутність збереженого інформаційного ресурсу, але з контексту можна припустити, що це не що інше, як відвернений збиток.

Для узагальнюючої характеристики рівня ефективності інформаційної безпеки автор пропонує оцінювати простий показник рентабельності витрат на інформаційну безпеку, зазначаючи, що «сума надлишкового інформаційного ресурсу повинна мати певний рівень кореляції з показниками чистого прибутку підприємства або можливості його отримання». При цьому не розкривається зміст поняття «надлишкового інформаційного ресурсу» та яким чином вимірювати «можливість отримання прибутку» [4].

У цілому погоджуючись з окремими ідеями представленого підходу, а саме необхідністю оцінювання відверненого збитку, наявності залишкового інформаційного ризику, співвіднесення цих показників з понесеними витратами на інформаційну безпеку, необхідності підтримання рентабельної діяльності підприємства, на нашу думку, підхід має ряд методологічних недоліків.

По-перше, окремі показники чітко не окреслені автором, зокрема «вартість збереженого та збільшеного інформаційного ресурсу», «надлишковий інформаційний ресурс», що дещо ускладнює розуміння окремих складових методики.

По-друге, автор не вказує, за який часовий період варто оцінювати запропоновані показники. Якщо припустити, що їх оцінювання здійснюється за результатами року і до складу витрат на інформаційну безпеку автор відносить і інвестиційні, й поточні витрати періоду, то методика є дискусійною з позицій дотримання принципів інвестиційного аналізу: інвестиційні витрати зазвичай генерують вигоди із запізненням, а не в межах періоду інвестування, тож отриманий ефект в наступні роки буде порівняно з заниженими витратами, що суттєво знижує об'єктивність оцінки.

По-третє, методика має статичний характер, не враховуючи різну вартість грошей у часі, тобто інвестиційні витрати та отримані вигоди відносяться до різних часових періодів і їх порівняння має передбачати приведення вартостей до одного часового горизонту.

Таким чином, на нашу думку, застосування цієї методики на практиці є досить проблематичним.

У межах першого підходу низкою авторів пропонується застосовувати як критерії ефективності системи організації інформаційної безпеки показник сукупної вартості володіння (англ. *Total Cost of Ownership*, *TCO*) [5–11].

Сукупна вартість володіння, або вартість життєвого циклу, – це загальна величина цільових витрат (прямих та непрямих), які вимушений нести власник з моменту вступу в право власності на певний продукт чи систему до моменту виходу з права власності та виконання власником зобов'язань, пов'язаних з володінням, у повному обсязі. Методика розрахунку сукупної вартості володіння була розроблена у 1987 р. компанією «Gartner Group» з випрацювання рішень у сфері інформаційних технологій з метою точного розрахунку фінансових витрат, пов'язаних з володінням і експлуатацією комп'ютерних мереж.

У 1994 р. компанія «Interpose» здійснила вдосконалення моделі, що перетворило її на повноцінну модель аналізу фінансової сторони використання ІТ-рішень. Зазвичай розгортання ІТ-рішення може передбачати включення у склад ТСО таких складових: **апаратні та програмні складові** мережеве обладнання та апаратна частина; серверне обладнання та програмне забезпечення; апаратне та програмне забезпечення для робочих станцій; встановлення та інтеграція апаратного і програмного забезпечення; дослідження у галузі закупівель; придбання гарантій та ліцензій; витрати на міграцію баз даних; ризики – уразливість, наявність оновлень та патчів; **операційні витрати**: інфраструктура (необхідна площа, підведення комунікацій); електрика для забезпечення роботи обладнання, охолодження, резервні потужності; витрати на тестування; збитки від простою, відключень та відмов обладнання; зниження продуктивності (наприклад, користувачі змушені чекати виконання задачі, що негативно впливає на потенційні доходи); безпека (порушення безпеки, завдання шкоди репутації, відновлення та запобігання інцидентам безпеки); процес резервного копіювання та відновлення; навчання допоміжного персоналу; аудит внутрішній та зовнішній; страхування; витрати на персонал (зарплата та супутні витрати); **довгострокові витрати:** заміна обладнання; переміщення обладнання; майбутнє оновлення або масштабованість витрат; виведення з експлуатації.

При цьому різні науковці обґрунтовують власні підходи щодо уточнення складу витрат, які включаються до сукупної вартості володіння. Такі методики представлені у роботах А. А. Рибидайла зі співавторами, В. В. Луговця та Л. Ю. Гальчинського Ознайомлення з методиками цих авторів дало змогу зробити такий висновок:

– методика за основними статтями обчислення витрат корелює з даними бухгалтерського обліку (лише окремі позиції витрат не фіксуються в регістрах бухгалтерського обліку і потребують додаткових спостережень та оцінок), що суттєво спрощує її застосування;

– методика має статичний характер, тобто оцінюються річні витрати (як інвестиційні – на основі амортизації, так і поточні) без урахування різних механізмів фінансування цих витрат та їх розподілу в часі.

Другий підхід до оцінювання ефективності корпоративної інформаційної безпеки ґрунтується на вимірюванні ефективності інвестицій у забезпечення корпоративної інформаційної безпеки [12–21].

Він передбачає застосування стандартних показників ефективності інвестиційних проєктів, зокрема чистої теперішньої вартості (*NPV*), внутрішньої норми дохідності (*IRR*), модифікованої внутрішньої норми дохідності (*MIRR*), індексу дохідності (*PI*).

Цей підхід характеризується методологічною коректністю, оскільки дотримується базових принципів інвестиційного аналізу, проте, на нашу думку, його не можна вважати комплексним. Він враховує лише ефективність управління інформаційною безпекою на стратегічному контурі, а заходи, що реалізуються на оперативно-тактичному рівні, випадають з контексту оцінювання.

Третій підхід передбачає розрахунок певного комплексу показників, які віддзеркалюють як економічні аспекти ефективності інформаційної безпеки, так і неекономічні. Зокрема, такі підходи представлені в роботах А. В. Велігури [22], М. Ю. Журавля [23] та багатьох інших. Так, Д. В. Дячков на основі розвитку роботи А. В. Велігури пропонує для оцінювання інформаційної безпеки застосовувати показники, що наведені у табл. 2.11.

Таблиця 2.11

Показники оцінки корпоративної інформаційної безпеки

Показник	Коротка характеристика
Оцінка програмно-технічної захищеності інформації	
Коефіцієнт фінансування програмної захищеності інформації	Співвідношення вартості програмного забезпечення, яке застосовується для створення інформаційного захисту, до загальних витрат на інформаційну безпеку

Продовження табл. 2.11

Показник	Коротка характеристика
Коефіцієнт фінансування технічної захищеності інформації	Співвідношення вартості технічного забезпечення, яке застосовується для створення інформаційного захисту, до загальних витрат на інформаційну безпеку
Коефіцієнт технічного захисту інформації	Співвідношення кількості відвернутих інформаційних атак до загальної кількості інформаційних атак за певний проміжок часу
Коефіцієнт програмної захищеності інформації	Співвідношення часу безперебійного функціонування корпоративної інформаційної системи до нормативного часу функціонування корпоративної інформаційної системи
Коефіцієнт фінансування програмно-технічної захищеності інформації	Співвідношення витрат на програмно-технічний захист інформаційних ресурсів до витрат на придбання інформаційних ресурсів
Коефіцієнт фінансування інформаційних служб підприємства	Співвідношення витрат утримання інформаційної служби підприємства до загальних витрат підприємства
Коефіцієнт автоматизації програмно-технічної захищеності інформації	Співвідношення автоматизованих процесів, спрямованих на програмно-технічний захист інформації до загальної кількості процесів, спрямованих на програмно-технічний захист інформації
Оцінка витрат на забезпечення інформаційної безпеки	
Коефіцієнт фінансування інформаційної безпеки	Співвідношення витрат на забезпечення інформаційної безпеки підприємства до загальних витрат підприємства
Коефіцієнт фінансування інформаційної безпеки, що забезпечує фінансовий напрям діяльності підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист фінансової діяльності підприємства, до витрат на забезпечення інформаційної безпеки підприємства
Коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист фізичних об’єктів підприємства, до витрат на забезпечення інформаційної безпеки підприємства
Коефіцієнт фінансування інформаційної безпеки, що забезпечує захист персоналу підприємства	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист персоналу підприємства, до витрат на забезпечення інформаційної безпеки підприємства

Продовження табл. 2.11

Показник	Коротка характеристика
Оцінка інформаційної надійності персоналу	
Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства	Співвідношення чисельності працівників, які мають доступ до комерційної таємниці (баз даних, банків даних тощо), що працюють на підприємстві більше одного року, до загальної чисельності працівників, які мають доступ до комерційної таємниці (баз даних, банків даних тощо)
Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства	Співвідношення чисельності працівників, звільнених з причини витоку інформації, до загальної чисельності звільнених працівників
Коефіцієнт підготовленості персоналу до розпізнавання загроз інформаційній безпеці	Співвідношення чисельності, ненавмисні дії яких призвели до витоку інформації через низький рівень компетентності персоналу та невміння розпізнавання загроз інформаційній безпеці, до загальної чисельності працівників, які мають доступ до закритої інформації
Коефіцієнт правової захищеності інформації	Співвідношення обсягу інформації, розголошення якої може спричинити негативні наслідки для підприємства, до загального обсягу юридично захищеної інформації
Коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку	Співвідношення інформаційних загроз (інформаційних атак), які відвернуті через дії персоналу, котрий забезпечує інформаційну безпеку, до загальної кількості інформаційних атак за певний проміжок часу
Оцінка інформації, що надається особам, які приймають рішення, інформаційною службою підприємства	
Коефіцієнт повноти інформації	Співвідношення обсягу інформації, що є в розпорядженні ОПР, до обсягу інформації, необхідної для ухвалення обґрунтованого рішення
Коефіцієнт точності інформації	Співвідношення обсягу релевантної інформації до загального обсягу наявної в розпорядженні ОПР інформації
Коефіцієнт суперечливості інформації	Співвідношення кількості незалежних свідчень на користь ухвалення рішення до загальної кількості незалежних свідчень у сумарному обсязі релевантної інформації

Закінчення табл. 2.11

Показник	Коротка характеристика
Коефіцієнт своєчасності надання інформації	Співвідношення обсягу своєчасно наданої ОПР інформації до обсягу інформації, необхідної для ухвалення обґрунтованого рішення
Коефіцієнт надійності інформації	Співвідношення обсягу інформації, наданої ОПР з перевірених джерел, до загального обсягу наданої ОПР інформації
Оцінка системи захисту інформації	
Ступінь інформаційного ризику	відсоток втрат (у грошову вираженні) спричинених пошкодженням інформаційної цілісності підприємства
Гнучкість системи інформаційної безпеки підприємства	Здатність системи управління інформаційною безпекою швидко адаптувати організаційну побудову до зовнішніх та внутрішніх потреб
Коефіцієнт керованості системи інформаційної безпеки підприємства	Співвідношення компетентностей керівного персоналу системи інформаційної безпеки до загальних компетентностей, якими повинен володіти керівник відповідного рівня
Частка програмного забезпечення, розробленого працівниками підприємства, яке задіяне для забезпечення інформаційної безпеки підприємства	
Частка технічних засобів, розроблених працівниками підприємства, яке задіяне для забезпечення інформаційної безпеки підприємства	

Джерело: [24]

Зазначений підхід, на нашу думку, можна охарактеризувати таким чином:

– має комплексний характер та передбачає певну систематизацію показників (зокрема, за елементами ресурсного забезпечення інформаційної безпеки), що дає можливість виявляти «слабкі місця» в організації та причини зниження рівня безпеки та її ефективності;

– методика певною мірою переобтяжена за кількістю показників, тому доцільність оцінювання окремих з них є досить дискусійною з точки зору їх значимості та відповідності принципу «розумної доцільності». Наприклад, групу показників, що характеризують інформацію для прийняття рішень, досить складно оцінювати з огляду на те, що такі поняття, як «релевантна інформація», «необхідна інформація

для ухвалення рішення», «кількість незалежних свідчень» можуть мати досить суб'єктивний характер, а тому у підсумку зазначені коефіцієнти не надаватимуть об'єктивної оцінки як рівня інформаційної безпеки, так і її ефективності. Такі показники, як коефіцієнт досвіду роботи, надійності, підготовленості персоналу, правової захищеності інформації у представленій інтерпретації, на нашу думку, не є показовими для оцінювання безпеки та її ефективності, тому витрачання ресурсів на ведення звітності, необхідної для оцінювання таких показників, може призводити до непродуктивних витрат із забезпечення інформаційної безпеки. До складно оцінюваних показників також можна віднести гнучкість системи інформаційної безпеки, адже абсолютно незрозуміло, як оцінити «здатність системи управління інформаційною безпекою швидко адаптувати організаційну побудову до зовнішніх та внутрішніх потреб»;

– методика не містить класичних показників ефективності. Важливим принципом забезпечення інформаційної безпеки є її економічна ефективність, тому, на нашу думку, система показників оцінювання КІБ має включати такі індикатори;

– невизначеність критеріїв оцінювання ускладнює інтерпретацію результатів аналізу, а відсутність інтегрального, або узагальнювального показника унеможливлює ідентифікацію рівня інформаційної безпеки підприємства в цілому.

Таким чином, вивчення сучасних підходів до оцінювання ефективності КІБ дало змогу, по-перше, зробити висновок про складність застосування єдиної методики з описаних вище для формування вичерпного висновку щодо ефективності КІБ, а по-друге, виявити ряд проблем, які потребують вирішення:

– обґрунтування принципів оцінювання та систематизації показників економічної ефективності;

– визначення чітких критеріїв оцінювання окремих показників;

– обґрунтування рекомендацій щодо логічної послідовності аналізу окремих показників;

– формування інтегрального, або узагальнювального показника ефективності КІБ.

На основі дослідження змісту корпоративної інформаційної безпеки, механізмів та специфічних особливостей її забезпечення ми пропонуємо виокремити такі принципи оцінювання економічної ефективності та систематизації показників:

1. Принцип помірної деталізації. Процеси забезпечення корпоративної інформаційної безпеки, не створюючи безпосередньо доданої вартості, досить витратні, тому формування переобтяженої системи показників, їх надмірна деталізація та рубрикація сприяє зростанню витрат на її впровадження в практичну діяльність. З іншого боку, деталізація показників за ресурсною складовою або за елементами корпоративного інформаційного поля тощо, на наш погляд, не дасть належного аналітичного ефекту (порівняно з понесеними на це витратами) з огляду на те, що ефект від заходів захисту інформації є результатом комплексного використання ресурсів, який досить складно розмежовувати за окремими компонентами.

2. Принцип орієнтації на контур управління та часовий горизонт реалізації заходів безпеки. На нашу думку, виправданим є поділ показників ефективності на такі, що відповідають стратегічному контуру управління та оперативно-тактичному, що пов’язано з різним механізмом фінансування витрат на такі заходи.

3. Принцип ієрархічності, який передбачає виокремлення основних та допоміжних показників ефективності, що дає змогу виокремлювати різні рівні аналізу та поглиблювати оцінку окремих аспектів ефективності.

4. Принцип комбінації методів аналізу. З огляду на складність та багатогранність поняття КІБ складно обійтись одним методом аналізу у вимірюванні її економічної ефективності, про що свідчить і полеміка з цього приводу в сучасних дослідженнях. Тому розумна комбінація аналітичних методів сприятиме підвищенню об’єктивності оцінювання.

5. Принцип логічної структурованості порядку оцінювання окремих показників, що дозволить при комплексному застосуванні набору аналітичних індикаторів, котрі ґрунтуються на використанні різних методів аналізу, поглиблювати результати попередніх оцінок.

На основі визначених принципів, узагальнення та розвитку наявних підходів до оцінювання ефективності КІБ пропонується до використання така система показників (табл. 2.12).

Таблиця 2.12

Система показників економічної ефективності корпоративної інформаційної безпеки

Показники	Основні	Допоміжні
Стратегічні	Чиста теперішня вартість (*NPV*) (>0; ↑); Внутрішня норма дохідності (*IRR*) (>r; ↑); Модифікована внутрішні норма дохідності (*MIRR*) (>r; ↑); Індекс дохідності (*PI*) (>1;↑)	Рентабельність інвестицій у КІБ (*Ri*) (↑); Капіталомісткість відверненої кібератаки (*K*)* (↓); Коефіцієнт віддачі навчання персоналу (*Ep*)* (↓); Частка програмного забезпечення, розробленого працівниками підприємства, яке задіяне для забезпечення інформаційної безпеки підприємства (*Qp*)(↑); Частка технічних засобів (*Qt*), розроблених працівниками підприємства, яке задіяне для забезпечення інформаційної безпеки підприємства (↑)
Оперативно-тактичні	Продуктивність інформаційної системи (*Pi*)* (↑); Рентабельність інформаційної системи (*Rinf*)* (↑); Віддача інформаційної системи (*Vinf*)* (↑);	Темп зростання кількості порушень регламентів передачі та зберігання інформації (*Tc*)* (↓); Темп зростання кількості інцидентів витоку конфіденційної інформації (*Ti*)* (↓); Темп зростання реалізованих поточних заходів із удосконалення інформаційних процесів (*Td*)* (↑)

** Запропоновано автором*

Джерело: розвинено та доповнено автором за [14–16, 22, 24]

Важливим аспектом у оцінюванні стратегічної економічної ефективності КІБ є оцінювання основних абсолютних показників, які є основою для розрахунку відносних основних індикаторів економічної ефективності КІБ. Зокрема, додаткового чистого грошового потоку від інвестицій, суми інвестиційних витрат на формування КІБ та вартості володіння.

Фактичним кінцевим результатом впровадження засобів щодо забезпечення КІБ можна вважати розмір (у грошовому еквіваленті), що відповідає попереджуваним втратам (попереджуваній шкоді від кібератак). Цей параметр (D) можна формалізувати таким чином:

$$D = D' - D'', \tag{2.11}$$

де D' та D'' – можливий збиток від атак до і після впровадження засобів і заходів з ІБ відповідно.

Використання зазначеного підходу передбачає таку послідовність дій для моделювання (наприклад, імітаційного) розміру попереджуваної шкоди від кібератак:

Крок 1. Розбиваємо потенційні втрати (збитки) на групи. Як критерій такого розбиття можна застосовувати категорійний розподіл інцидентів ІБ за ступенем небезпеки для ОБІ, застосовуючи типові метрики ІБ [25].

Крок 2. На підставі наявної статистики кіберінцидентів по ОБІ та використовуючи СППР або експертів виконуємо оцінку значення величини втрат (попереджуваної шкоди) для кожного інциденту. Ця величина може варіюватися від мінімального (*min*) до максимального (*max*) значення. Подібний крок виконується як до, так і після реалізації заходів щодо посилення ІБ ОБІ.

Крок 3. Застосовуючи попередньо обраний закон розподілу, створити модель величини втрат (до і після впровадження заходів і засобів ІБ).

Крок 4. Розрахувати сумарне значення попереджуваної шкоди від кібератак на підставі попередніх кроків 1–3.

Крок 5. Розрахувати статистичні характеристики для величин, на основі яких була створена модель, а також підсумкові показники економічної ефективності впроваджених коштів і проведених заходів щодо посилення ІБ ОБІ.

Для візуалізації результату розрахунку доцільно побудувати гістограму розподілу результуючого значення попереджуваної шкоди від кібератак, або гістограму інтегрального відсотку розподілу попереджуваної шкоди від кібератак. Точний підбір закону розподілу сумарного результуючого значення попереджуваної шкоди від кібератак дозволить досить точно оцінювати ймовірні характеристики в будь-якому місці гістограми або по відношенню до інтервалу, який аналізується.

Таким чином, імовірнісна характеристика попереджуваної шкоди від кібератак може бути прийнята як обґрунтований критерій ефективності заходів, спрямованих на підвищення ІБ ОБІ [26].

Інвестиційні витрати на формування КІБ оцінюються на основі методології інвестиційного аналізу і включають витрати на придбання техніки, технологій, транспортування, монтаж, введення в експлуатацію, розроблення.

Крім інвестиційних витрат, ТСО включає всі поточні витрати на утримання та обслуговування інформаційних систем підприємства.

Отримані на підставі реалізації кроків 1–5 результати можна використовувати для будь-якого основного показника стратегічного контуру (*NPV, PI, IRR, MIRR*). Алгоритми оцінювання цих показників широко висвітлюються в спеціальній літературі.

Для уточнення оцінок ефективності корпоративної інформаційної безпеки, що забезпечується на стратегічному рівні, ми пропонуємо застосовувати коефіцієнт рентабельності інвестицій у КІБ як співвідношення середньорічного відверненого збитку до середньорічного обсягу інвестицій у КІБ, частку програмних та технічних засобів, розроблених у межах підприємства. Такий підхід обумовлюється тим, що

часто подібні розроблення обходяться дешевше підприємству, а з іншого боку – це відображає рівень високих компетентностей задіяного у забезпеченні КІБ персоналу. Важливим напрямом забезпечення КІБ є постійне вдосконалення компетентностей персоналу, задіяного в цьому процесі. Витрати на навчання та розвиток персоналу є поточними витратами, які мають стратегічний характер, оскільки віддача від них не є миттєвою. Тому показник ефективності навчання працівників, залучених до процесів формування КІБ, ми пропонуємо включити до системи допоміжних вимірників економічної ефективності КІБ стратегічного контуру управління. Також вважаємо за доцільне вимірювати капіталомісткість однієї кібератаки, яка дозволить зрозуміти порівнянність інвестиційних витрат із потенційними загрозами інформаційній безпеці підприємства.

У межах оперативно-тактичного контуру управління як основні показники пропонується використовувати коефіцієнти продуктивності, рентабельності, віддачі інформаційної системи, які обчислюються за показниками чистої виручки, чистого прибутку та відверненого збитку відповідно до середньорічної вартості володіння. Показники продуктивності та рентабельності ми вважаємо за потрібне оцінювати з огляду на те, що інформаційні процеси пронизують всі напрями діяльності підприємства, забезпечуючи здійснення операційної, фінансової, інвестиційної складової, а вдосконалення інформаційної системи КІБ має сприяти зростанню ефективності функціонування підприємства в цілому.

На оперативно-тактичному рівні пропонується оцінювати темпи зростання кількості інцидентів витоку конфіденційної інформації, заходів з поліпшення інформаційних процесів та порушення регламентів зберігання та передавання інформації. Не будучи за своєю природою класичними, зазначені допоміжні показники економічної ефективності надають уявлення про зміни якості політики КІБ.

Інтерпретація авторських показників, що пропонуються для оцінювання ефективності КІБ в межах стратегічного та оперативно-тактичного контурів управління, представлена в табл. 2.13.

Таблиця 2.13

Характеристика показників економічної ефективності корпоративної інформаційної безпеки

Показники	Коротка характеристика
Капіталомісткість відверненої кібератаки	Співвідношення середньорічних інвестиційних витрат на КІБ до кількості відвернених кібератак
Коефіцієнт віддачі навчання персоналу	Співвідношення приросту витрат на навчання персоналу інформаційних служб та служб безпеки до приросту кількості уникнених інформаційних атак
Продуктивність інформаційної системи	Співвідношення чистої виручки від реалізації до річної вартості володіння інформаційною системою
Рентабельність інформаційної системи	Співвідношення чистого прибутку до середньорічної вартості володіння інформаційною системою
Віддача інформаційної системи	Співвідношення відверненого збитку до середньорічної вартості володіння інформаційною системою
Темп зростання кількості порушень регламентів передання та зберігання інформації	
Темп зростання кількості інцидентів витоку конфіденційної інформації	
Темп зростання реалізованих поточних заходів із вдосконалення інформаційних процесів	

Джерело: розроблено автором

На основі сформованих часткових показників (табл. 2.12) пропонується до використання інтегральний показник економічної ефективності КІБ.

Його формування здійснюється за такими основними етапами:

На першому етапі формується матриця показників (матриця $\mathbf{X} = (X_{ij})$, де X_{ij} – значення j-го показника для i-го об'єкта), що включаються до інтегрального індикатора. До його складу ми зараховуємо *IP*, коефіцієнт продуктивності навчання персоналу, капіталомісткість кібератаки, продуктивність *IC*, рентабельність *IC*, темп зростання кількості порушень регламентів передавання та зберігання інформації,

темп зростання кількості інцидентів витоку конфіденційної інформації, темп зростання реалізованих поточних заходів із вдосконалення інформаційних процесів.

На другому етапі формується матриця стандартизованих значень показників X, тобто матриця $\boldsymbol{X}$ трансформується в матрицю $\boldsymbol{Z}$. Це обумовлено тим, що показники можуть мати різну природу і незрівнянні один з одним значення. Елементи матриці $\boldsymbol{Z}$ обчислюються за такою формулою:

$$Z_{ij} = \frac{x_{ij} - \overline{X_j}}{\sigma_i}, \tag{2.12}$$

де $\overline{X}_j$ – середнє значення показника;

σ_j – стандартне відхилення показника X.

На третьому етапі здійснюється диференціація ознак матриці спостережень та формуються точки-еталони. Необхідність такої диференціації обумовлена різним впливом часткових показників на економічну ефективність КІБ. У переліку запропонованих нами часткових показників показниками-стимуляторами є: індекс дохідності, продуктивність ІС, рентабельність ІС, темп зростання реалізованих поточних заходів із вдосконалення інформаційних процесів; а показниками дестимуляторами – коефіцієнт продуктивності навчання персоналу, капіталомісткість кібератаки, темп зростання кількості порушень регламентів передачі та зберігання інформації, темп зростання кількості інцидентів витоку конфіденційної інформації.

На основі здійсненого розподілу показників на стимулятори та дестимулятори формується точка-еталон, яка являє собою точку P_0 з координатами Z_{01}, Z_{02} і т. д.:

$$Z_{0j} = \max Z_{ij}, \text{якщо } j \in \mathbf{J} \tag{2.13}$$

$$Z_{0j} = \min Z_{ij}, \text{якщо } j \notin \mathbf{J}, \tag{2.14}$$

де J – множина показників-стимуляторів.

На четвертому етапі здійснюється розрахунок евклідової відстані (C_{i0}), яка становить собою відстань між окремими стандартизованими показниками та точками-еталонами (5):

$$C_{i0} = \sqrt{\sum_{j=1}^{n}(Z_{ij} - Z_{0j})^2}, \quad (2.15)$$

Отримані значення відстаней безпосередньо використовуються при розрахунку інтегрального показника.

На п’ятому етапі розраховують значення інтегрального показника (d_i):

$$d_i = 1 - \frac{C_{i0}}{C_0} \quad (2.16)$$

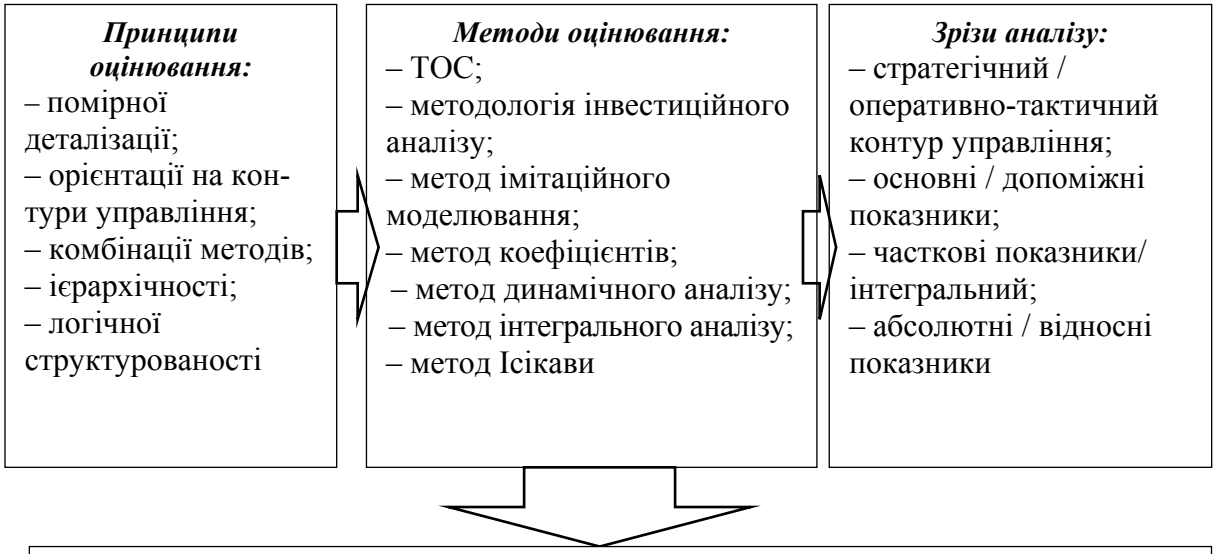
$$C_0 = \bar{C}_0 + 2 \times S_0 \quad (2.17)$$

$$\bar{C}_0 = \frac{\sum_{i=1}^{m} C_{i0}}{m} \quad (2.18)$$

$$S_0 = \sqrt{\frac{\sum_{i=1}^{m}(C_{i0} - \bar{C}_0)^2}{m}} \quad (2.19)$$

На шостому етапі формують висновок щодо рівня економічної ефективності КІБ та виявляють основні «слабкі місця» у її забезпеченні. Для цього може бути використаний метод Ісікави, який дає змогу поглиблювати аналіз шляхом якісного дослідження причин погіршення часткових показників, що беруть участь в оцінюванні інтегрального індикатора.

Таким чином, в узагальненому вигляді архітектуру оцінювання економічної ефективності КІБ можна представити таким чином (рис. 2.1).



1. Формування первинної інформаційної бази

2. Оцінювання основних абсолютних показників економічної ефективності КІБ (*ТОС, відвернений збиток, інвестиційні витрати*)

3. Оцінювання основних відносних часткових індикаторів економічної ефективності КІБ стратегічного контуру управління

4. Оцінювання допоміжних відносних часткових індикаторів економічної ефективності КІБ стратегічного контуру управління

5. Оцінювання основних відносних часткових індикаторів економічної ефективності КІБ оперативно-тактичного контуру управління

6. Оцінювання допоміжних відносних часткових індикаторів економічної ефективності КІБ оперативно-тактичного контуру управління

7. Оцінювання інтегрального показника економічної ефективності КІБ оперативно-тактичного контуру управління

8. Виявлення «слабких місць» у ефективності КІБ та їх причин

Рис. 2.4. Архітектура процесу оцінювання економічної ефективності КІБ

Джерело: розроблено автором

Запропонований підхід щодо оцінювання економічної ефективності КІБ ґрунтується на поєднанні методів ТОС, інвестиційного аналізу, імітаційного моделювання, коефіцієнтного, динамічного та інтегрального аналізу, методу Ісікави, окреслює чітку послідовність та логіку застосування запропонованих показників, деталізованих за контурами управління, ієрархічністю, що дає змогу структурувати та автоматизувати процес оцінювання економічної ефективності КІБ, здійснювати його на постійній основі. Результати його застосування є базою для подальшого вдосконалення як самого процесу формування КІБ, так і підвищення його економічної ефективності.

Список бібліографічних посилань

1. Бєгун А. В. Інформаційна парадигма безпеки економічної системи. *Моделювання та інформаційні технології в економіці*. 2011. № 83. С. 144–151.

2. Бєгун А. В. Аспектноорієнтована технологія оптимізації захисту додатків Web-порталу. *Моделювання та інформаційні технології в економіці*. 2010. № 81. С. 189–196.

3. Бєгун А. В. Модель оцінювання ефективності захисту інформаційних ресурсів банку // Сб. научн. труд. «Анализ, моделирование, управление, развитие экономических систем». Симферополь : ТНУ. 2012. С. 51–53.

4. Бєгун А. В. Оцінка економічної ефективності інформаційної безпеки підприємства. *Інвестиції: практика та досвід*. 2012. № 21. С. 35–36.

5. Модель процесно-орієнтованої оцінки ефективності впровадження інформаційних технологій для поліпшення управління адміністративно-господарчими процесами /

А. А. Рибидайло, І. Г. Зотова, О. С. Левшенко та ін. // зб. наук. пр. ЦВСД НУОУ. Київ, 2014. № 1 (50).

6. Тюріна Н. М., Параконний В. Т. Оцінка вартості та ефективності використання інформаційних систем управління на промислових підприємствах // Вісник Хмельницького Нац. ун-ту. Економічні науки. 2006. № 2. Т. 2. С. 22–27.

7. Andresen J. L. A Framework for Selecting an IT Evaluation Method: in the Context of Construction // Danmarks Tekniske Universitet, 2001. 257 p.

8. Cronk M. A., Fitzgerald E. Conceptual Framework for Furthering Understanding of ‹IT business value› and its Dimensions // PACIS 1997 Proceedings. 1997. P. 405–415.

9. Patel N. V., Irani Z. Evaluating information technology in dynamic environments: a focus on tailorable information systems // Logistics Information Management. 1999. Vol. 12. P. 32–39.

10. Remenyi D. Money A., Sherwood-Smith A. M. The Effective Measurement and Management of IT Costs and Benefits // Oxford : Butterworth-Heinemann. 2000. 362 p.

11. Луговець В. В., Гальчинський Л. Ю. Оцінка сукупної вартості володіння операційними системами в органах державної влади // Економічний вісник НТУУ «КПІ». 2017. № 14. С. 491–497.

12. Pieters W., Probst C. W., Lukszo Z., Montoya L. Cost-effectiveness of security measures: A model-based framework // In Approaches and processes for managing the economics of information systems. IGI global, 2014. P. 139–156.

13. Boiko A., Shendryk V., Boiko O. Information systems for supply chain management: uncertainties, risks and cyber security // Procedia computer science. 2019. № 149. P. 65–70.

14. Chronopoulos M., Panaousis E., Grossklags J. An options approach to cybersecurity investment // IEEE Access 2017. № 6. P. 12175–12186.

15. Hallman R. A., Major M., Romero-Mariona J., Phipps R., Romero E., Slayback S. M., San Miguel J. M. Determining a Return on Investment for Cybersecurity Technologies in Networked Critical Infrastructures // International Journal of Organizational and Collective Intelligence (IJOCI). 2021. № 11(2). P. 91–112.

16. Nagurney A., Shukla S. Multifirm models of cyber-security investment competition vs. cooperation and network vulnerability // European Journal of Operational Research. 2017. № 260 (2). P. 588–600.

17. Veksler V. D., Buchler N., Hoffman B. E., Cassenti D. N., Sample C., Sugrim S. Simulations in cyber-security: a review of cognitive modeling of network attackers, defenders, and users // Frontiers in psychology. 2018. № 9. P. 691.

18. Gonzalez C., Ben-Asher N., Morrison D. Dynamics of decision making in cyber defense: Using multi-agent cognitive modeling to understand cyberwar // In Theory and Models for Cyber Situation Awareness. Springer, Cham, 2017. P. 113–127.

19. Maqbool Z., Pammi V. C., Dutt V. Behavioral Cyber-security: Investigating the influence of Patching Vulnerabilities in Markov Security Games via Cognitive Modeling // IJCSA. 2019. № 4(1). P. 185–209.

20. Gordon L., Loeb M., Lucyshyn W. Information security expenditures and real options: A wait- and-see approach // Computer Security Journal. 2003. № 19 (2). P. 1–7.

21. Majd S, Pindyck R. Time to build, option value, and investment decisions // Journal of Financial Economics. 1987. № 1 (1). P. 7–27.

22. Велігура А. В. Оцінювання стану інформаційної безпеки підприємства // Управління проектами та розвиток виробництва: Зб. наук. пр. Луганськ : вид-во СНУ ім. В. Даля, 2014. № 4 (52). С. 28–39.

23. Журавель М. Ю., Полозова Т. В., Стороженко О. В. Формування системи показників оцінки рівня інформаційної безпеки підприємства // Вісник економіки транспорту і промисловості. 2011. № 33. С. 171–177.

24. Дячков Д. В. Методичні підходи до оцінки інформаційної безпеки підприємства. URL : http://dspace.pdaa.edu.ua:8080/bitstream/123456789/2572/1/СТАТТЯ_СУМИ_ДЯЧКОВ.pdf (дата звернення: 17.06.2022).

25. Gordon L., Loeb M., Lucyshyn W. Information security expenditures and real options: A wait-and-see approach // Computer Security Journal. 2003. № 19 (2). P. 1–7.

26. Ефективність методики розрахунку показників інвестицій в систему інформаційної безпеки об’єктів інформатизації / В. І. Чубаєвський, О. В. Криворучко, В. А. Лахно та ін. *Кібербезпека: освіта, наука, техніка*. 2021. № 4 (12). С. 96–105.

Розділ 3

ІНСТРУМЕНТИ ТА ЗАСОБИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Демаскувальні ознаки конфіденційних корпоративних даних

У міру зростання кількості злочинів у сфері незаконного (неправомірного) втручання в роботу інформаційних систем (ІС) проблематика виявлення та боротьба з несанкціонованим доступом (НСД) до інформаційних ресурсів стала однією з основних проблем для багатьох підприємств у всьому світі [1, 2]. Збільшення кількості комп'ютерних злочинів та зростання складності сценаріїв реалізації цільових (таргетованих) кібернетичних атак у США, державах ЄС та Азії [3, 4] змушують міжнародне співтовариство не лише шукати шляхи підвищення рівня інформаційної безпеки (ІБ) ІС на технічному та організаційному рівнях, а й удосконалювати законодавство у цій галузі.

По суті, в основі будь-якого комп'ютерного злочину лежить НСД до інформації, що обробляється, зберігається або передається в ІС суб'єктів економічної діяльності. Небезпеки, пов'язані з реалізацією нових сценаріїв отримання НСД до інформаційних ресурсів підприємств, зростають у міру того, як суб'єкти господарської діяльності впроваджують у свої бізнес-процеси нові інформаційні технології (ІТ), як-от, електронні платежі, системи електронного документообігу тощо. Зауважимо, що НСД нерідко лише випереджає інші злочини в економічній сфері, адже в умовах автоматизованого оброблення інформації зловмиснику необхідно отримати доступ до ресурсів ІС підприємств. Світовий та європейський досвід у сфері боротьби з комп'ютерними злочинами, що стосуються отримання НСД до ресурсів ІС підприємств, не новий. Наприклад, ще 1983 року за Ради Європи почала функціонувати експертна група, котра займається вивченням особливостей комп'ютерної злочинності [5].

Необхідно зазначити, що стрімкі темпи розвитку ІТ значно випереджають темпи реалізації нормативно-правової бази, котра регулює відповідальність за скоєні комп'ютерні злочини. Це, у свою чергу, ставить перед стороною захисту перманентне завдання, пов'язане з пошуком критеріїв безпеки, а також оцінкою ефективності систем захисту інформації (СЗІ).

У міру ускладнення сценаріїв проведення кібернетичних атак, особливо таргетованих, постійно розширюється і простір ознак, що характеризують способи отримання НСД до інформаційних ресурсів підприємств. З огляду на це навіть кваліфікованим експертам у сфері ІБ без підтримки спеціалізованих програмних продуктів при прийнятті рішення у подібних питаннях обійтися складно. Усе це зумовлює необхідність продовження досліджень у напрямі інтелектуалізації на основі інформаційних технологій процедури первинної формалізації неправомірних дій комп'ютерних зловмисників, які роблять спроби отримати НСД до ІС суб'єктів господарської діяльності.

У наукових працях [6, 7, 8] проаналізовано класифікаційні методи обґрунтування вимог до СЗІ. Проте, як зазначають автори, ці методи не позбавлені низки недоліків, зокрема, не дають змоги повноцінно реалізовувати синтез контурів ІБ при проєктуванні автоматизованих систем (АС).

Саме ця причина, на думку науковців [9, 10, 11], робить перспективним підхід, що базується на формалізації конфліктно-динамічних процесів, що відбуваються при НСД до ресурсів ІС. Такий підхід, на думку авторів цих досліджень, дозволяє ефективніше забезпечити вирішення завдання, пов'язаного з нормуванням вимог до ІБ підприємств. Проте, авторами [9, 11] не наведено практичних прикладів застосування викладеного підходу.

Розвитком формального підходу до опису динаміки НСД до ресурсів ІС можна вважати праці [12, 13], у яких авторами розвинено підхід, відповідно до якого для формалізації конфліктно-динамічних процесів під час НСД до ІС застосовано математичний апарат Марківських процесів. Але

недоліком такого підходу є та обставина, що необхідно у кожному конкретному випадку виробляти побудову графа, що описує алгоритм реалізації НСД до ІС. І хоч це дає дослідникам наочне уявлення про етапи реалізації атаки, проте водночас вимагає досить високої кваліфікації експерта з ІБ та витрат часу для побудови подібного графа.

Також зазначимо, що для конкретної ІС при композиційній побудові функціональної структури дій зловмисника, який реалізує процеси НСД до ІС, необхідно виконати формалізацію можливих неправомірних дій для обґрунтування простору ознак НСД.

Питанням опису простору ознак НСД до різноманітних інформаційних ресурсів присвячено досить багато досліджень. Наприклад, в [14] здійснено огляд та аналіз наявних методів забезпечення ІБ безпеки автоматизованих систем аутентифікації та розподілених мереж. Ця праця має оглядовий характер і конкретних рекомендацій не містить.

Автори інших розвідок акцентують увагу на необхідності прийняття цілеспрямованого методу моніторингу безпеки та аналітики загроз [15, 16, 17]. Це робить актуальним завдання формування простору ознак НСД до ІС. Як і багато інших праць з цієї проблематики, зазначені дослідження не дають конкретних рекомендацій щодо формування простору ознак НСД до ресурсів ІС підприємств.

Існує досить багато трактатів, присвячених ефективності застосування певного математичного апарату для опису функцій НСД до інформаційних ресурсів підприємств. До них належать: теорія ймовірностей [18], нечіткі множини [19], теорія ігор [20], графи та автомати [21], мережі Петрі та випадкові процеси [22].

Перспективним, але недостатньо вивченим у сфері ІБ, залишиться напрям застосування математичного апарату Марківських та напівмарківських випадкових процесів для оцінки загроз та функцій НСД [12, 13, 23].

Відповідно до [23, 24], Марківські та напівмарківські процеси можна застосовувати для оцінки впливу на ІБ різних функцій НСД до інформаційних ресурсів підприємств. Особливо це стосується випадків, коли атака (фактична спроба отримання

НСД до інформаційних ресурсів) є рідкісною та незалежною подією. Для вирішення цього завдання необхідно насамперед формалізувати процедуру формування множини ознак неправомірних дій щодо НСД до ресурсів ІС підприємств.

Виходячи з наведеного вище, для дослідження впливу функцій НСД до ресурсів ІС підприємств виправдано використання Марківських та напівмарківських випадкових процесів.

Таким чином, спираючись на проведений короткий аналіз публікацій, присвячених тематиці дослідження, можна зробити висновок, що, як і раніше, залишається актуальним завдання розвитку математичного апарату, пов'язаного з формалізацією формування простору ознак неправомірних дій щодо НСД до ресурсів ІС підприємств. Ця обставина і визначає основну мету нашого дослідження – опис способу та формалізація формування функціональної моделі неправомірних дій щодо реалізації загроз НСД до ресурсів ІС підприємств.

У процесі формування багатокритеріальної множини для спроб НСД (загроз ІБ або кібернетичних атак) до інформаційних ресурсів підприємства для кожного класу функцій НСД при автоматизації процедур розпізнавання загроз ІБ необхідно побудувати кілька елементарних класифікаторів (ЕК) із заздалегідь заданими властивостями. Зауважимо, що в електронних системах виявлення спроб НСД зазвичай використовують класифікатори, які зустрічаються в описах об'єктів одного класу і не зустрічаються в описах об'єктів інших класів. З іншого боку, набори значень ознак функцій НСД, які є в описі одного з класів НСД, характеризують всі об'єкти цього класу, отже, більш інформативні. Тому, як і раніше, залишається релевантним і таке завдання, як чітка математична систематизація ознак НСД доступу до інформаційних ресурсів підприємств. Це дозволить у майбутніх автоматизованих системах пошуку вразливостей та спроб НСД до інформаційних ресурсів компаній ефективно застосовувати принцип «незустрічності» наборів із допустимих значень ознак, що, своєю чергою, дасть змогу будувати такі вирішальні правила для СЗІ, за яких розпізнавання спроб НСД (або загроз ІБ) проводилося б мінімальною кількістю помилок.

На підставі результатів робіт [12, 13, 23] опис імовірності реалізації функції НСД до ресурсів ІС підприємства (P_{UNA}) можна виразити так:

$$P_{UNA} = \prod_{i=1}^{N} \left(1 - \frac{1}{\left(1 + \sum_{k=1}^{N} \frac{\lambda_i^k}{\vartheta_i^k} \cdot \left(1 + \beta_i^k \cdot \frac{\vartheta_i^k}{\chi_i^k} \right) \right)} \right), \quad (3.1)$$

де N – число методів реалізації функцій НСД на різних етапах;

i – етап реалізації НСД до ресурсів ІС (або загрози ІБ підприємства);

k – спосіб i-го етапу реалізації НСД (наприклад, початкове сканування портів ІС для наступного етапу завантаження шкідливого програмного забезпечення). Спосіб k має експоненційний розподіл, що характеризується λ_i^k як відсоток виявлених за допомогою СЗІ спроб НСД (загроз ІБ);

β_i^k – відсоток загроз ІБ або спроб НСД, які не були виявлені штатними СЗІ для k-го способу i-го етапу реалізації НСД;

$\chi \frac{k}{i}$ – параметр, що характеризує експоненційний час реалізації дій зловмисника, який реалізує функції НСД у ході k-го способу i-го етапу реалізації НСД;

$\vartheta \frac{k}{i}$ – параметр, що характеризує експоненційний час, який потрібен штатним СЗІ для нейтралізації виявлених дій зловмисника під час k-го способу i-го етапу реалізації НСД.

Значення змінної $\lambda \frac{k}{i}$ може бути у найпростішому випадку визначено на основі статистичних даних. Наприклад, це можуть бути дані антивірусного ПЗ, фаєрвола або системи виявлення вторгнень.

Візуалізуємо опис НСД до інформації умовного підприємства у вигляді ієрархічної структурної схеми (див. рис. 3.1), яка послужить основою для опису ієрархічної структури ознак НСД до ресурсів ІС.

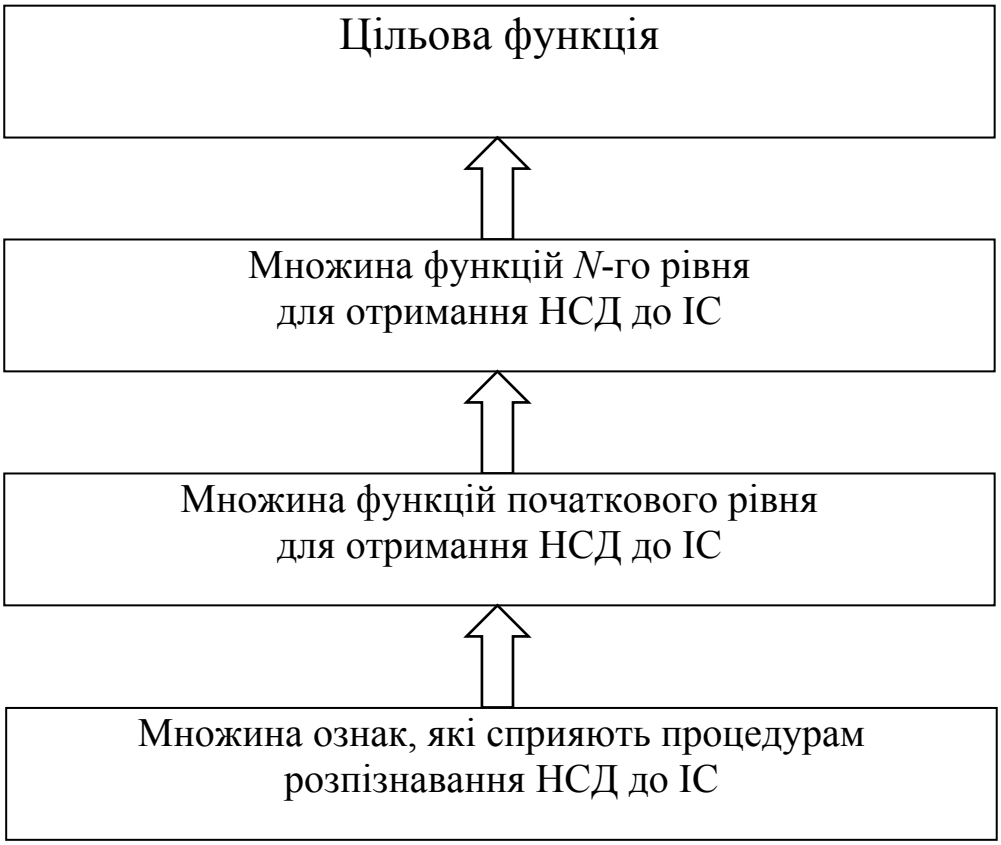


Рис. 3.1. Сутнісні характеристики інформаційного простору

Джерело: узагальнено та доповнено за [12, 13, 23]

Вважаємо, що у разі необхідності і при виникненні нових способів отримання НСД з боку зловмисників кількість ієрархічних рівнів можна змінювати. Припустимо, що комп'ютерні зловмисники, залежно від мотивів та кваліфікації, можуть мати різні цілі НСД, тоді для їх досягнення ними може бути використаний різноманітний арсенал засобів, спрямований на досягнення тактичних або стратегічних цілей атаки. В останньому разі НСД тільки випереджає таргетовану атаку, а основним завданням зазвичай є спроба отримання контролю над бізнес-процесами підприємства або компонентами ІС.

Запропонована ієрархічна структурна схема формування простору ознак НСД до ресурсів ІС підприємства має композиційний характер, що дозволяє аналітично передбачати кінцеве число методів НСД.

При цьому є такі обмеження:

– існує кінцевий набір ознак розпізнавання дій щодо НСД до ІС;

– є причинно-наслідкові зв'язки між реалізованими порушником функціями з НСД до ресурсів ІС та їх ознаками;

– необхідно дотримуватись детермінованого порядку виконання зазначених вище функцій.

Вважатимемо, що $\{RS\}$ – множина ознак, які мають достатню інформативність [25] для розпізнавання дій щодо НСД до ресурсів ІС. Потужність ($C^{(1)}$) цієї множини ознак є підставою для опису таких дій зловмисника. Тоді можна записати такий вираз:

$$\{RS\} \triangleq C^{(1)}, \tag{3.2}$$

де $rsi \triangleq c_i^{(1)}$, i=1,2,…, I.

Відповідно до [1, 2, 7, 9, 12, 18] функції, що реалізуються зловмисником при НСД до інформації, практично повністю ідентичні найменуванню цих ознак, як це показано в табл. 3.1.

Таблиця 3.1

Перший рівень ієрархії формування простору ознак НСД до ресурсів ІС підприємства

№ п/п	Основні функції НСД	Позначення
Функції збору відомостей		
1	про ІС та ІТ підприємства, об'єкта атаки	$c_1^{(1)}$
2	про персонал підприємства, що має доступ до ІС	$c_2^{(1)}$

Закінчення табл. 3.2

№ п/п	Основні функції НСД	Позначення
Вивчення можливостей отримання доступу		
3	до каналів зв'язку ІС поза приміщенням ПК та серверів	$c_3^{(1)}$
4	до каналів зв'язку ІС всередині приміщень підприємства	$c_4^{(1)}$
Отримання доступу		
5	до даних користувача	$c_5^{(1)}$
6	віддаленого доступу	$c_6^{(1)}$
Знімання інформації		
7	з клавіатур ПК	$c_7^{(1)}$
8	з моніторів ПК	$c_8^{(1)}$
9	з мережевих пристроїв ІС та ін.	$c_9^{(1)}$
Впровадження в ІС підприємства шкідливого ПЗ		
10	мережевих «черв'яків»	$c_{10}^{(1)}$
11	троянського ПЗ	$c_{11}^{(1)}$
12	ПЗ, яке використовує вразливості ОС та/або ІС	$c_{12}^{(1)}$
Інші дії		
13	подолання інженерних перешкод	$c_{13}^{(1)}$
14	сканування портів	$c_{14}^{(1)}$
15	використання закладних пристроїв та ін.	$c_{15}^{(1)}$

Джерело: розроблено автором

Зрозуміло, що, враховуючи специфіку бізнес-процесів підприємства та особливості ІТ, які у них застосовані, ознаки не є постійними. Однак якщо говорити про більшу частину інформації, яка циркулює в ІС підприємств, перелік ознак буде досить стабільним. Частково це показано у табл. 3.1. І це дає підстави формалізувати безліч функцій першого ієрархічного рівня структурної схеми формування простору ознак НСД до ресурсів ІС підприємства.

$$C^{(1)} = \left\{c_i^{(1)}\right\},\ i = 1,2,\ldots,I, \tag{3.3}$$

де $I = |C^{(1)}|$ – потужність множини ознак НСД до ресурсів ІС.

Оскільки структурна схема формування простору ознак НСД до ресурсів ІС підприємства має ієрархічний характер, то далі використовуємо вираз (3.3) для формування множини функцій $C^{(2)}$:

$$C^{(2)} = \left\{c_j^{(2)}\right\},\ j = 1,2,\ldots,\left|C^{(2)}\right|. \tag{3.4}$$

Оскільки відповідно до раніше прийнятого припущення функції НСД до ресурсів ІС мають композиційну структуру, то справедлива нерівність виду:

$$\left|C^{(1)}\right| < \left|C^{(2)}\right|. \tag{3.5}$$

У табл. 3.2 функції НСД, які раніше в табл. 3.1 віднесені до першого ієрархічного рівня, наприклад, до категорій зняття інформації (рядки 7, 8, 9 таблиці 3.1) та впровадження в ІС підприємства шкідливого ПЗ (рядки 10, 11, 12 табл. 3.1), розширені. Таким чином, сформовано множину $C^{(2)}$.

Таблиця 3.2

Фрагмент другого рівня ієрархії формування множини ознак НСД до ресурсів ІС підприємства

№ п/п	Ієрархічні рівні			
	Перший		Другий	
	Найменування	Позначення	Найменування	Позначення
	…	…	…	…
Знімання інформації				
7	З клавіатур ПК	$c_7^{(1)}$	Встановлення закладного ПЗ	$C_7^{(2)}$
8	З моніторів ПК	$c_8^{(1)}$		
9	З мережевих пристроїв ІС та ін.	$c_9^{(1)}$		

Закінчення табл. 3.2

№ п/п	Ієрархічні рівні			
	Перший		Другий	
	Найменування	Позначення	Найменування	Позначення
	…	…	…	…
Впровадження в ІС підприємства шкідливого ПЗ				
10	мережевих «черв'яків»	$c_{10}^{(1)}$	Впровадження 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	$C_{10}^{(2)}$
11	троянського ПЗ	$c_{11}^{(1)}$		
12	ПЗ, яке використовує вразливості ОС та/або ІС	$c_{12}^{(1)}$		

Джерело: розроблено автором

Для функцій, які входять до множини й утворені у результаті композиції ознак НСД до ресурсів ІС, потрібно застосувати причинно-наслідковий підхід, тобто розглянути зв'язки між цими функціями та відповідними функціями, що належать $|C^{(1)}|$.

Сформована множина $C^{(2)}$:

$$C^{(2)} = \left\{ c_j^{(2)} \right\}, \; j = 1,2,..., \; j \qquad (3.6)$$

на наступному рівні аналізу ієрархічної структурної схеми формування простору ознак НСД до ресурсів ІС підприємства може бути розширена на третьому рівні – $C^{(3)}$.

Доцільність формування третього та наступних рівнів диктується специфікою бізнес-процесів підприємства і визначається тими ІТ, які конкретне підприємство використовує у цих бізнес-процесах. Наприклад, якщо це транспортна компанія, то НСД може бути реалізований не лише через ІС, а й електронні підсистеми, відповідальні за відстеження:

– маршруту;
– вантажу;
– витрати пального;
– зв'язку із диспетчером;
– інші.

Одним із завдань формування множини ознак НСД до ресурсів ІС підприємства є пошук інформативних описів цих ознак для автоматизації пошуку спроб НСД або фрагментів таких описів. У роботі [26] показано, що інформативними можна вважати такі фрагменти, які зустрічаються в описах об'єктів одного класу спроб НСД (загроз або кібернетичних атак), але не зустрічаються в описах об'єктів інших класів.

При побудові ефективної процедури автоматизації пошуку спроб НСД до інформаційних ресурсів ІС підприємств у працях [25, 26] було запроваджено таке поняття, як елементарний класифікатор – це фрагмент опису об'єкта, що використовується для навчання системи розпізнавання спроб НСД. Для кожного класу загроз ІБ (спроб НСД або кібернетичних атак), відповідно до [26], будують множину елементарних класифікаторів із заздалегідь заданими властивостями.

Запропоновано метод побудови вирішального правила для інтелектуального розпізнавання загроз інформаційно-комунікаційним системам торговельної галузі (ІКСТГ), у якому розпізнавання проводилося з мінімальною кількістю помилок.

Як інформативну значущість ознаки функції НСД до інформаційних ресурсів підприємства використовується такий параметр [25]:

$$IZ_{pa} = \frac{\sum_{(sp_a, NP_{pa}) \in MC^{AL}(KL)} {}^{\nu(sp_a, NP_{pa})}_{p_{aj} \in NP_{pa}}}{\sum_{(sp_a, NP_{pa}) \in MC^{AL}(KL)} {}^{\nu(sp_a)}}, \quad (3.7)$$

де $\nu_{(sp_a, NP_{pa})}$ – функція значимості елементарного класифікатора класу функції НСД;

NP_{pa}= {p_1..., p_N } – сукупність підмножин, що характеризують цілі реалізації функцій НСД;

KL_i – клас функцій НСД (або загроз ІБ, кібернетичних атак на ІС підприємства);

sp_a – математичний опис об'єкта KL_i;

AL – алгоритм виявлення функції НСД;

MC – набір всіх елементарних класифікаторів виявлення функцій НСД;

p_{aj} – опорна множина ознак виявлення функцій НСД.

Фінальним результатом побудови ознакової множини функцій НСД до ресурсів ІС підприємства стане таблиця з описом усіх функцій НСД. Це дасть можливість фахівцям з ІБ підприємства на наступних етапах експлуатації ІС не тільки виконувати аудит ІБ, а й у міру необхідності формувати ефективні контури СЗІ для кожного бізнес-процесу. Іншими словами, може бути чітко визначена цільова функція, що описує варіанти дій зловмисника, який намагається реалізувати спектр функцій НСД до інформаційних ресурсів ІС підприємства.

Таким чином, на відміну від інших досліджень, присвячених цій тематиці, як-от [27, 28, 29], для коректності та обґрунтованості вимог контурів ІБ підприємства формалізація ознакової множини функцій НСД до ресурсів ІС враховує інформативність конкретної ознаки.

Використання наведеної методології на етапі первинної формалізації вимог до побудови контурів захисту інформаційних ресурсів підприємств, на нашу думку, позбавлене основного недоліку, який властивий графічним методам. При застосуванні викладеного вище підходу не потрібно будувати громіздкі графічні схеми (функціональні діаграми). Як показує практика, побудова подібних діаграм часто пов'язана з суб'єктивним трактуванням і не враховує реальну інформативність ознакового простору спроб НСД.

Таким чином, у цьому підрозділі запропоновано підхід до процедури формалізації ознакового функціонального подання неправомірних дій комп'ютерного зловмисника

в ході реалізації функцій НСД до ресурсів ІС підприємств та об'єднань.

Виконано формалізацію 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 невеликої кількості. Це дає змогу ефективно реалізувати первинну формалізацію неправомірних дій комп'ютерних зловмисників для подальшого математичного опису параметра ймовірності НСД, наприклад, на основі Марківських ланцюгів.

Список бібліографічних посилань

1. Olinder N., Tsvetkov A. Leading Forensic and Sociological Aspects in Investigating Computer Crimes // In 6th International Conference on Social, economic, and academic leadership (ICSEAL-6-2019). Atlantis Press, 2020. P. 252–259.

2. Bokovnya A. Y., Khisamova Z. I., Begishev I. R., Latypova E. Y., Nechaeva E. V. Computer crimes on the COVID-19 scene: analysis of social, legal, and criminal threats // Cuestiones Políticas. 2020. № 38 (66). P. 463–472.

3. Nurse J. R., Bada M. The group element of cybercrime: Types, dynamics, and criminal operations // arXiv preprint arXiv:1901.01914. 2019.

4. Okereafor K., Adelaiye O. Randomized cyber attack simulation model: a cybersecurity mitigation proposal for post covid-19 digital era // International Journal of Recent Engineering Research and Development (IJRERD). 2020. № 5 (07). P. 61–72.

5. Chawki M. A. Critical look at the regulation of cybercrime // Computer Crime Research Center. URL : http://www. crime-research.org/library/Critical.doc (date of access: 15.07.2022).

6. Yan X., Cui B., Xu Y., Shi P., & Wang Z. A method of information protection for collaborative deep learning under GAN

model attack // IEEE/ACM Transactions on Computational Biology and Bioinformatics. 2019. № 18 (3). P. 871–881.

7. Yang J., Zhou C., Yang Sh., Xu H. et al. Anomaly detection based on zone partition for security protection of industrial cyber-physical systems // IEEE Transactions on Industrial Electronics. 2018. V. 65. № 5. P. 4257–4267.

8. Глущак В. В., Новіков О. М. Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника // System research and information technologies. 2013. № 2. С. 89–100.

9. Романюков М. Г. Критерії оцінки ймовірності витоку інформації через технічні канали. *Інформатика та математичні методи в моделюванні*. 2015. № 3 (5). С. 240–248.

10. Wang J., Shan Z., Gupta M., Rao H. R. A longitudinal study of unauthorized access attempts on information systems: The role of opportunity contexts // MIS Quarterly, 2019. № 43 (2). P. 601–622.

11. Torres J. M., Sarriegi J. M., Santos J., Serrano N. Managing information systems security: critical success factors and indicators to measure effectiveness // In International Conference on Information Security (2006, August). Berlin, Heidelberg : Springer, 2006. P. 530–545.

12. Lakhno V., Kasatkin D., Blozva A. Modeling cyber security of information systems smart city based on the theory of games and markov processes // 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology / Proceedings. 2019. № 9061383, P. 497–501.

13. Lakhno V. A. et al. Machine Learning and Autonomous Systems // Proceedings of ICMLAS 2021. Chapter Title: Modeling and Optimization of Discrete Evolutionary Systems of İnformation Security Management in a Random Environment.

14. Юдін О. К., Коновалов Е. О., Рогоза І. Є. Методи виявлення атак до інформаційних ресурсів автоматизованих систем // Захист інформації. 2010. Т. 12. № 2 (47). URL :

https://jrnl.nau.edu.ua/index.php/ZI/article/view/1940 (дата звернення: 15.06.2022).

15. Alhayani B., Abbas S. T., Khutar D. Z., Mohammed H. J. Best ways computation intelligent of face cyber attacks // Materials Today: Proceedings. 2021. URL : https://www. sciencedirect.com/science/article/pii/S2214785321016989 (дата звернення: 15.06.2022).

16. Oliveira N., Praça I., Maia E., Sousa O. Intelligent cyber attack detection and classification for network-based intrusion detection systems // Applied Sciences. 2021. № 11 (4), P. 1674.

17. Kolev A., Nikolova P. Instrumental Equipment for Cyber Attack Prevention // Information & Security: An International Journal. 2020. № 47 (3). P. 285–299.

18. Anderson R., Moore T. The economics of information security // Science. 2006. № 314 (5799). P. 610–613.

19. Ak M. F., Gul M. AHP–TOPSIS integration extended with Pythagorean fuzzy sets for information security risk analysis // Complex & Intelligent Systems. 2019. № 5 (2). P. 113–126.

20. Fielder A., Panaousis E., Malacaria P., Hankin C., Smeraldi F. Game theory meets information security management // In IFIP International Information Security Conference (2014, June). Berlin, Heidelberg : Springer, 2014. P. 15–29.

21. Zegzhda P. D., Zegzhda D. P., Nikolskiy A. V. Using graph theory for cloud system security modeling // In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. Berlin, Heidelberg : Springer, 2012. P. 309–318.

22. Kiviharju M., Venäläinen T., Kinnunen S. Towards modelling information security with key-challenge Petri nets // In Nordic Conference on Secure IT Systems. Berlin, Heidelberg : Springer, 2009. P. 190–206.

23. Kasenov A. A., Kustov E. F., Magazev A. A., Tsyrulnik V. F. A Markov model for optimization of information security remedies // In Journal of Physics: Conference Series. 2020. Vol. 1441. № 1. P. 012043. IOP Publishing.

24. Abraham S., Nair S. Cyber security analytics: a stochastic model for security quantification using absorbing markov chains // Journal of Communications. 2014. № 9 (12). P. 899–907.

25. Lakhno V., Boiko Y., Mishchenko A., Kozlovskii V., Pupchenko O., Development of the intelligent decisionmaking support system to manage cyber protection at the object of informatization. // Eastern-European Journal of Enterprise Technologies 2017. № 2 (9-86). P. 53–61.

26. Lakhno V., Kazmirchuk S., Kovalenko Y., Myrutenko L., Zhmurko T. Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features // Eastern-European Journal of Enterprise Technologies 2016. № 3 (9). P. 30–38.

27. Мельник Г. В. Моделювання системи управління інформаційними ризиками в корпоративній інформаційній системі. *Бізнес Інформ*. 2013. № 9. С. 95–99.

28. Opirskyy I. Analysis of static models of unauthorized access to information networks State. *European Cooperation*. 2016. № 2 (9). P. 92–106.

29. Бойченко О. С., Гуменюк І. В., Гладич Р. І. Математична модель оцінки ризику несанкціонованого доступу до інформації користувачами інформаційно-телекомунікаційної системи // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. 2019. № 16. С. 124–134.

3.2. Ідентифікація несанкціонованого доступу до корпоративної інформації

У сучасному світі високотехнологічні електронні пристрої, які стали звичними для ефективних бізнес-процесів, спричинили й нові загрози для інформаційної безпеки (ІБ) не тільки для їхніх власників, а й для підприємств загалом. Своєчасне виявлення загроз ІБ – це перший крок до їхньої

ліквідації або мінімізації потенційної шкоди. Саме тому увага багатьох фахівців у галузі ІБ прикута до розвитку технічних засобів виявлення подібних загроз ІБ. На ринку технічних систем захисту інформації (ТСЗІ) наявна велика кількість пристроїв, призначених для вирішення як вузькоспрямованих, так і масштабних завдань зі знімання, реєстрації, перехоплення, приймання тощо будь-якої електронної та іншої інформації, необхідної для реалізації бізнес-процесів підприємств.

Бізнес-середовище багатьох сучасних суб'єктів господарювання, які активно впроваджують у свої функціональні процеси інформаційні технології (ІТ), останнім часом зазнало якісних змін. Свою лепту в ці процеси вносить і посилення тенденцій щодо глобалізації економіки, зростання конкуренції, появи на ринку нових економічних суб'єктів, збільшення мобільності бізнесу та ін. Зауважимо, що в таких умовах, навіть якщо не ставити завдання з цілеспрямованого ведення конкурентної розвідки, менеджменту підприємств необхідно докладати значних зусиль для збирання та аналізування відповідної бізнес-інформації. Наприклад, якщо підприємство працює з зовнішніми постачальниками, то її спеціалістам необхідна інформація про постачальників, компанії-субпідрядників, дистриб'юторів, транспортних компаній, що займаються логістичним забезпеченням, оптових і роздрібних продавців, страхових компаній тощо.

Нині за допомогою технічних засобів розвідки (ТЗР) зловмисники можуть не тільки вести спостереження за об'єктом, який їх цікавить, а й здійснювати за допомогою спеціальної техніки, наприклад, підслуховування переговорів або перехоплювати радіосигнали. Таке перехоплення дозволяє злочинцю виконати семантичний аналіз перехопленої інформації.

Зазначимо, що конкуренція за права володіння будь-якою інформацією, науковими досягненнями чи матеріальними об'єктами існує протягом усієї історії людства. Залежно від обставин упродовж усього часу існування промислового

шпигунства різні дійові особи, які представляють як сторони захисту, так і нападу, мінялися своїми ролями. Так чи інакше, незмінними залишалися лише об'єкти захисту: приміщення, в яких міститься інформація; матеріальні носії; засоби оброблення інформації та ін.

У ході розвитку електронних пристроїв та ІТ акцент сторони захисту та атакуючої сторони змістився у бік, відповідно, захисту (чи атаки) на технічні канали передавання інформації (ТКПІ).

Так, у працях [1–3] авторами проведено досить глибокий аналіз можливостей засобів технічної розвідки. Проте ці дослідження мають швидше ретроспективний характер, не містять методологічних рекомендацій, спрямованих на зниження рівня загроз витоку інформації.

Натомість у роботах [4–6] розглянуто перспективи розвитку та можливості технічних засобів розвідки (ТЗР) для конкурентної розвідки. Першочергова увага авторами приділена можливостям ТЗР перехоплення побічного електромагнітного випромінювання та наведення (ПЕМВН) від засобів обчислювальної техніки (ЗОТ). Це пов'язано з широким впровадженням у бізнес-процеси практично всіх підприємств засобів обчислювальної техніки та іншого офісного обладнання – принтерів, сканерів, факсів та ін. Автори цих досліджень зосередилися виключно на технічних аспектах застосування ТЗР. Проте, на нашу думку, не розкрито суб'єктивну складову проявів ефекту захищеності інформації від витоків у ТКПІ.

Питання витоків інформації через шпигунське програмне забезпечення розглянуто в розвідках [7–9]. Цей напрям є порівняно новим, оскільки ринок ПЗ стрімко змінюється, зокрема, виникли системи електронного документообігу.

У роботах [10, 11] дослідники зосередили увагу на потенційних загрозах витоку інформації через різні ТКПІ, а також дали вичерпну класифікацію каналів витоку інформації (КВІ).

Автори праць [12, 13] приділили особливу увагу захисту від витоків по віброакустичних каналах, справедливо вважаючи, що з розвитком ІТ ці канали залишаються одними з основних джерел загроз бізнес-процесів підприємств.

Зауважимо, що сторона захисту інформації, як правило, не досить оперативно може реагувати на зміну контексту кібернетичних загроз. А саме цей вид загроз сьогодні, на думку низки дослідників [14, 15] та практиків у сфері захисту інформації [16], є найбільшою небезпекою для інформаційних ресурсів підприємств.

У роботах [1, 5, 11, 13, 14] розглянуто основні умови, за яких виникають параметричні канали витоку інформації (КВІ). До таких умов автори віднесли: наявність у системах нелінійних елементів, встановлення зловмисниками напівактивних закладних пристроїв, застосування атакуючою стороною високочастотних генераторів з антенами та ін. Зауважимо, що останній КВІ виявити досить складно, оскільки для цього необхідно скласти повну карту електромагнітної обстановки, а така робота є частиною методики аналізу та оцінки актуальності загроз витоків інформації. Авторами такої роботи не проведено.

У розвідках [17, 18] наведено результати досліджень з проблематики систематизації проявів ефекту захищеності інформації від витоків по ТКПІ. Однак ці дослідження мають фрагментарний характер і не завжди пов’язані з системними проявами суб’єктно-об’єктних відносин у бізнес-процесах підприємств.

Таким чином, вимоги до протидії ТЗР в цілому та до ступеня захищеності інформаційних ресурсів підприємств, що постійно зростають, а також обґрунтованості заходів запобігання витоку інформації по ТКПІ є актуальними й потребують розвитку методологічного апарату та відповідного прикладного програмного забезпечення (ПЗ), що сприяє автоматизації рутинних трудомістких розрахунків.

Усе сказане вище зумовило релевантність нашого дослідження, головна мета якого – автоматизувати оцінку актуаль-

ності загроз витоку інформації щодо ТКПІ в умовах динамічного вдосконалення ТЗР. Це дає можливість адекватно оцінювати вже на етапі проєктування ТСЗІ заходи щодо запобігання витоку інформації по ТКПІ, насамперед побічних електромагнітних випромінювань і наведень, та по акустичних (віброакустичних) каналах.

Завдання комплексного захисту на підприємствах, принаймні зміни середовища, охоплюють дедалі більше коло питань, як-от обстеження різних фізичних полів, що виникають під час роботи технологічного та офісного обладнання підприємств.

Вирішення завдань, пов'язаних із захистом інформації у межах потенційно можливого перехоплення даних ТЗР, передбачає необхідність проведення цілого комплексу заходів. У цьому першим етапом є виявлення КВІ через різні ТКПІ. А крім того, необхідно провести аналіз інформації, що захищається, і врахувати відповідні демаскувальні ознаки.

В основу методики, що застосовується в інтелектуальній ІС щодо оцінювання актуальних загроз ІБ (у контексті оцінювання конфіденційності інформації) покладемо автоматизацію експертизи. Експертизі піддаються обставини, які дозволяють оцінити фактори, котрі певною мірою впливають на ступінь захищеності інформації.

Розглянемо таку важливу складову методики, як оцінювання рівнів загроз витоку конфіденційної інформації через побічне електромагнітне випромінювання та наведення (ПЕМВН) і віброакустичні сигнали.

Для початку виділимо джерела та ознаки, які дають змогу або експерту, або автоматично за допомогою інтелектуальної ІС віднести їх до потенційних джерел загроз для ІБ підприємства.

При цьому вважаємо, що у множинах виду, що формуються КВІ при експертному оцінюванні, необхідно враховувати всі ознаки відповідного КВІ.

Тоді індекс i – номер джерела. Наприклад, $i = 1$ – випадковий порушник, $i = 2$ – дилетант; $i = 3$ – підготовлений

порушник тощо. Додатково можна врахувати кваліфікацію порушника та його можливу тактику (див. рис. 3.2).

Наступна множина описує фактори вразливості та загрози інформації – $\{\nu_j\}$ (див. табл. 3.3), де індекси j – номери факторів вразливості.

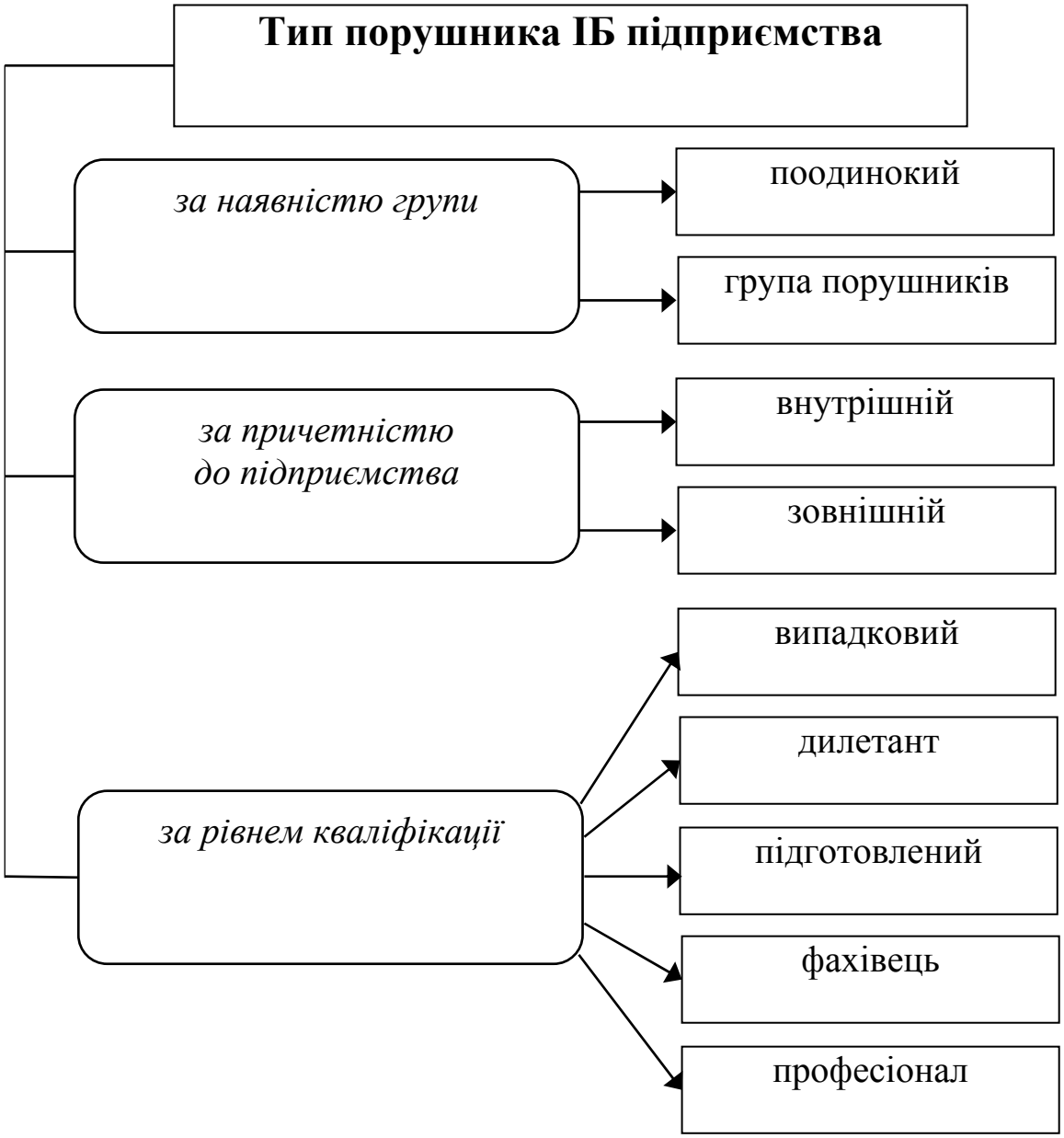


Рис. 3.2. Класифікація порушників ІБ підприємств

Джерело: укладено автором

Для множини $\{v_j\}$ вважаємо, що будь-які види загроз з часом або в міру залучення певних заходів захисту інформації чи усунення вразливостей можуть втрачати свою актуальність. Критерієм актуальності загроз стане їх потенційна ймовірність виконання порушником. Коефіцієнт реалізованості визначимо експертним шляхом. Інтервал коефіцієнта реалізованості прийнятий у діапазоні від нуля до одиниці. Відповідно, нульове значення експерт виставляє в ситуації, коли ймовірність виконання загрози під час експлуатації відповідної вразливості або повністю відсутня, або незначна. Одиниця у цьому випадку відповідає максимально високому рівню виконання загрози відповідної вразливості КВІ.

Неактуальні загрози при автоматизованих розрахунках не брати до уваги, а зосередитися лише на актуальних загрозах.

Таблиця 3.3

Множина факторів вразливостей та загроз

Вид загрози	Актуальність Неактуальна – 0 Актуальна – 1	Коефіцієнт реалізованості
Витік каналами ПЕМВН (*за рахунок:*)		
Побічного електромагнітного випромінювання техніки	[0; 1]	[0; 1]
Наведення по ланцюгах живлення	[0; 1]	[0; 1]
Спеціальних засобів знімання інформації, які використовує атакуюча сторона	[0; 1]	[0; 1]
Тощо	[0; 1]	[0; 1]
Витік акустичними та віброакустичними каналами (*за рахунок:*)		
Перехоплення за допомогою спеціальної апаратури (СпАп) для реєстрації акустичних та віброакустичних хвиль	[0; 1]	[0; 1]
Перехоплення за допомогою СпАп для реєстрації мовної інформації	[0; 1]	[0; 1]
Тощо	[0; 1]	[0; 1]

Джерело: укладено автором

Таким чином, у табл. 3.3 перелічені фактори, що характеризують потенційний перелік вразливостей. Основна розрахункова залежність з метою оцінки актуальності загроз витоку інформації з ТКПІ за умов динамічного вдосконалення ТЗР визначить імовірність наявності відповідних умов виконання відповідної загрози порушником з відповідним рівнем підготовки.

Вважаємо, що попереднє оцінювання виконується експертами під час анкетування. А анкета складена таким чином, що, оскільки межі актуальності/неактуальності загроз та коефіцієнта реалізованості не завжди чітко визначені, то можливо уявити їх відповідними нечіткими лінгвістичними змінними. Наприклад, для актуальності загроз така змінна α_{ij} може бути: «так, актуальна»; «ймовірно, актуальна»; «можливо актуальна»; «малоймовірно, актуальна»; «ні, неактуальна». Експерт виставляє оцінку, керуючись своїми суб'єктивними оцінками можливостей щодо використання i-го потенційного джерела загроз витоку інформації для j-ої вразливості.

Тоді ймовірність буде визначено так:

$$P_j = 1 - \left(k_{j,1}\left(1 - p_{j,1}\right) \cdot k_{j,2}\left(1 - p_{j,2}\right)\right), \tag{3.8}$$

де $k_{j,1}$ – коефіцієнт, що набуває значення, якщо для j-го потенційного джерела загроз витоку інформації характерна вразливість та $k_{j,1} = 0$ – в іншому разі.

На наступному етапі оцінки актуальності загроз витоку інформації з ТКПІ в умовах динамічного вдосконалення ТЗР формується безліч джерел загроз витоку технологічної інформації. Технологічна інформація має свою специфіку, яка визначається особливостями бізнес-процесів підприємства. Адже цілком логічно, що для, наприклад, банківської сфери чи машинобудівного підприємства така технологічна інформація кардинально відрізнятиметься. В узагальненому вигляді опишемо це так: $\{th_c\}, c = 1,2,..., C.$

Для множини $\{th_c\}$, наприклад, загрози можуть виглядати так (див. табл. 3.4, де наведено лише фрагмент найзагальніших загроз).

Для множини $\{th_c\}$ джерел загроз витоку технологічної інформації вважаємо, що будь-які види джерел загроз з часом можуть втрачати свою актуальність.

Дані, наведені в табл. 3.3 та 3.4, дозволяють виконувати кількісне оцінювання рівнів загроз витоку технологічної інформації за ТКПІ, залежно від специфіки підприємства:

$$P_c^v = 1 - \prod_{j=1}^{N}(1 - \lambda_{j,c} \cdot P_j), \qquad (3.9)$$

де P_c^v – ймовірність виконання c-ї загрози витоку інформації щодо ТКПІ в умовах динамічного вдосконалення ТЗР;

N – максимальна кількість факторів вразливостей та загроз, що визначаються специфікою бізнес-процесів підприємства (беремо за табл. 3.1);

$\lambda_{j,c}$ – коефіцієнт актуальності, який приймається на підставі застосування апарату нечіткої логіки (в діапазоні від 0 до 1).

Таблиця 3.4

Множина $\{th_c\}$ джерел загроз витоку технологічної інформації

Вид загрози	Актуальність Неактуальна – 0 Актуальна – 1	Коефіцієнт реалізованості
Витік каналами ПЕМВН (*за рахунок:*)		
Радіоелектронного обладнання	[0; 1]	[0; 1]
Сполучних ліній та сторонніх провідників, які виходять за межі контрольованих зон	[0; 1]	[0; 1]
Просочування інформативних сигналів у ланцюгах електроживлення та заземлення	[0; 1]	[0; 1]
Тощо	[0; 1]	[0; 1]

Закінчення табл. 3.4

Вид загрози	Актуальність Неактуальна – 0 Актуальна – 1	Коефіцієнт реалізованості
Витік акустичними та віброакустичними каналами (*за рахунок:*)		
Акустичних сигналів оптико-електронними каналами	$[0;1]$	$[0;1]$
Прямих повітряних каналів	$[0;1]$	$[0;1]$
Тощо	$[0;1]$	$[0;1]$

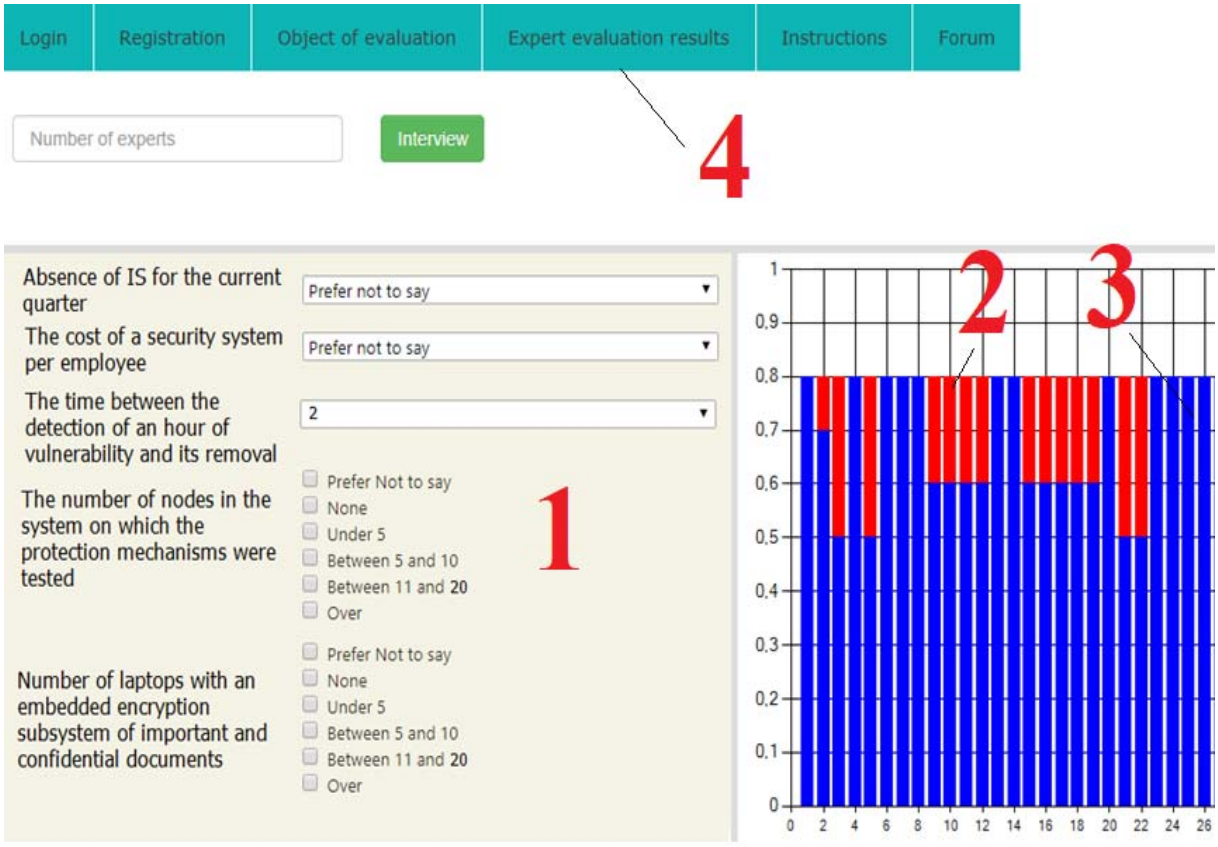
Джерело: укладено автором

При оцінюванні припускаємо, що зовнішній або внутрішній порушник ІБ не має можливостей впливати на інформацію, котра захищається в технічних КВІ. У нього немає можливостей змінити обсяг інформації, тобто основна мета порушника – знімання інформації через технічні канали за допомогою ТЗР для її подальшого аналізу. У цьому випадку загрози від зовнішнього або внутрішнього порушника з середнім рівнем кваліфікації є неактуальними.

Таким чином, вирішення комплексу завдань, пов'язаних із захистом інформаційного простору підприємств від несанкціонованого доступу за допомогою ТЗР або від деструктивних впливів на інформаційні ресурси, передбачає створення системи постійного збирання, оброблення, аналізу відповідних даних. Ці дані стосуються оцінки актуальності загроз витоку інформації з ТКПІ в умовах динамічного вдосконалення ТЗР. Крім того, додатковим завданням у міру розвитку ТЗР стає також отримання інформації про вразливі елементи обладнання та технологічні процеси підприємств, наміри протидіючої сторони тощо.

Для програмної реалізації комплексу «Assessment of threats» для оцінки актуальності загроз витоку інформації вибрано MySQL, HTML, CSS. Це дозволило розробити інтуїтивно зрозумілий інтерфейс (рис. 3.3). Для реалізації модулів оповіщення та графічного представлення результатів оцінки актуальності загроз витоку інформації через ТКПІ застосовано мову програмування Python.

На рис. 3.3 представлений скриншот основного діалогового вікна ПЗ «Assessment of threats». Щоб підвищити рівень об'єктивності, вважаємо, що експерт з інформаційної безпеки повинен спеціалізуватися у питаннях аналізу каналів витоків інформації певного виду. Наприклад, він є фахівцем у галузі акустичних (віброакустичних) КВІ або в галузі витоку інформації через канали ПЕМВН.



1 – анкета експерта; 2 – актуальні загрози витоку інформації через ТКПІ (червоні стовпці); 3 – нормативний рівень захисту ТКПІ від витоків досягнуто (сині стовпці); 4 – головне меню програмного комплексу «Assessment of threats»

Рис. 3.3. Загальний вид програмного комплексу «Assessment of threats» для оцінювання актуальності загроз витоку інформації (скріншот)

Джерело: укладено автором

На рис. 3.4 та 3.5 показані порівняльні результати, отримані під час опитування експертів та висновків, зроблених ними самостійно та за допомогою запропонованого ПЗ

«Assessment of threats». У процесі перевірки програмного забезпечення брали участь 7 експертів. Для оцінювання актуальності загроз витоку інформації було запрошено експертів з досвідом роботи в галузі захисту інформації не менше 5 років.

З рис. 3.4 видно, що розбіжність у думці експертів, які використовували ПЗ «Assessment of threats», на 13–16 % менше, ніж для варіанта оцінювання без використання цього ПЗ.

У ході тестування на ПЗ «Assessment of threats» на 45–55 % скоротилися витрати часу оцінювання ознак несанкціонованого доступу до ТКПІ підприємства.

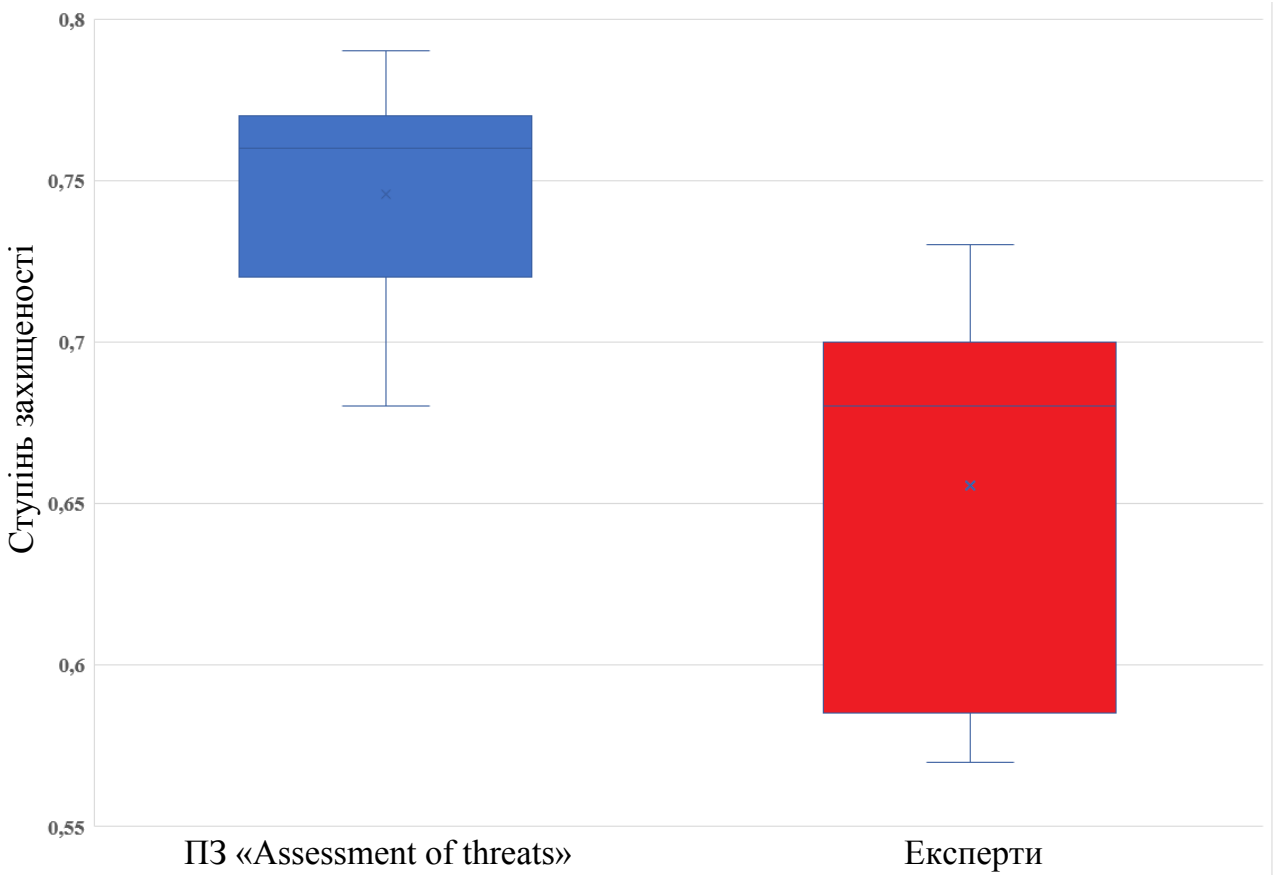


Рис. 3.4. Результати оцінювання експертами самостійно та за допомогою ПЗ «Assessment of threats» ступеня захищеності ТКПІ підприємства

Джерело: укладено автором

Порівняно з аналогічними рішеннями, розглянутими в [18–21], ПЗ «Assessment of threats» має такі переваги:

– можлива інтеграція розробленого ПЗ з наявною системою захисту інформації;

– поліпшується оперативність прийняття рішень у системах управління ІБ;

– можливе гнучке налаштування ПЗ «Assessment of threats» за рахунок розширення переліку параметрів, що входять до множини факторів вразливостей та джерел загроз витоку технологічної інформації.

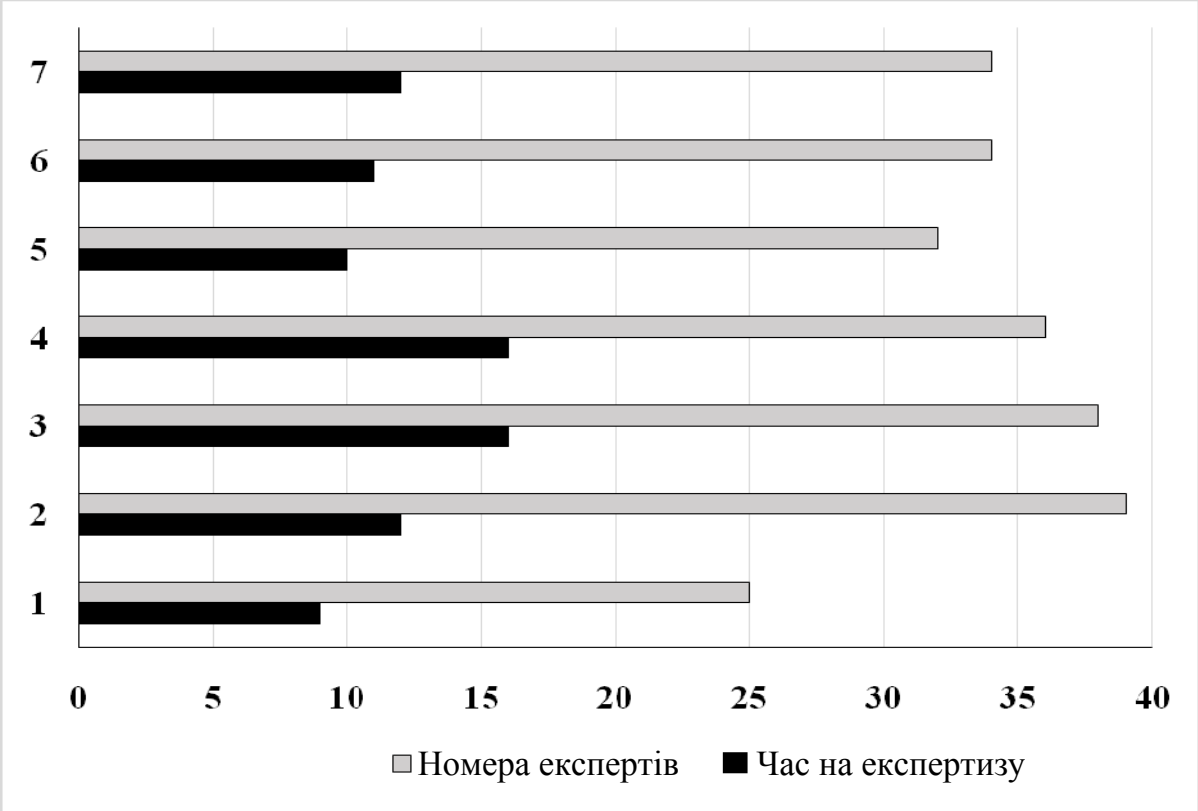


Рис. 3.5. Час, що витрачається експертами самостійно та за допомогою інтерфейсу ПЗ «Assessment of threats» для оцінювання ознак несанкіонованого доступу до ТКПІ підприємства

Джерело: укладено автором

Виявленим у процесі тестування недоліком ПЗ «Assessment of threats» є необхідність залучення на початковому етапі формування бази знань незалежних експертів, знайомих з особливостями захисту конкретного підприємства та його ТКПІ.

Також виявленим недоліком запропонованого підходу є той факт, що ПЗ «Assessment of threats» не дає можливості на цьому етапі дослідження врахувати випадкові стани ТКПІ та динаміку виникнення загроз. Тільки застосування розробленого ПЗ «Assessment of threats», зрозуміло, не гарантує підвищення ступеня захисту ТКПІ підприємства від витоків. Тут потрібен комплексний підхід, наприклад, поєднання запропонованого ПЗ та розрахунок ризиків, пов'язаних із втратою інформації. Також поки що не береться до уваги такий важливий показник, як тривалість процесів перехоплення інформативних сигналів через ТКПІ. Це питання потребує додаткового дослідження.

Таким чином, запропонований методологічний підхід дозволяє автоматизувати та систематизувати прояви ефекту захищеності інформації від витоків технічними каналами. Він доповнює імовірнісну модель виконання загроз, яка дає змогу на основі запропонованого програмного забезпечення (ПЗ) залучати кілька експертів для оцінки актуальності загроз витоку інформації щодо ТКПІ в умовах динамічного вдосконалення ТЗР. Розроблене ПЗ у комплексі з програмним забезпеченням, яке призначене для оцінювання ризиків втрати інформації, дозволяє комплексно оцінити рівень захищеності ТКПІ підприємства. Розроблене ПЗ сприяє зниженню витрат на проведення вузькоспеціальних досліджень у питаннях щодо оцінювання актуальності загроз витоку інформації з ТКПІ в умовах динамічного вдосконалення ТЗР. Таким чином, використання запропонованого ПЗ дає можливість автоматизувати процедуру оцінювання актуальності загроз витоку інформації з ТКПІ в умовах динамічного вдосконалення ТЗР та вдосконалити процес оцінювання захищеності підприємств шляхом використання релевантних оцінок експертів.

Список бібліографічних посилань

1. Ivanov A. V., Trushin V. A., Beresneva A. V., Markelova G. V. The experimental research of security of speech information of leakage from technical channels with account of forcing speech effect // In 12th International Conference on Actual Problems of Electronics Instrument Engineering (APEIE, 2014, October). IEEE, 2014. P. 266–272.

2. Razumov P. V., Zelensky A. A., Cherckesova L. V., Safaryan O. A., Korochentsev D. A., Boldyrikhin N. V., Lyashenko N. G. Development of an Adaptive Fuzzy Algorithm for Identifying Technical Channels of Information Leakage // In Proceedings of Sixth International Congress on Information and Communication Technology. Singapore : Springer, 2022. P. 297–305.

3. Конахович Г. Ф., Назаренко Є. Л., Свириденко В. М. Захист інформації від витоку по технічних каналах // Науко-ємні технології. 2009. № 2 (2). С. 90–93.

4. Anjaria K., Mishra A. Theoretical framework of quantitative analysis based information leakage warning system // Karbala International Journal of Modern Science. 2018. № 4 (1). P. 151–163.

5. Guri M., Hasson O., Kedma G., Elovici Y. An optical covert-channel to leak data through an air-gap // In 14th Annual Conference on Privacy, Security and Trust (PST, 2016, December). IEEE, 2016. P. 642–649.

6. Кримський Т. С. Способи вчинення злочинів, пов'язаних з несанкціонованим доступом до комп'ютерних мереж та мереж електрозв'язку // Юридична наука. 2020. № 7 (109). С. 331–338.

7. Shahzad R. K., Haider S. I., Lavesson N. Detection of spyware by mining executable files // In International Conference on Availability, Reliability and Security (2010, February). IEEE, 2010. P. 295–302.

8. Kirda E., Kruegel C., Banks G., Vigna G., Kemmerer R. Behavior-based Spyware Detection // In Usenix Security Symposium (2006, August). 694 p.

9. Javaheri D., Hosseinzadeh M., Rahmani A. M. Detection and elimination of spyware and ransomware by intercepting kernel-level system routines // IEEE Access. 2018. № 6. P. 78321–78332.

10. Chhetri S. R., Faezi S., Al Faruque M. A. Information leakage-aware computer-aided cyber-physical manufacturing // IEEE Transactions on Information Forensics and Security. № 201813 (9). P. 2333-2344.

11. Zander S., Armitage G., Branch P. Covert channels and countermeasures in computer network protocols [reprinted from ieee communications surveys and tutorials] // IEEE Communications Magazine. 2007. № 45 (12). P. 136–142.

12. Луценко В. М., Якименко О. М. Дослідження методів захисту локальних джерел побічних випромінювань персональних комп'ютерів при створенні КСЗІ. *Захист інформації*. 2011. № 2. С. 95–98.

13. Свінцицький А. В., Степанов В. А., Леонов Б. Д. Удосконалення законодавства щодо термінології у сфері спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації. Інформація і право. 2020. № 3 (34). С. 55–61.

14. Yildirim E. The importance of information security awareness for the success of business enterprises // In Advances in human factors in cybersecurity. Springer, Cham. 2016. P. 211–222.

15. Schiavone S., Garg L., Summers K. Ontology of information security in enterprises // Electronic Journal of Information Systems Evaluation. 2014. № 17 (1). P. 71–87.

16. Fedotova G. V., Kovalenko O. A., Malyutina T. D., Glushchenko A. V., Sukhinin A. V. Transformation of information security systems of enterprises in the context of digitization of the national economy // In Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT. Springer, Cham. 2019. P. 811–822.

17. Abbas J., Mahmood H. K., Hussain F. Information security management for small and medium size enterprises // Science International-Lahore. 2015. № 27 (3). P. 2393–2398.

18. Li X. Decision making of optimal investment in information security for complementary enterprises based on game theory // Technology Analysis & Strategic Management. 2021. № 33 (7). P. 755–769.

19. Хлапонін Ю. І. Неоднозначність трактування та протиріччя деяких визначень в нормативних документах системи технічного захисту інформації. *Сучасний захист інформації*. 2015. № 4. С. 104–109.

20. Олашин М. М., Гапяк С. С. Кримінальні процесуальні аспекти зняття інформації з електронних інформаційних систем // Вісник ЛТЕУ. Юридичні науки. 2018. № 7. С. 233–242.

21. Дудикевич В. Б., Микитин Г. В., Гарасим Ю. Р. Інтегральна безпека інформації: концептуальна модель, автоматизована система оброблення даних з обмеженим доступом. *Сучасний захист інформації*. 2011. № 3. С. 21–31.

3.3. Криптосистема корпоративної інформаційної безпеки

З моменту появи спочатку інформаційних систем (ІС), а потім корпоративних ІС, проблема захисту інформації (ЗІ) у них не втрачає своєї актуальності. Свідченням цього є масштабні кібернетичні атаки, що прокотилися Україною та світом за останній рік [1, 2]. Накопичені у сфері захисту інформації досвід, а також нові вимоги до побудови політики інформаційної безпеки (ПІБ) підприємств дозволили виробити досить ефективні рекомендації щодо побудови системи управління інформаційною безпекою (СУІБ), яка сьогодні інтегрує окремі, часто розрізнені заходи, спрямовані на забезпечення ЗІ та ІБ підприємства.

Центральним процесом у СУІБ підприємств є процес «Управління подіями» (або Event Management – EM). Тільки компетентна організація цього процесу може забезпечити належний рівень усієї послідовності етапів ефективного функціонування СУІБ підприємства. Йдеться про послідовність робіт: 1) планування (Plan); 2) реалізація (Do); 3) перевірка (Check); дія (Act) [3, 4]. Цей ланцюжок заходів щодо забезпечення ІБ підприємства підтвердив свою ефективність для превентивних, реактивних та/або ретроспективних заходів у межах захисту корпоративної інформації як невеликих суб’єктів господарської діяльності, так і великих компаній.

Зауважимо, що розв'язання завдання, пов'язаного з організацією у межах СУІБ підприємства, процесу ЕМ має комплексний характер.

Залежно від масштабу підприємства та специфіки його бізнес-процесів різні суб'єкти господарської діяльності використовують свої набори процесів та підпроцесів СУІБ. Також, як показує практика [5], відрізняються і підходи до ієрархії та інтеграції процесів і підпроцесів СУІБ.

У міру інтеграції України та її суб'єктів господарської діяльності до глобалізованого міжнародного ринку українські підприємства як методологічну основу побудови СУІБ застосовують стандарти серії ISO/IEC 2700x [5, 6].

Проте зауважимо, що у багатьох випадках таке формування СУІБ підприємства на основі ISO/IEC 2700x не враховує особливостей ЕМ у вітчизняних підприємствах. Така ситуація стала наслідком того, що міжнародна практика побудови СУІБ підприємств насамперед спирається на процес управління інцидентами. При цьому багато фахівців у галузі ІБ підприємств думають, що ЕМ є менш значущим фактором. Вважаючи, що пріоритет при побудові ефективної СУІБ відданий виключно управлінню інцидентами, можна випустити з уваги таку обставину. Тільки процес управління інцидентами не може втілити ефективний проактивний підхід у межах надання ІТ-послуг та СУІБ підприємства, а отже, не забезпечує максимально високий рівень ІБ підприємства.

Обмежена увага до впровадження процесу ЕМ на підприємствах найчастіше є наслідком відсутності стандартизованої та загальновизнаної методології, котра має бути адаптована до ПІБ підприємств. Складності вирішення цього завдання зумовлені насамперед тими обсягами та трудомісткістю підготовчих робіт, які необхідно провести аналітикам ІБ підприємства. Причому чим більший масштаб підприємства, тим більше параметрів, що стосуються як організаційного, так технічного рівнів ІС або КІС підприємств, необхідно врахувати.

Питанням побудови ефективної СУІБ підприємства присвячено чимало досліджень. Зауважимо, що деякі автори

[7–11] по-різному трактують такий термін, як «подія» (event) у тих СУІБ. Таке «різночитання» саме собою створює складнощі у роботі аналітиків ІБ підприємства, насамперед лише на рівні термінології.

У проаналізованих працях [7–11] науковці не враховують те, що в ході реалізації процесів, пов'язаних з ЕМ спочатку аналітика або аудитора ІБ, цікавить факт запису про подію, що відбулася. Такий запис може бути фіксований у системі збирання даних служби ІБ підприємства. Додатково фіксуються пов'язані події та стани КІС, наприклад, може йтися про підвищені рівні завантаження процесорів (або ядер) серверів, нетипові встановлені мережеві з'єднання [12] тощо. Наведені приклади також є подіями. Однак більшість нормативних документів з управління інформаційною безпекою [12–16], подібним подіям не приділяють належної уваги. На думку авторів [13, 14], не варто звужувати визначення події, якщо йдеться про забезпечення ІБ підприємства. У розвідках [17–19] йдеться про те, що різночитання поняття «управління подіями» може призвести до фактичного дублювання подій та активностей, а це спричиняє неефективне використання ресурсів сторони захисту КІС. І, що найважливіше, може призвести до ситуації, коли важливі події в контексті ІБ можуть бути втрачені з поля зору аналітика з інформаційної безпеки підприємства [20, 21].

У межах цього дослідження проаналізовано два найбільш ефективні варіанти організації процесу ЕМ – американський та європейський, а саме: детально проведено порівняння між стандартом NIST SP 800-92 [22] та методологією ITIL [23].

Так, у [22] регулюються питання управління логами (Log Management). У цьому документі лог (log) сприймається як запис, що відповідає певній події у системі. Систему тут треба розуміти, наприклад, як КІС чи мережу підприємства. За своїми цілями і беручи до уваги контекст трактування можна говорити про опис лога як про опис управління подією.

У свою чергу у [23] розглядається комплекс процесів СУІБ, а також питання управління подіями.

У табл. 3.5 наведено детальне порівняння цих документів та визнаних світових практик з виділенням їх сильних та слабких сторін.

Таблиця 3.5

Світові практики організації процесу ЕМ у СУІБ

Нормативний документ	Сфера дії	Переваги та особливості	Недоліки
Стандарт NIST SP 800-92 [22]	Федеральні агенції США	Ключові переваги та особливості для: – виділення пріоритетних логів; – встановлення політиками та процедурами управління логами; – створення та підтримання захищених інфраструктур управління логами; – проведення заходів, пов'язаних із навчанням персоналу; – моніторингу статусу ведення подій стосовно всіх джерел подій; – моніторингу ротації подій; ведення архіву; – контролю життєвого циклу (ЖЦ або (Event Life Cycle)) системи обліку логів; – забезпечення синхронізації подій; гнучкого налаштування процедур фіксації логів; – документування та складання звітності	Непослідовність під час викладу процесних аспектів
Методологія ITIL [23]	Будь-які підприємства чи організації	Ключові переваги та особливості для: – визначення головних активностей процесу ЕМ; – реєстрації подій; – запис подій	Не враховано практичні аспекти реалізації сучасних ІТ-інфраструктур підприємств. Не враховані особливості КІС та контекст обробки подій, особливо у межах ЖЦ

Джерело: укладено автором

Таким чином, проведений аналіз літературних джерел, у тому числі провідних світових стандартів [22], методик [23], теоретичних та практичних досліджень [7, 11, 16, 19], дає змогу зробити такий висновок.

Зазначені документи не містять структурованого опису процесу ЕМ, яке апріорі включає принципи безперервного вдосконалення. Нагадаємо ці принципи у такій послідовності: 1) планування (Plan); 2) реалізація (Do); 3) перевірка (Check); дія (Act) [3, 4]. Крім того, у більшості з розглянутих теоретичних праць не було враховано найважливіші аспекти реалізації сучасних ІТ-інфраструктур підприємств, особливості сучасних бізнес-процесів та особливості оброблення подій, що реалізуються у межах їх життєвого циклу.

Отже, можна констатувати, що потрібно сформувати комплексний підхід до організації процесів ЕМ. Цей комплексний підхід повинен враховувати взаємопов'язаність з іншими процесами управління. Крім того, він повинен бути гармонізований зі стандартами ISO/IEC 2700x.

Удосконалення процесів управління ІБ зумовлює необхідність врахування всієї сукупності принципів управління. Очевидно, що ці принципи беруть до уваги й особливості таких об'єктів, як:

– «інформаційна безпека»;

– «необхідність запобігання інцидентам»;

– «необхідність ослаблення інцидентів» [21, 22].

Традиційний підхід передбачає вирішення проблеми підвищення рівня ІБ підприємства шляхом збільшення витрат на СУІБ. Це здебільшого сприяє зниженню рівня ризиків, пов'язаних із втратою інформації. Цей підхід, з погляду математичного моделювання процесів забезпечення ІБ підприємства, базується на пошуку та обґрунтуванні оптимальних значень показників ризику втрати інформації, а також на пошуку відповідних значень мінімальних витрат на побудову ефективної системи ІБ підприємства.

Якщо виходити з припущення, що підхід до побудови СУІБ має бути системним, то в сучасних реаліях (зміна

передумов кібернетичних загроз, збільшення складності сценаріїв кібернетичних атак), акцент потрібно робити на адаптивності та інваріантності способів реалізації інфраструктурних рішень ІБ підприємства.

Впровадження ІТ у процеси управління ІБ і, зокрема, в організацію процесів управління подіями ІБ підприємств сприяє недопущенню потенційно можливих втрат. З урахуванням досліджень [3, 4, 7, 8, 20, 24] у межах побудови СУІБ підприємства запропоновано доповнення до способу організації процесу управління подіями (ЕМ) (див. рис. 3.6).

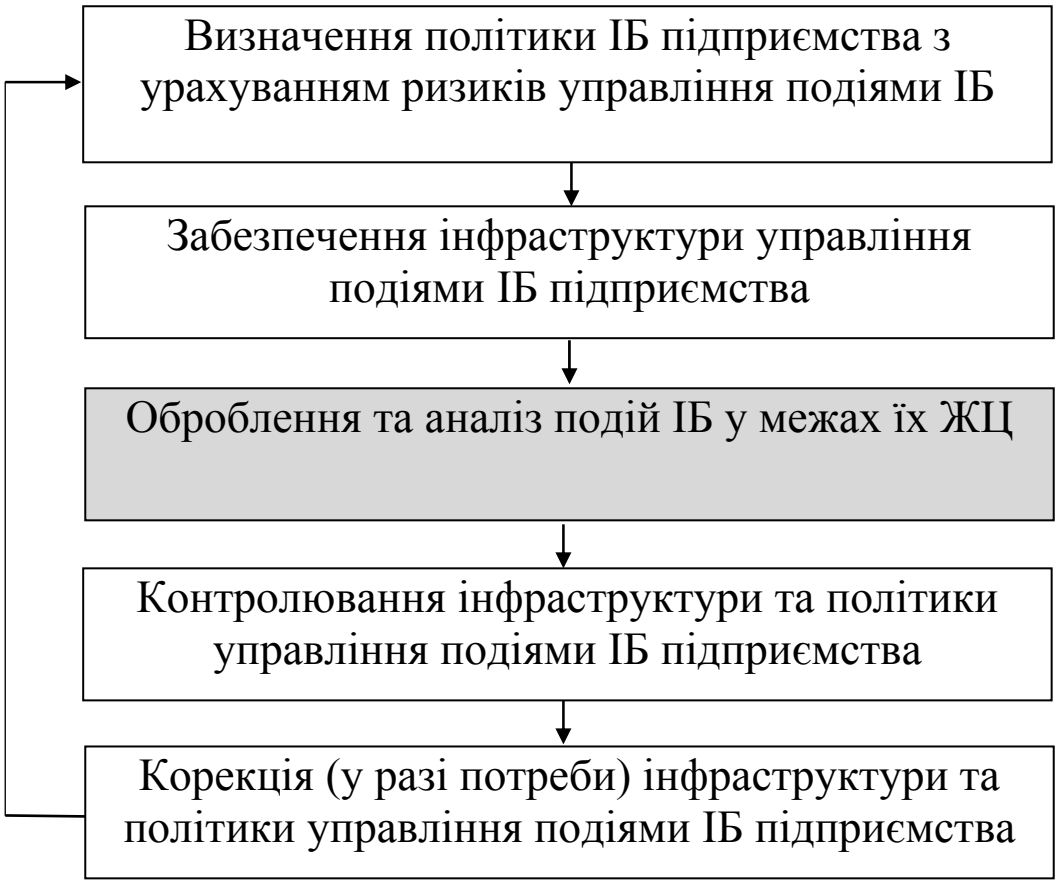


Рис. 3.6. Схема адаптивного процесу управління подіями ІБ підприємств

Джерело: укладено автором

На відміну від наявної практики запропоновані доповнення дозволяють враховувати той факт, що:

– практично не всі події реєструються;

– не всі ті події, які були зареєстровані, відправляються на оброблення до системи класу SIEM (Security information and event management) [10] або SIP (Security event management) [25];

– оброблення подій може викликати нові події.

Запропонована на рис. 3.6 схема адаптивного процесу ЕМ дає змогу, на нашу думку, врахувати і особливості, що пов'язані з:

– визначенням політики ЕМ для КІС підприємства;

– забезпеченням інфраструктурних рішень щодо управління подіями;

– обробкою подій у межах їх ЖЦ;

– контролем за інфраструктурними рішеннями щодо управління подіями;

– контролюванням політики ЕМ;

– у разі потреби – з корекцією інфраструктурних рішень щодо управління подіями;

– у разі потреби – з корекцією політики ЕМ.

З урахуванням тієї обставини, що у межах цього дослідження першочерговий інтерес становлять економічні аспекти організації управління політикою ІБ підприємства, більш докладно зупинимося на такому підпроцесі рис. 3.6, як «Обробка та аналіз подій ІБ у межах їх ЖЦ» (на рис. 3.6 цей підпроцес виділено сірою заливкою).

Зауважимо, що саме цей підпроцес, більш деталізований на рис. 3.7, дозволяє в кінцевому підсумку на підставі аналізу подій ІБ мінімізувати потенційні ризики, пов'язані з можливими втратами інформаційних ресурсів (ІР) підприємств, а отже, й мінімізувати потенційну економічну шкоду, що може бути завдана недотриманням політики ІБ підприємства.

Блок-схема, представлена на рис. 3.7, включає такі основні елементи.

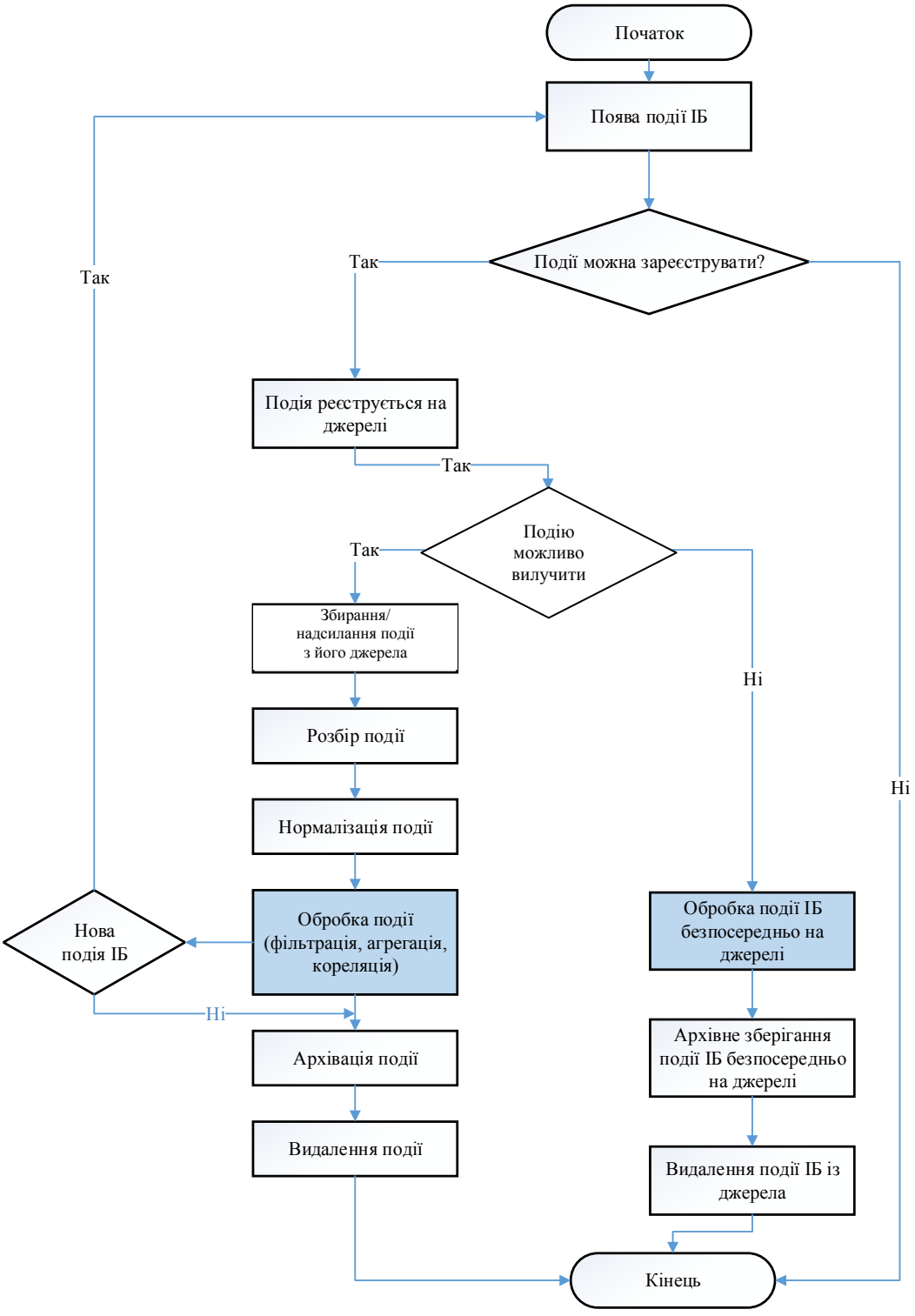


Рис. 3.7. Оброблення та аналіз подій ІБ у межах їх ЖЦ

Джерело: укладено автором

Фактична поява події. На основі зміни або збереження станів, які мають значення для ІБ. Крім того, можуть вплинути на працездатність компонентів КІС її інфраструктури (наприклад, мережі); можуть надати або вже впливають на СУІБ підприємства.

Реєстрація подій. На цьому етапі виконуються відповідні записи в журналах (наприклад, у файлі лог, таблицях баз даних). На цьому етапі зареєстровані події готові до відправлення.

Надсилання повідомлення про подію. На цій стадії відбувається передавання події «точці», яка виконує роль пункту централізованої оброблення. Це можуть бути апаратно-програмні комплекси класів SIEM [10] чи SIP [25].

Розбір подій. На цьому етапі з події виділяються метадані.

Нормалізація події. Цей етап відповідає процедурі конвертації відповідних полів подій у найбільш вигідне та прийнятне для подальшого опрацювання уявлення.

Окремо зупинимося на обробці подій, яка включає такі підетапи, як:

Фільтрування. На цьому підетапі з подій виключаються деякі параметри, наприклад, за критерієм важливості джерела подій, що в результаті дозволяє скоротити витрати часу та ресурсів на оброблення подій.

Агрегація. Цей підетап відповідає процедурі поєднання однотипних чи фактично однакових подій. Об’єднана подія фактично може містити кілька окремих, але подібних до параметрів подій. Це додатково сприяє скороченню витрат часу та ресурсів на оброблення подій.

Кореляція. Цей підетап відповідає пошуку взаємозв’язків між двома чи більше подіями. Як основу кореляції становлять спеціальні шаблони на основі правил та/або статистичних значень тощо.

Збереження архіву та видалення подій.

На підетапі оброблення подій (на рис. 3.7 цей блок виділено заливкою) аналітик ІБ може за допомогою відповідного

програмного забезпечення (ПЗ) проаналізувати параметри, що характеризують стійкість управління ІБ КІС, при цьому вважаючи, що КІС може бути об'єктом кібернетичної атаки. Нижче представлений фрагмент моделі, що становить обчислювальне ядро, призначене для оброблення подій ІБ.

Вважатимемо, що результатом оброблення подій ІБ може стати визначення (як окремий випадок) показника, який характеризує можливе зниження функціональної ефективності КІС у результаті деструктивних дій атакуючої сторони.

Справедливо таке ставлення:

$$(\Delta EF, R_c \to \min_{0<q<1}, \qquad (3.10)$$

де ΔEF – параметр, який характеризує можливе зниження функціональної ефективності КІС внаслідок деструктивних дій атакуючої сторони;

R_c – витрати ресурсів, пов'язані з побудовою ефективної СУІБ підприємства (зокрема, його КІС);

q – ймовірність забезпечення ІБ КІС.

Дослідженням, присвяченим пошуку оптимальних розв'язків цього завдання, присвячено багато праць різних авторів, які для пошуку рішення можуть застосовувати різні методи та моделі (див. рис. 3.8). Це питання виходить за межі цього дослідження, тому ми не зупинятимемося на ньому докладно.

Запропоновані нами рішення та доповнення, на відміну від аналогічних досліджень інших авторів, як-от [17, 18, 24, 26, 27, 28], характеризуються інваріантністю по відношенню до способів реалізації інфраструктурних рішень ІБ. Це твердження справедливе і до ІБ КІС підприємств.

Запропоновані доповнення, зрештою, дозволяють, не змінюючи методичний інструментарій, масштабувати такий підхід і адаптувати його СУІБ різних підприємств. Подальшим розвитком досліджень у цьому напрямі можуть стати роботи, що пов'язані з організацією процесів управління подіями ІБ.

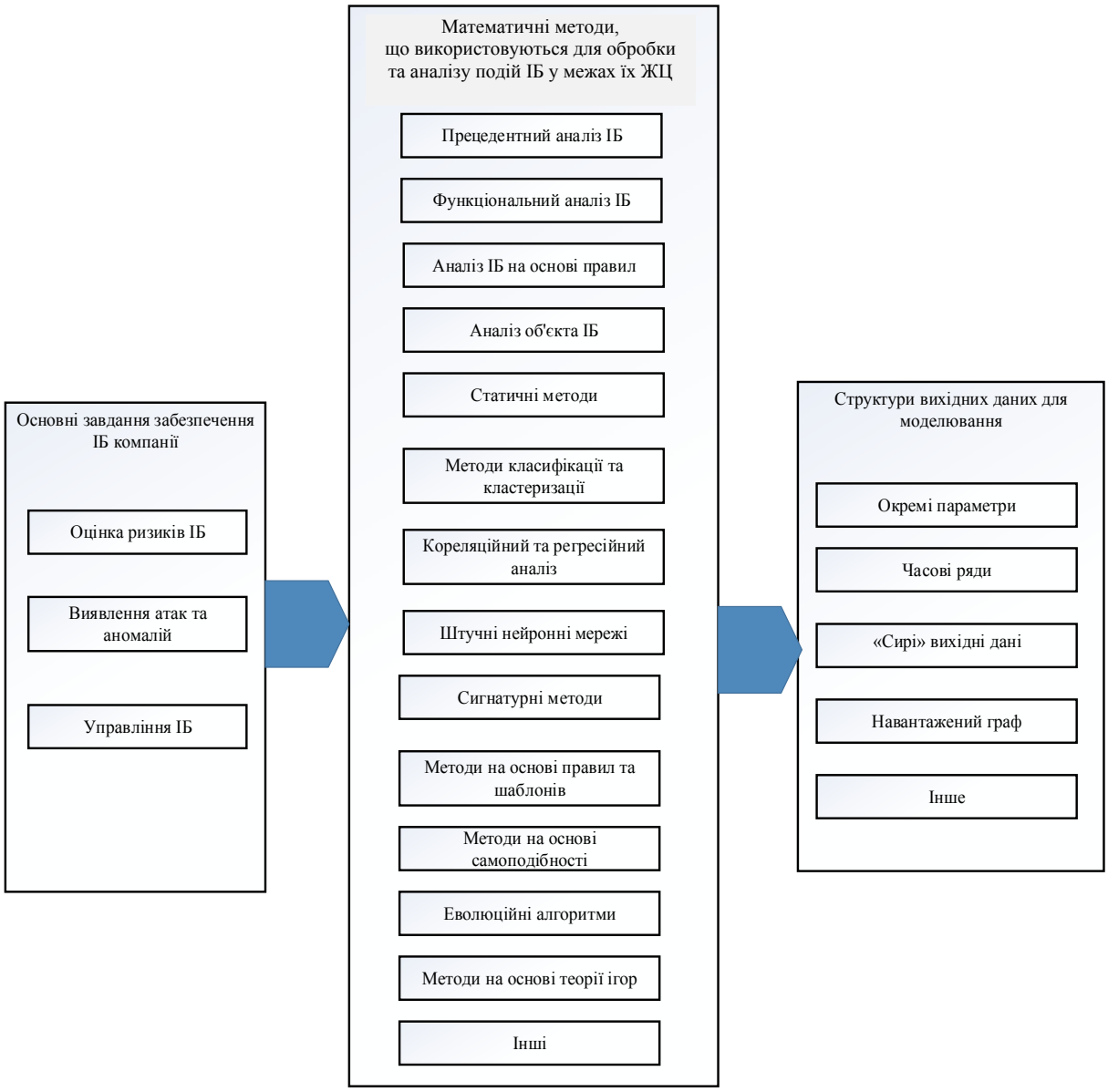


Рис. 3.8. Схема відповідності завдань забезпечення ІБ підприємства та математичних методів їх вирішення

Джерело: укладено автором

Синтез процедур адаптивного моніторингу (див. рис. 3.9) [28] та управління подіями ІБ підприємства в сучасних умовах є нетривіальним завданням.

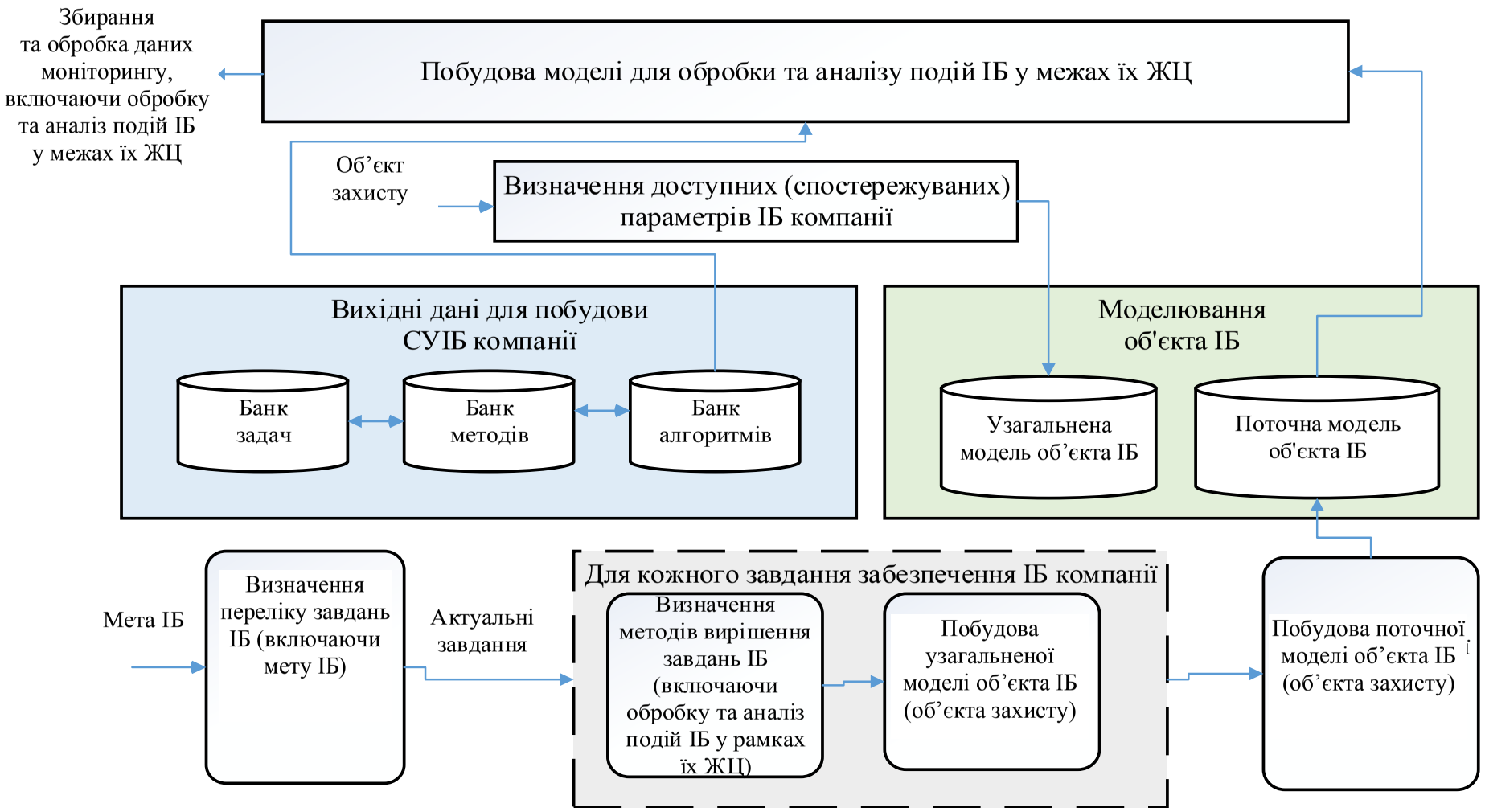


Рис. 3.9. Розширена схема адаптивного моніторингу ІБ, що включає процедури оброблення та аналізу подій ІБ у межах їх ЖЦ

Джерело: розроблено автором

Нетривіальність завдання обумовлюється також різноманіттям завдань ІБ та динамічними особливостями об'єктів захисту. Імплементація методології теорії систем дала можливість сформулювати загальні принципи такого адаптивного моніторингу та управління подіями інформаційної безпеки:

– ієрархічна пов'язаність подій ІБ;

– цілісність;

– подібність подій ІБ.

На рис. 3.9 концептуально показано розширену схему адаптивного моніторингу ІБ, включаючи процедури оброблення та аналізу подій ІБ у межах їх ЖЦ.

Таким чином, під час процесу алгоритмізації процедур, пов'язаних з обробкою та аналізом подій ІБ у межах їх ЖЦ, та відповідно до принципу цілісності об'єкти захисту (наприклад, КІС підприємств) потрібно аналізувати у 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 оброблення подій ІБ у межах їх ЖЦ полягає у побудові взаємних відображень між завданнями ІБ і відповідними методами їх вирішення. У цьому основну роль відіграють доступні дані, необхідні для залучення потенціалу конкретного методу чи моделі у процесах оброблення та аналізу подій ІБ у межах їх ЖЦ. Керуючись подібними відображеннями, можна оптимізувати схеми моніторингу. За такої оптимізації важливо сконцентрувати увагу аналітика з ІБ на ієрархічній пов'язаності подій інформаційної безпеки. 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 оброблення та аналізу подій ІБ у межах їх ЖЦ, відповідає принципам ієрархічної пов'язаності, цілісності та подібності подій ІБ.

Запропоновано доповнення до способу організації процесом управління подіями інформаційної безпеки для підприємства. На відміну від наявних рішень, деталізовано алгоритм підпроцесу «Оброблення подій». Ця деталізація має комплексний характер. Крім того, вона охоплює життєвий цикл події ІБ. Виконані дослідження дають змогу на практиці заповнити потенційні прогалини інформації при створенні системи управління ІБ підприємства. Додатковою перевагою пропонованого рішення є можливість задіяння такого підпроцесу як незалежного, що дозволяє спростити процедуру управління ІБ підприємства в цілому і знизити витрати на її побудову для невеликих підприємств.

Запропоновані рішення та доповнення, на відміну від аналогічних досліджень, характеризуються інваріантністю по відношенню до способів реалізації інфраструктурних рішень ІБ усього підприємства та її КІС зокрема. Це, зрештою, дозволяє, не змінюючи методичний інструментарій, масштабувати даний підхід і адаптувати його СУІБ різних підприємств.

Список бібліографічних посилань

1. White G. Generation Z: Cyber-Attack Awareness Training Effectiveness // Journal of Computer Information Systems. 2021. P. 1–12.

2. Lallie H. S., Shepherd L. A., Nurse J. R., Erola A., Epiphaniou G., Maple C., & Bellekens X. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic // Computers & Security. 2021. № 105, 102248.

3. Fonseca-Herrera O. A., Rojas A. E., & Florez H. A model of an information security management system based on NTC-ISO/IEC 27001 standard // IAENG Int. J. Comput. Sci. 2021. № 48(2). P. 213–222.

4. Culot G., Nassimbeni G., Podrecca M., Sartor M. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda // The TQM Journal. 2021.

5. Tanadi Y., Soeprajitno R. W., Firmansah G. L., El Karima T. ISO 27001 Information Security Management System: Effect of Firm Audits in Emerging Blockchain Technology // Riset Akuntansi dan Keuangan Indonesia. 2021. № 6 (2), P. 198–204.

6. Wu W., Shi K., Wu C. H., Liu J. Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance // Journal of Global Information Management (JGIM). 2021. № 30 (3), P. 1–16.

7. Хох В. Д., Мелешко Е. В., Смірнов О. А. Дослідження методів аудиту систем управління інформаційною безпекою // Системи управління, навігації та зв'язку : Зб. наук. пр. 2017. № 1 (41), С. 38–42.

8. Бегун А. В., Осипова О. І., Урденко О. Г. Про одну з ситуаційних моделей управління інформаційною безпекою підприємства // Моделювання та інформаційні системи в економіці : зб. наук. пр. / М-во освіти і науки України, ДВНЗ «Київ. нац. екон. ун-т ім. Вадима Гетьмана»; [редкол.: О. Є. Камінський (відп. ред.) та ін.]. Київ : КНЕУ, 2020. Вип. 100. С. 39–50.

9. Gabriel R., Hoppe T., Pastwa A., Sowa S. Analyzing malware log data to support security information and event management: Some research results // In 2009 First International Confernce on Advances in Databases, Knowledge, and Data Applications. IEEE, 2009. P. 108–113.

10. Bhatt S., Manadhata P. K., Zomlot L. The operational role of security information and event management systems // IEEE security & Privacy. 2014. № 12 (5). P. 35–41.

11. Kang K., Kim J. A case study on converged security with event correlation of physical and information security // International Journal of Security and Its Applications. 2015. № 9 (9). P. 77–94.

12. Lopez M. A., Silva R. S., Alvarenga I. D., Rebello G. A., Sanz I. J., Lobato A. G., Pujolle G. Collecting and characterizing a real broadband access network traffic dataset // In 2017 1st Cyber Security in Networking Conference (CSNet, 2017, October). IEEE, 2017. P. 1–8.

13. Siponen M., Willison R. Information security management standards: Problems and solutions // Information & management. 2009. № 46 (5). P 267–270.

14. Ključnikov A., Mura L., Sklenár D. Information security management in SMEs: factors of success // Entrepreneurship and Sustainability Issues. 2019. № 6 (4). P. 2081.

15. Shatnawi M. M. Applying Information Security Risk Management Standards Process for Automated Vehicles // Bánki Közlemények (Bánki Reports). 2019. № 2 (1). P. 70–74.

16. Renners L., Heine F., Rodosek G. D. Modeling and learning incident prioritization // In 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS, 2017, September). IEEE, 2017. Vol. 1. P. 398–403.

17. Кожедуб Ю. Аналіз документів з керування ризиком кібербезпеки // Information Technology and Security. 2017. Т. 5. № 1. С. 82–95.

18. Овчаренко М. Ю., Сєвєрінов О. В. Аналіз правил кореляції в системах управління інформаційною безпекою та подіями безпеки Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доповідей одинадцятої Міжнар. науково-технічної конференції (8–9 квітня 2021 р.) ВА ЗС АР; НТУ «ХПІ»; НАУ, ДП «ПДПРОНДІАВІАПРОМ»; УмЖ, 2021. Т. 2, секції 3–5. С. 46.

19. Ушатов В., Сєвєрінов О.В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки // Global Cyber Security Forum : матеріали першого Міжнар. науково-практичного форуму, 14–16 листопада 2019 р. Харків : ХНУРЕ, 2019. С. 104–105.

20. Sievierinov O. V., Ovcharenko M. Y. Analysis of correlation rules in Security information and event management systems // Computer and information systems and technologies. 2020. P. 24–25.

21. Miller D. et al. Security information and event management (SIEM) implementation. McGraw-Hill, 2011.

22. National Institute of standards and technology. Special Publication 800-92. Guide to Computer Security Log Management. 2006. 61 p.

23. ITIL Service Operation Second edition. 2011. P. 58–72.

24. Печенюк А. Особливості організації інформаційної безпеки сучасного підприємства. *Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації*. 2014. № 2. С. 165–168.

25. Ko K., Kim H. K., Kim J., Lee C. Y., Cha S. G., Jeong H. C. Design and Implementation of SIP-aware Security Management System // In International Workshop on Information Security Applications (2009, August). Berlin, Heidelberg : Springer, 2009. P. 10–19.

26. Akhmetov B., Lakhno V., Malyukov V., Akhmetov B., Yagaliyeva B., Lakhno M., Gulmira Y. A Model for Managing the Procedure of Continuous Mutual Financial Investment in Cybersecurity for the Case with Fuzzy Information // Lecture Notes on Data Engineering and Communications Technologies. 2022. № 93 P. 539–553.

27. Lakhno V., Plyska L. Analysis of Models for Selection of Investment Strategies // IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 : Proceedings, 2021. № 9468024, P. 43–46.

28. Yakymenko Y., Muzhanova T., Lehominova S. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FIREEYE // Кібербезпека: освіта, наука, техніка. 2021. № 4 (12). С. 36–50. URL : https://csecurity.kubg.edu.ua/index.php/ journal/article/view/251 (дата звернення: 17.06.2022).

3.4. Аудит систем захисту корпоративної інформації та оцінювання ризиків корпоративної інформаційної безпеки

Динаміка збільшення кількості та складності кібератак на різні об'єкти інформатизації лише за останні кілька років [1, 2] показує, що, незважаючи на всі зусилля сторони захисту протиставити атакуючим все більш технічно досконалі апаратно-програмні засоби інформаційної безпеки, і досі не втрачає актуальності проблематика отримання поточних та прогнозних оцінок рівня ІБ ОБІ. Це завдання особливо стало актуальним для об'єктів критично важливої інфраструктури (КВІС) держави [3], несанкціоноване втручання у комп'ютерні системи (КС) яких може спричинити збої в бізнес-процесах і позначитися на безпеці людей. Наприклад, навіть короткочасна відмова КС, скажімо, підприємств комунальної сфери, здатна викликати перебої у постачанні електроенергії, води, перебої з постачанням у торговельні мережі тощо.

Чим складніша структура ОБІ і що складнішими є застосовувані на ОБІ інформаційні технології (ІТ), тим складніше побудувати для нього відповідну сучасним вимогам систему його інформаційної безпеки. Якийсь важливий об'єкт інформатизації апріорі передбачає необхідність мати сучасну систему управління, зокрема в питаннях, що стосуються ІБ. Такі системи сьогодні стали невід'ємною частиною систем менеджменту (СМ), інтеграція яких до завдань забезпечення ІБ ОБІ передбачає необхідність побудови системи проведення періодичного аудиту ступеня захищеності ОБІ. Це, зокрема, можливо шляхом експертного чи комп'ютерного отримання оцінок (метрик) ІБ у СУІБ.

Проблемі проведення аудиту ІБ (далі – АІБ) для різних ОБІ присвячено чимало робіт, з-поміж яких варто згадати ті, що стали класичними, для вирішення завдань АІБ [4–6].

Так, у розвідці [6] показано важливість аналізу інформаційних потоків для коректного проведення процедур аудиту в інформаційних системах ОБІ. Але автор не розглядає потенціал застосування інтелектуальних систем підвищення якості процедур аудиту ІБ.

У праці [7] аналізується взаємозв'язок процедур внутрішнього аудиту ІБ та зовнішнього аудиту. Проте авторами не взято до уваги постійний розвиток систем захисту ІБ.

Дослідження [8] присвячено особливостям проведення аудиту ІБ для загроз «нульового дня» (*zero-day*). Зокрема, авторами зазначено, що постачальники засобів ІБ зазвичай можуть запропонувати лише варіант постійного розвитку та вдосконалення технічних засобів захисту інформації (ЗЗІ).

Так, у [9, 10] науковці наголошують на тому, що, хоча постійне вдосконалення СЗІ необхідне, проте це «вигідно» переважно виробникам ЗЗІ, тобто лише одне вдосконалення ЗЗІ не здатне самостійно вирішити проблему постійного протистояння СЗІ та загроз ІБ. Більше того, як показано в [11, 12], якщо сторона захисту стикається з цільовою (таргетованою) атакою, то покладатися лише на ЗЗІ буде помилкою.

У зв'язку з цим багато експертів [8, 13, 14] акцентують увагу на необхідності застосування не тільки технічних підходів (використання ЗЗІ) для протидії кібернетичним загрозам, а й впровадження комбінованих методів. Авторами детально не розкрито поняття комбінованих методів, але згадується про потребу їх побудови на базі сімейства стандартів ISO серії 27001 та 19011 [15–19].

Наукову проблему, якої стосується це дослідження, можна сформулювати так. Необхідно подолати суперечність між станом теорії інформаційної безпеки в тій частині, яка регламентує вимоги до проведення аудитів ІБ ОБІ та залежать від контексту кіберзагроз сформованими практиками забезпечення ІБ ОБІ.

Вирішення зазначеної проблеми, зокрема, передбачає необхідність перегляду наявних статичних моделей управління ІБ. Як одне із підзавдань треба згадати необхідність вдосконалення системи АІБ. Отже, процедура прийняття рішень при фіксованій кількості альтернатив зумовлює потребу створення нових підходів до процедур аудиту ІБ, що повинна враховувати відповідальна особа.

Зазначимо, що методологія проведення аудиту ІБ добре відома та відпрацьована фахівцями, але поки що не до кінця розробленими є питання щодо впровадження в процедури аудиту інтелектуальних систем підтримки прийняття рішень (ІСППР). При цьому зростаючі вимоги до якості проведення процедур аудиту ІБ диктують необхідність залучення потенціалу ІСППР у ході оперативного реагування на виявлені загрози в інформаційних системах (ІС). Це робить завдання підвищення ступеня захищеності, і навіть отримання поточних і прогнозних оцінок ІБ ОБІ, релевантним.

Вирішувати завдання підвищення ступеня захищеності, а також отримання поточної та прогнозної оцінки ІБ ОБІ найбільш доцільно, застосовуючи точні чисельні оцінки – метрики ІБ [4, 5].

Це відповідає основним положенням «базового» стандарту системи управління інформаційною безпекою 27004:2009 [17]. Як джерела даних під час реалізації процедур аудиту ІБ (як внутрішнього, так і зовнішнього) можуть бути використані такі відомості:

– результати аналізу та оцінки ризиків для ІБ ОБІ;

– звіти попередніх процедур АІБ;

– журнали реєстрації інцидентів ІБ;

– звіти систем виявлення вторгнень або такої категорії ПЗ як *Security information and event management* (SIEM);

– повідомлення персоналу про інциденти ІБ;

– результати, отримані під час тестування функціональних підсистем КС ОБІ;

– результати, отримані під час тренінгів з ІБ персоналу ОБІ та ін. [6].

З огляду на зазначене вище, сформулюємо таку постановку завдань дослідження:

– розвиток методу СУІБ для проведення аудиту ІБ ОБІ та отримання чисельних поточних та/або прогнозних оцінок ступеня його захищеності в умовах динамічного протистояння з атакуючою стороною;

– розроблення та апробація інтелектуальної системи підтримки прийняття рішень, спрямованих на збільшення ступеня ІБ з можливістю синтезу чисельної оцінки результативності аудиту ІБ ОБІ.

У процесі розроблення програми проведення аудиту ІБ (далі – ПАІБ) не всі зв'язки між свідченнями АІБ можуть враховуватися в конкретній ситуації. Це передусім зумовлено відсутністю необхідної інформації.

Під час проведення аудиту ІБ великих компаній чи підприємств об'єкт аудиту повністю розглянути досить складно. Аудиторам доцільніше вибрати найважливіші інформативні свідоцтва аудиту або метрики ІБ. Ці відібрані метрики матимуть велику значущість і вартість їх отримання буде невисока.

Зазвичай для того, щоб побудувати модель об'єкта АІБ (далі – ОАІБ), доцільно задіяти вагові коефіцієнти значущості свідчень аудиту.

Як показала практика проведення аудитів ІБ, облік значущості свідоцтв аудиту є складним завданням. При цьому важливим фактором є досвід аудитора та особи, яка відповідає за складання програми АІБ і системний аналіз результатів, які одержують у процесі аудиту. Некоректна постановка вихідних завдань АІБ може звести до нуля головну мету АІБ ОБІ, що проводиться, або дати недостовірні результати. Усе сказане вище й обумовлює ефективність комбінації експертних та математичних методів оброблення отриманих експертних оцінок. Як показав аналіз літературних джерел [10, 20], для вирішення зазначеного вище завдання можуть застосовуватися такі методи: парних порівнянь; балових оцінок; векторів переваг; аналізу ієрархій (МАІ) та ін.

Досить докладний аналіз результативності застосування цих методів представлений у [20].

Враховуючи, що відбір метрик ІБ має свої особливості, що диктуються як його галуззю для кожного ОБІ, так і ступенем критичності, далі формалізуємо типове завдання відбору метрик АІБ. У цьому пропонується керуватися таким алгоритмом (див. рис. 3.10).

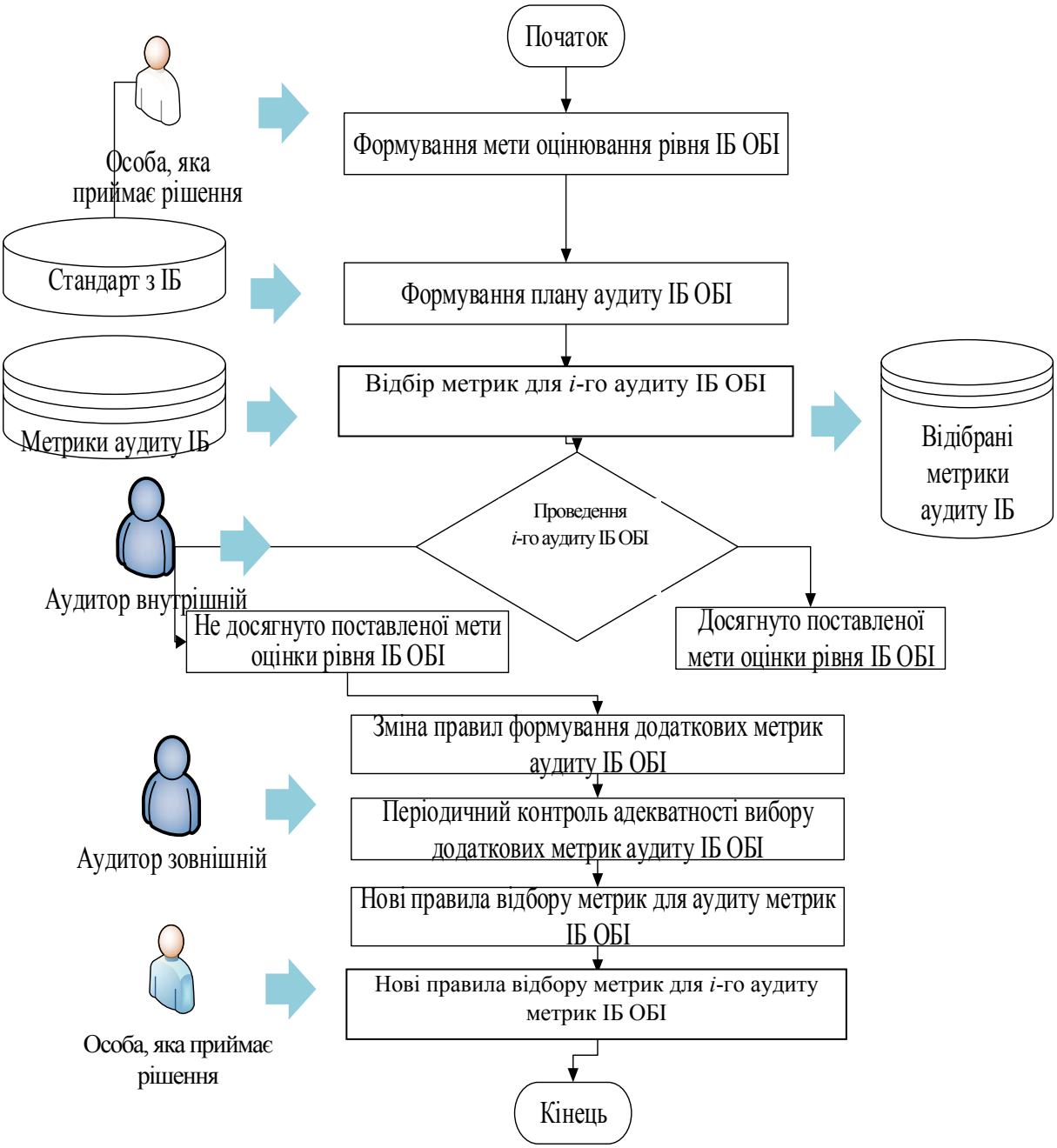


Рис. 3.10. Блок-схема алгоритму відбору індивідуальних критеріїв (метрик ІБ)

Джерело: укладено автором

У модифікованому алгоритмі проведення аудиту ІБ порівняно з базовими процедурами необхідно брати до уваги такі нові обставини:

1. Потрібно орієнтуватися насамперед на відібрані аудиторами пріоритетні метрики ІБ, які раніше могли не зустрічатися протягом попереднього циклу процедури аудиту ІБ ОБІ.

2. Необхідно контролювати відхилення, що з'явилися, в якісних характеристиках відібраної метрики ІБ.

3. Треба формувати правила відбору та заміни раніше відібраних метрик ІБ, наприклад, керуючись результатами попередніх аудитів ІБ або у зв'язку зі зміною контексту загроз для інформаційних систем ОБІ.

Побудова ієрархії метрик ІБ під час аудиту така.

Етап 1. Визначаємо підцілі АІБ. Це можуть бути приватні завдання, наприклад:

оцінити доступність, конфіденційність, цілісність інформації в ІС;

обґрунтувати безліч СА, які включені до програми АІБ (ПАІБ);

вивести відповідні аудиторські докази, передбачені ПАІБ. Свідчення АІБ зазвичай розраховані аналітиками ІБ.

Етап 2. Відбираємо фактори, які є важливими для 2-го рівня ієрархії ПАІБ. На цьому етапі:

збирають об'єктивні свідоцтва АІБ. До таких можна, наприклад, віднести важливі з погляду критеріїв аудиту факти;

фокусують сили та засоби АІБ, як-от аудиторські групи, окремі аудитори ІБ та ін.

Зауважимо, що для кожного ОБІ завдання аудиту ІБ має свою специфіку, яка визначається ступенем критичності інформаційних процесів у бізнес-процесах організації.

З урахуванням публікацій [20–23] можна модифікувати МАІ за рахунок додаткового застосування таких кроків:

Крок 1. Оцінюємо стійкість локальних ранжувань на основі векторів змін елементів матриць парних порівнянь.

Крок 2. Знаходимо експертні оцінки парних порівнянь, які найбільше впливають на зміну локальних ранжувань альтернатив рішень та зміну рівнів узгодженості множини оцінок.

Крок 3. Оцінюємо чутливість глобального ранжування альтернатив рішень до зміни ваги елементів ієрархії.

Крок 4. Знаходимо найбільш чутливі та стійкі елементи для кожного рівня ієрархії.

Фактично MAI необхідний на етапі розрахунку проміжних показників та визначення остаточного рангу об'єктів. Це аналогічно процедурам завдання функцій належності нечітких множин, що використовуються для опису об'єктів спостереження та вимог до них.

У MAI для того, щоб знайти рангу p_i об'єкта, застосовують формулу:

$$p_i = \sum_{j=1}^{n} g_j \cdot v_{ij}, \tag{3.17}$$

де i – порядковий номер об'єкта;
n – кількість критеріїв (метрик ІБ);
j – порядковий номер критерію;
g_j – показник важливості критерію (метрики ІБ);
v_{ij} – показник переваги i-го об'єкта за j-м критерієм.

Неважко помітити певну схожість із найпростішою моделлю односпрямованої нейронної мережі. Теоретично нейронних мереж при цьому застосовують таку формулу [24]:

$$y = f(\sum_{i=0}^{N} w_i \cdot u_i), \tag{3.18}$$

де y –вихідний сигнал нейрона.
N – кількість входів нейрона;
w_i – синаптичні ваги входів;
u_i – вхідний сигнал i-го нейрона; $u_0 = -1$;

Очевидна подібність цих формул. У цьому випадку показник переваги об'єкта за різними метриками ІБ вимогам v_{ij} ставиться у відповідність до синаптичних ваг входів нейрона w_i. Тоді процес обчислення параметрів переваг об'єкта за різними вимогами виконує функції навчання нейронів.

Враховуючи специфіку завдання проведення аудиту ІБ, пропонують такі зміни для модифікації MAI. Це дозволяє як врахувати специфіку предметної сфери проведення АІБ ОБІ, так і подальшої адаптації запропонованих змін практичної реалізації інтелектуальної СППР за допомогою методів об'єктно-орієнтованого проєктування.

По-перше, введемо обмеження на вихідні дані. Це зумовлено особливостями організації процедури АІБ ОБІ. Багато критеріїв оцінки ступеня кібербезпеки ОБІ розділимо на дві частини. Це, відповідно, загальні та індивідуальні критерії (метрики ІБ).

Загальні критерії – це критерії, які пред'являють будь-які ОБІ під час проведення АІБ. Ця безліч залежить від призначення та функціоналу, які реалізовані інформаційними системами ОБІ. Вважаємо, що множина загальних критеріїв, наприклад, надійність, вартість, є обмеженою та постійною.

Водночас кожна процедура АІБ ОБІ має враховувати його специфіку. Враховуємо ці індивідуальні критерії (метрики ІБ) в окремій множині. Індивідуальні критерії є виключно важливими для конкретного ОБІ. Якщо хоча б один критерій не виконаний, то стан захисту ОБІ не задовольняє необхідний рівень ІБ.

По-друге, у процесі модифікації МАІ зроблено таке припущення. Порівняльна оцінка важливості загальних критеріїв може бути здійснена за допомогою класичної експертної оцінки. У цій ситуації немає необхідності вдаватися до залучення парних порівнянь МАІ. Це тому, обставини, що кількість загальних критеріїв щодо забезпечення ІБ ОБІ порівняно невелика. Як показує досвід, більшість практик забезпечення ІБ, вирішальними стають відібрані чотири – п'ять критеріїв (метрик ІБ).

По-третє, внесемо корективи до алгоритму обчислення синаптичних ваг входів нейронів. Значення синаптичних ваг входів нейронів, які відповідають кожному об'єкту, що порівнюється, розраховуємо, використовуючи систему нечітких правил типу IF-THEN. Правила побудовані з урахуванням застосування методу Такаги-Сугено. Як вихідні дані подібної системи використовуємо критерії ІБ ОБІ, які відповідають цьому нейрону. Крім того, беремо до уваги індивідуальні критерії ІБ ОБІ.

Прийнято такі вихідні дані для модифікованого МАІ, який можна використовувати в процедурах аудиту ІБ ОБІ:

1) безліч $\{Y_i\}, i \in [1, n]$, яка містить експертні оцінки важливості кожної з метрик ІБ, n – кількість критеріїв (метрик ІБ);

2) множина $\{Z_i\}, j \in [1, m]$, яка містить індивідуальні критерії (метрики ІБ) ОБІ, m – кількість індивідуальних критеріїв.

Виконання порівняльної оцінки важливості загальних критеріїв передбачає такі етапи:

Етап 1. Керуючись необхідним рівнем ІБ ОБІ, експерт представляє важливість всіх загальних критеріїв ІБ у вигляді множини $\{Y_i\}, i \in [1, n]$, наприклад для $Y \in [1, 0]$, тут «0» відповідає ситуації, коли відсутні вимоги до ІБ об'єкта аудиту, а «10» – максимальна важливість критерію (за аналогією з МАІ Т. Сааті).

Етап 2. Перетворюємо множину $\{Y_i\}$ на множину $\{u_i\}$. Перетворення реалізуємо шляхом нормалізації елементів на інтервал:

$$u_i = \frac{Y_i}{\sum_{i=1}^{n} Y_i}. \qquad (3.19)$$

Отримана множина $\{u_i\}$ буде містити порівняльні показники важливості загальних критеріїв ІБ, які аналізуються в ході проведення АІБ ОБІ.

Нейронна мережа, що використовується під час обчислення рангів об'єктів аудиту, міститиме кількість нейронів h, яка дорівнює кількості об'єктів l, потенційно прийнятних у контурах захисту інформації та кібербезпеки ОБІ. Кожен з нейронів має кількість входів, що дорівнює кількості загальних вимог n. На виході нейронів буде формуватися значення, яке і визначить ранг відповідного об'єкта аудиту.

База нечітких правил (БНП) відбору індивідуальних метрик аудиту ІБ, що дозволяє розрахувати синаптичні ваги входів кожного з нейронів, включатиме правила виду:

$$\{R^k\}:\ IF\ (x_k\ this\ A_k)\ THEN\ w_k = c_k,$$

$$w_i = \frac{\sum_{k=1}^{K} \mu_{A_k}\cdot(x_k)\cdot w_k}{\sum_{k=1}^{K} \mu_{A_k}\cdot(x_k)} \cdot \prod_{j=1}^{m} \mu_{z_j}\cdot(z_j), \qquad (3.20)$$

де $\{R^k\}, k \in [1, K]$ – БНП, котра містить нечітких правил;

$c_k, k \in [1, K]$ – константа, яка залежить від конкретного правила, $c_k, k \in [0,10]$;

$A_k = \{x_k, \mu_{AK}(x_k)\}, k \in [1, K]$ – нечіткі множини, які задані функціями приналежності $\mu_{AK}(x_k)$ на множині можливих значень характеристик об'єкта аудиту ІБ, що відповідають загальним метрикам ІБ;

$x_k, k \in [1, K]$ – значення змінних, які характеризують властивості об'єкта аудиту ІБ і відповідають реалізації загальних критеріїв ІБ ОБІ;

$z = \{z_j, \mu_{zj}(z_j)\}, j \in [1, m]$ – класична множина, що задається функціями приналежності $\mu_{zj}(z_j)$, рівними 0 або 1. Ця множина описує значення властивостей об'єкта аудиту ІБ, які відповідають за реалізацію індивідуальних критеріїв (метрик ІБ);

$z_j, j \in [1, m]$ – змінні, що характеризують властивості об'єкта аудиту ІБ відповідно до індивідуальних критеріїв;

$i, i \in [1, n]$ – номер входу відповідного нейрона.

Функції, розташовані в частині з оператором правил *THEN*, визначаємо як константи. Тоді ці функції прийматимуть максимальні значення у разі, якщо властивості об'єктів аудиту ІБ відповідають нечітким множинам. До таких нечітких множин можна віднести, наприклад, такі: інформація про результативність «миттєвих аудитів» ІБ; інформація про результативність аудитів всіх типів; інформація про інциденти ІБ; інформація про нові переваги у політиці ІБ особи, яка приймає рішення, тощо. У процесі досліджень

було встановлено, що залучення для лінгвістичної оцінки властивостей об'єкта аудиту ІБ лише п'яти, шести термів дозволить оцінювати об'єкт із досить великим ступенем. При цьому ми зберігаємо простоту та наочність моделі, що вдосконалює класичний МАІ.

Множину індивідуальних критеріїв АІБ Z задаємо на множині групових та індивідуальних властивостей всіх об'єктів, що входять до контурів ІБ ОБІ. Функція належності $\mu_{zj}(z_j)$ множини дорівнюватиме одиниці тих властивостей об'єктів АІБ, які забезпечують реалізацію індивідуальних критеріїв. Відповідно, нульове значення буде у разі решти властивостей.

Множина індивідуальних критеріїв, які ставляться у відповідність окремим об'єктам АІБ, становлять собою підмножини множини Z. До множини, що відповідає конкретному об'єкту аудиту ІБ, включаємо тільки ті індивідуальні критерії АІБ, які можуть бути пред'явлені до об'єкта контурів ІБ ОБІ.

На нашу думку, у порівнянні з класичним МАІ Т. Сааті застосування в процедурах аудиту ІБ подібної нечіткої нейронної системи має низку переваг. По-перше, це дозволить прискорити та спростити обчислення синаптичних ваг. По-друге, з'явиться можливість досить точно враховувати індивідуальні критерії (метрики ІБ), характерні для різних об'єктів аудиту ІБ. По-третє, нечітка система дасть змогу врахувати та оцінити величини кількісного та якісного характеру для різних метрик. Це насамперед стосується метрик, описаних як чисельні метрики ІБ.

У результаті модифікований МАІ можна концептуально реалізувати у вигляді такої нейро-нечіткої системи, зображеної на рис. 3.11.

Така схема передбачає об'єднання нейронної мережі, в якій здійснюються порівняння об'єктів контурів ІБ, а також нечіткої системи, що заснована на застосуванні бази нечітких правил, описаних вище.

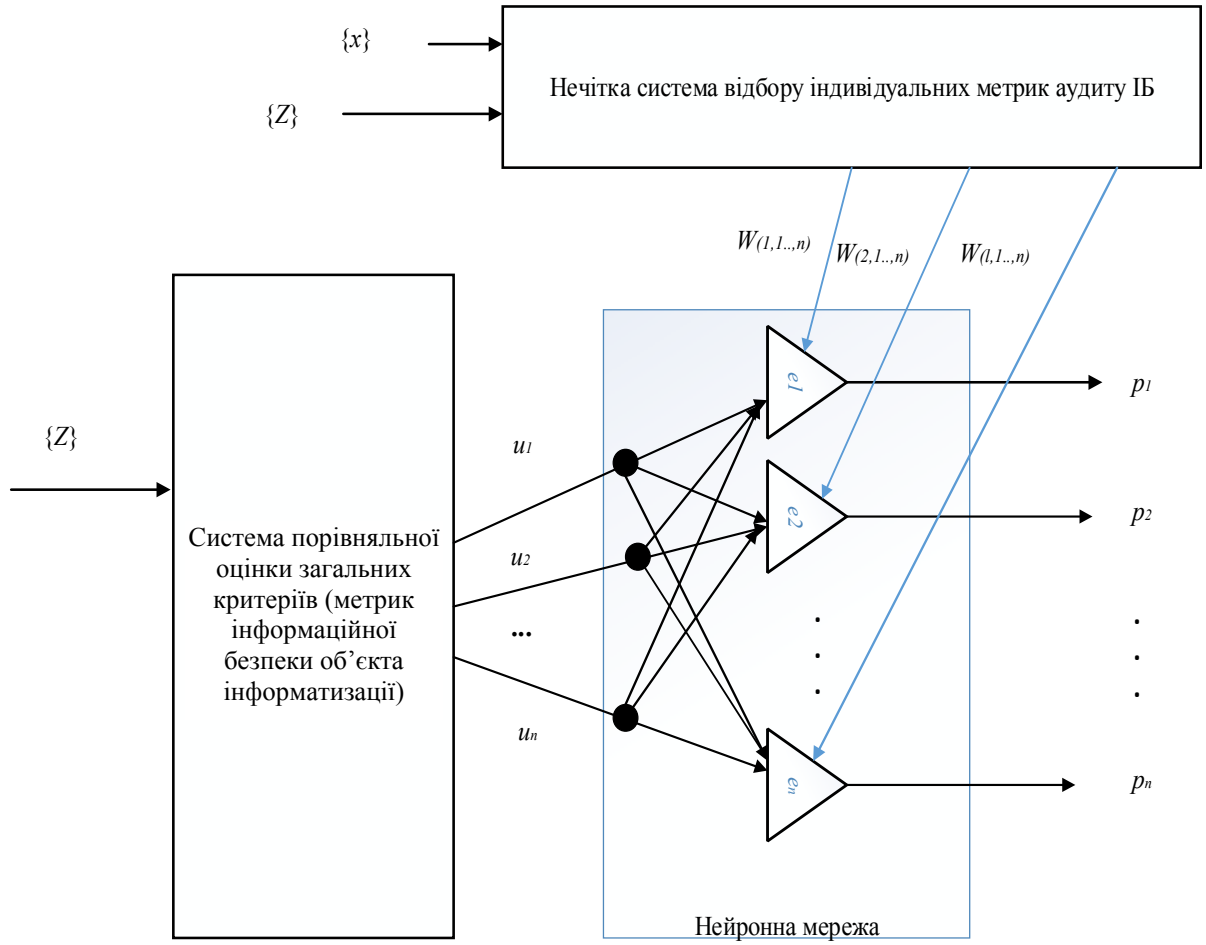


Рис. 3.11. Концептуальна структура нейро-нечіткої системи для модифікованого методу аналізу ієрархій

Джерело: укладено автором

Нечітка система, у відповідності до розробленої схеми, буде здійснювати обчислення синаптичних ваг входів нейронів. При цьому враховуються й індивідуальні критерії (див. табл. 3.6), відібрані для процедур аудиту ІБ конкретного ОБІ.

На вхід нейро-нечіткої системи подаватимуться експертні оцінки важливості критеріїв для конкретного ОБІ, а на виході зчитуються ранги p_1, …, p_n об'єктів контурів ІБ.

Інтелектуальна СППР забезпечує введення індивідуальних критеріїв та експертних оцінок важливості загальних критеріїв, що перевіряються під час аудиту ІБ ОБІ. Результати порівняння об'єктів представлено у вигляді графіка (див. рис. 3.12) [25].

Таблиця 3.6

Приклад формування загальних та індивідуальних метрик 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 аудит 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	Встановлений бізнес-ризик

Джерело: укладено автором

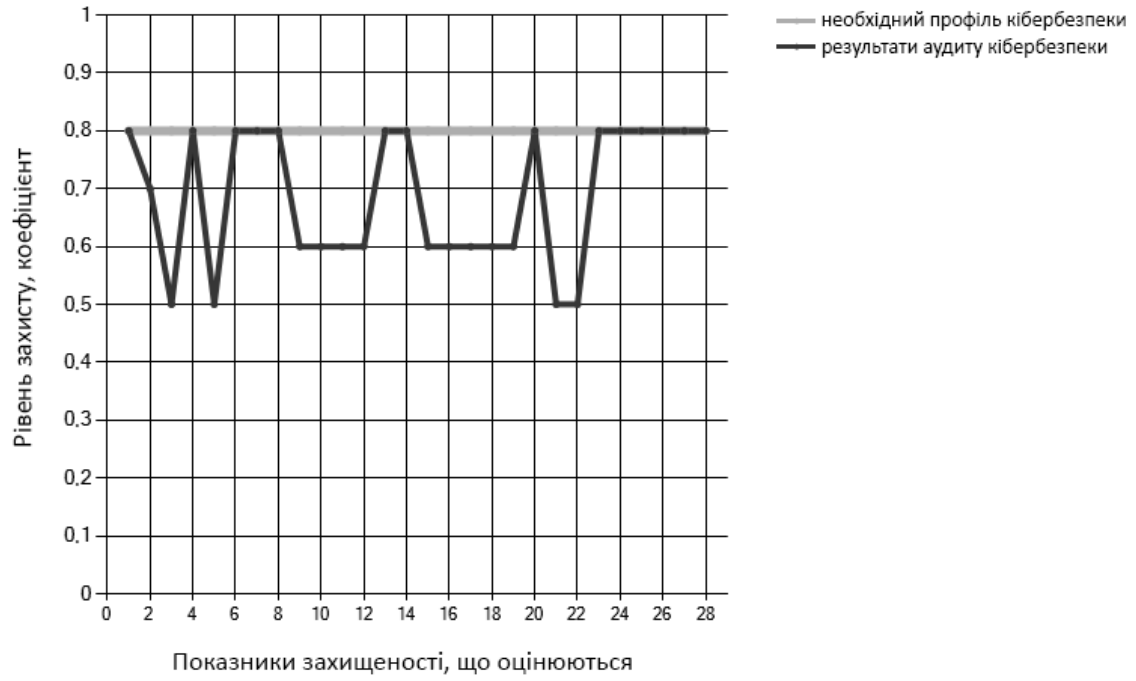


Рис. 3.12. Результати проведення аудиту ІБ ОБІ та зіставлення еталонних вимог до метриків ІБ та досягнутого рівня

Джерело: укладено на основі [25]

В основу виконаних досліджень були покладені ідеї, що дали змогу гармонійно поєднати теорію нейронних мереж та нечітких множин, методи прийняття рішень та метод аналізу ієрархій для проведення та вдосконалення процедур аудиту інформаційної безпеки різних об'єктів інформатизації.

Як видно на рис. 3.12, застосування модифікованого МАІ дозволило отримати графік поточного стану ІБ обстеженого об'єкта інформатизації (лінія блакитного кольору). Причому відібрані критерії ІБ приблизно на 25–30 % нижчі від еталонних значень, хоча при застосуванні класичного МАІ не було таких розбіжностей. Метод апробований під час виконання аудитів ІБ низки підприємств України та Казахстану.

Не вдаючись у детальний аналіз відомих і технічно складно реалізованих кібератак, наприклад, Stuxnet [26] або «Лабіринт місячного світла» [27] та ін., зауважимо, що зараз корисливі мотиви атакуючих відходять на другий план.

Проблематика забезпечення ІБ ОБІ будь-якого масштабу має комплексний характер. Подібний комплексний підхід включає досить великий перелік необхідних заходів, спрямованих на забезпечення ІБ ОБІ. Наприклад, сюди належать заходи, спрямовані на:

– пошук оптимальної стратегії інвестування у засоби захисту інформації (ЗЗІ);

– формування оптимального складу ЗЗІ за контурами ІБ ОБІ;

– оцінку ризиків для інформаційних активів ОБІ та ін.

У цей далеко не повний перелік заходів багато дослідників [28, 29] включають питання організації ефективного аудиту ІБ для ОБІ.

Однак якщо питання технічного забезпечення ІБ ОБІ на сьогодні добре вивчені і, більше того, розроблено багато нових підходів до забезпечення ІБ, заснованих на інноваційних технологіях, то процеси проведення АІБ все ще залишаються новою сферою для дослідників. І справді, сучасні технології привнесли у сферу ІБ підходи, що ґрунтуються на когнітивних технологіях [30, 31], нейронних мережах [32, 33], еволюційних алгоритмах [34, 35] та ін. У той же час більшість досліджень у галузі організації та проведення АІБ зосереджено переважно на організаційній стороні питання. При цьому недостатньо уваги,

на наш погляд, приділено саме розробленню нових методів і моделей АІБ, заснованих на нових технологіях, наприклад, на застосуванні апарату штучних нейронних мереж (ІНС) у процедурах АІБ ОБІ.

Усе сказане вище зумовило релевантність проведення додаткових досліджень, спрямованих на вивчення перспективності залучення апарату ІНС та оцінювання ризиків у процедурах АІБ. Насамперед це стосується АІБ розподілених обчислювальних мереж (РВС) ОБІ, які сьогодні стали основою багатьох бізнес-процесів підприємств та організацій.

Зупинимось на найбільш значущих дослідженнях у галузі автоматизації оцінювання ризиків для ІБ підприємств. Так, у працях [36, 37] показано, що організація ефективної системи управління інформаційною безпекою (СУІБ) ОБІ має бути орієнтована на пріоритетність завдання управління ризиками ІБ.

У розвідках [38–40] обґрунтовано, що функція внутрішнього аудиту (ФВА або IAF) може відігравати важливу роль для забезпечення ІБ ОБІ. Процедури АІБ дозволяють власникам інформаційних активів (ІА) краще зрозуміти, як їм удосконалити ІБ свого підприємства, компанії чи організації. Однак у цих роботах не порушені практичні аспекти використання інтелектуальних технологій у питаннях проведення АІБ ОБІ.

У дослідженнях [40, 41] автори зазначають, що для проведення АІБ ОБІ, як правило, використовується унікальний набір даних, який вивчається експертами. Після цього експертами виробляються рекомендації, які можуть вплинути на ефективність організації ІБ на ОБІ. Однак автори не роблять однозначних висновків щодо доцільності застосування у процедурах АІБ ІТ.

Акцентовано увагу на принципах та завданнях АІБ підприємств у працях [42, 43], проте у них залишається нерозкритим питання потенціалу застосування нових ІТ підвищення ефективності АІБ.

Інші науковці [44, 45] пропонують модель оцінки ризиків порушення політики ІБ (далі ПІБ) ОБІ, що ґрунтується на застосуванні нечітких когнітивних карт. Однак такий підхід хоч і дає змогу враховувати безліч загроз ІБ, але залишається складно алгоритмізованим. Це перекладає всю основну роботу на експерта, а тому підвищує ймовірність суб'єктивної оцінки результатів АІБ ОБІ.

У [46–48] розглянуто практичні аспекти реалізації АІБ на основі штучної нейронної мережі (ШНМ) та проаналізовано питання навчання ШНМ і її тестування під час АІБ конкретного ОБІ. Проте багато питань тут не розкрито, наприклад, немає статистичної оцінки результатів навчання ШНМ. Також відсутнє узагальнення можливості розробленої ШНМ завдань АІБ різних ОБІ.

Можливість автоматизації процедур АІБ шляхом застосування різноманітних систем підтримки прийняття рішень (СППР) та інших ІТ розглянуто у роботах [49–51]. Проте автори зазначають, що ці дослідження ще не завершені, тож про повномасштабну автоматизацію АІБ ОБІ говорити поки що передчасно.

Як показано у розвідках [52, 53], невід'ємною частиною процедур АІБ є аналіз та оцінювання ризиків ІБ для ОБІ, причому останнє має бути виконано на стадії проєктування ІС для ОБІ. Для вирішення цього завдання автори [52, 53] використовували апарат нечіткої логіки (НЛ) та ШНМ, однак їм не вдалося навести переконливих доводів, яким чином виконано, виконується оцінювання апостеріорних ймовірностей у ході реалізації загроз ІБ для ОБІ в умовах динамічного протистояння з атакуючою стороною.

Усе зазначене й зумовило актуальність досліджень, спрямованих на розроблення нових моделей та розвиток методики проведення АІБ ОІБ. Акцент у дослідженні робиться на залучення потенціалу ШНМ та НЛ під час проведення АІБ.

Середовище кібернетичних загроз, що динамічно змінюється, для ОБІ, особливо критично важливих комп'ютерних систем (КВКС), змушує бік захисту активно розвивати моделі і методи безперервного АІБ. В умовах динамічного протистояння з атакуючою стороною одним із пріоритетних завдань АІБ є завдання, пов'язане з аналізом та прогнозування ризиків.

У роботах [54–56], присвячених перспективам застосування ШНМ для завдань аудиту ризиків ІБ, акцент робиться на ситуації, коли аудитори мають досить великі вибірки даних. Зауважимо, що у межах нашого дослідження ми не торкаємося обговорення загальних обмежень ШНМ як інструмента аудиту та оцінки ризиків ІБ ОБІ. Цей аналіз виконано багатьма авторами раніше.

Відповідно до [57, 58], розмір ризику ІБ для ОБІ можна визначити так:

$$R = f(A, T, V), \tag{3.21}$$

де A, T, V – параметри, що характеризують цінність активу, ймовірність реалізації загроз та ймовірність наявності вразливостей відповідно.

Як правило, в ході АІБ обчислюють значення ризиків порушення ІБ для ОБІ загалом – R_{FR}.

Для цього можна використовувати таку залежність:

$$R_{FR} = \sum_{n=1}^{N} R_{FR_{cu}}, \tag{3.22}$$

де N – кількість сегментів розподілених обчислювальних мереж (РОМ);

R_{FRcu} – рівень ІБ для окремого сегмента РОМ.

Значення R_{FRcu} можна визначити, застосовуючи таку залежність:

$$R_{FR_{cu}} = \sum_{st=1}^{ST} P_{\Sigma}^{T} \cdot \left(\frac{IAV_{ST}}{IAV_{\Sigma}}\right), \tag{3.23}$$

де ST – кількість джерел загроз ІБ для сегмента РОМ ОБІ;

P_{Σ}^{T} – результуюче значення ймовірності реалізації загроз ІБ сегменту РОМ;

IAV_{ST}, IAV_{Σ} – вартість інформаційних активів сегмента та ОБІ (РОМ) у цілому відповідно.

Значення P_{Σ}^{T} може бути найдено так:

$$P_{\Sigma}^{T} = 1 - \prod_{st}(1 - P_{ST}^{T}), \tag{3.24}$$

де P_{ST}^{T} – значення ймовірності реалізації загрози ІБ у межах конкретного сегмента РОМ. Ці значення визначають, наприклад, на основі побудови моделі загроз для певних видів загроз та класів атак.

У процесі проведення АІБ і, відповідно, аналізу ризиків, експерт оцінює апріорну імовірнісну інформацію про можливість реалізації загрози. Однак у міру вивчення нової інформації, отриманої в ході аудиту інформаційної безпеки, можуть як підтвердити, так і спростувати апріорну інформацію.

У запропонованому рішенні оцінки ризиків ІБ пропонується застосовувати Байєсовські мережі (БМ) довіри [59].

Наприклад, нехай для БМ були задані апріорні умовні ймовірності виникнення тих чи інших подій. Після цього було проведено навчання мережі на основі статистичних даних [60]. Дані прийняті на основі інформації на сайті Національної бази вразливості США (US National Vulnerability Database).

У подібній БМ цільові змінні – потенційні загрози, перед якими РОМ ОБІ може бути вразливою. Усі змінні цієї БМ дискретні. Кожна змінна (або загроза) може набувати одного з п’яти значень, кожне з яких відповідає ймовірності її реалізації: trivial, low, medium, high, critical (несуттєва, низька, середня, висока, критична відповідно). Інші змінні у БМ є характеристиками. Набір цих характеристик дозволяє ідентифікувати загрозу та визначити її ймовірність. Ці змінні поділені на категорії, що класифікують загрози ІБ або описують різні види комп’ютерних зловмисників. Наприклад, розглянемо БМ для загрози несанкціонованого доступу (НСД) до інформаційних ресурсів РОМ ОБІ:

1. Мета НСД. Розглядається порушення конфіденційності (p_confidentiality), цілісності (p_integrity) чи доступності (p_availability) інформаційних ресурсів РОМ ОБІ.
2. Положення джерела НСД (n_network). Приймалися три категорії джерел: внутрішньосегментний, міжсегментний, зовнішній;
3. Необхідність аутентифікації для реалізації загрози (a_authentication);
4. Кваліфікація атакуючого (a_qualification): висока, середня, низька.

У табл. 3.7 наведено приклад частини даних для опису умовних ймовірностей для загрози «Модифікація даних в інформаційній системі» ОБІ.

Таблиця 3.7

Приклад частини таблиці умовних ймовірностей для загрози «Модифікація даних в інформаційній системі»

Ідентифікатор змінної для загроз		Оцінка умовної імовірності					
Фактори	*p_availability*	Повна					
	p_integrity	Повна					
	p_confidentiality	Повна					
	n_network	Міжсегментна					
	a_authentication	Відсутня		Слабка			
	a_qualification	Низька	Середня	Висока	Низька	Середня	Висока
Рівень загроз	*trivial*	0,00059	0,00059	0,025	0,0074	0,0074	0,025
	low	0,00059	0,00059	0,025	0,0074	0,0074	0,025
	medium	0,00059	0,00059	0,9	0,0074	0,0074	0,9
	high	0,998	0,998	0,025	0,97	0,97	0,025
	critical	0,00059	0,00059	0,025	0,0074	0,0074	0,025

Джерело: укладено автором на основі статистичних даних [60]

У процесі розроблення методу проведення АІБ, який був би заснований на отриманні чисельних оцінок ризиків порушення ІБ з використанням ШНМ, необхідно сформувати дані для навчальної вибірки. Далі виконується вибір структури ШНС.

Приклад навчальної вибірки для топології мережі наведено у табл. 3.8 та на рис. 3.13.

РОМ умовно було розбито на 4 сегменти, кожен з яких відповідає мережі головного офісу та відокремлених структурних підрозділів.

Таблиця 3.8

Фрагмент навчальної вибірки для ШНМ

Можливості реалізації загроз				Сегменти РОМ ОБІ				Ризики ІБ
P1	*P2*	*P3*	*P*	*S1*	*S2*	*S3*	*S4*	
0	0	0	0	0	0	0	0	0
0	0	0	1	0	0,1	0,3	0,4	0
…	…	…	…	…	…	…	…	
1	1	1	1	0,6	0,1	0,4	0,2	0,21

Джерело: укладено автором

ШНМ включає 10 нейронів у прихованому шарі та чотири нейрони у вихідному шарі. При навчанні багатошарового персептрона використано алгоритм зворотного поширення помилки.

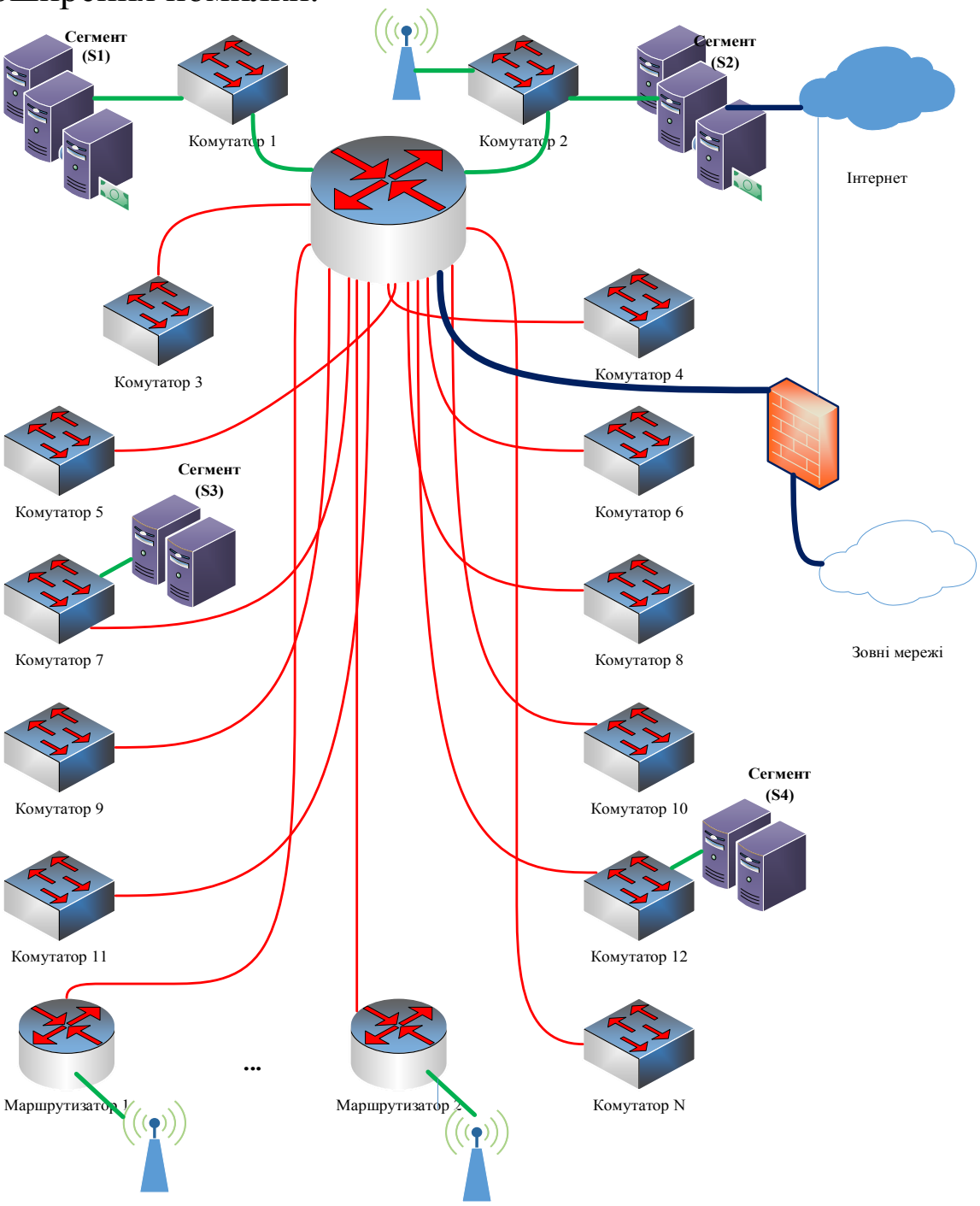


Рис. 3.13. Архітектура мережі умовного підприємства (топологія РОМ ДТЕУ)

Джерело: укладено автором

Цінність інформаційних масивів (ІМ) може задати власник. Власник ІМ визначає їх цінність керуючись їх корисністю для своїх бізнес-процесів, а також враховуючи важливість ІМ та потенційні збитки у разі їхньої втрати.

Зауважимо, що в ході розроблення ШНМ враховувалася специфіка навчальної вибірки. Входом такої ШНМ є дані, що отримані, наприклад, з антивірусного ПЗ, фаєрволів, системи виявлення вторгнень тощо. Ці дані, відповідно, застосовують як вихідну інформацію при оцінюванні загальної активності в мережі та навантаженні, а також показують рівень потенційно небезпечної активності.

Обчислювальні експерименти було проведено з урахуванням РОМ ДТЕУ (див. рис. 3.13).

Обчислювальні експерименти для спроєктованої ШНМ виконані за допомогою пакета Neural Network Toolbox for MATLAB. Навчальна вибірка включала 1200 зразків. Тестова вибірка – 600 зразків. У результаті одержано графіки поверхонь, наприклад, як на рис. 3.14.

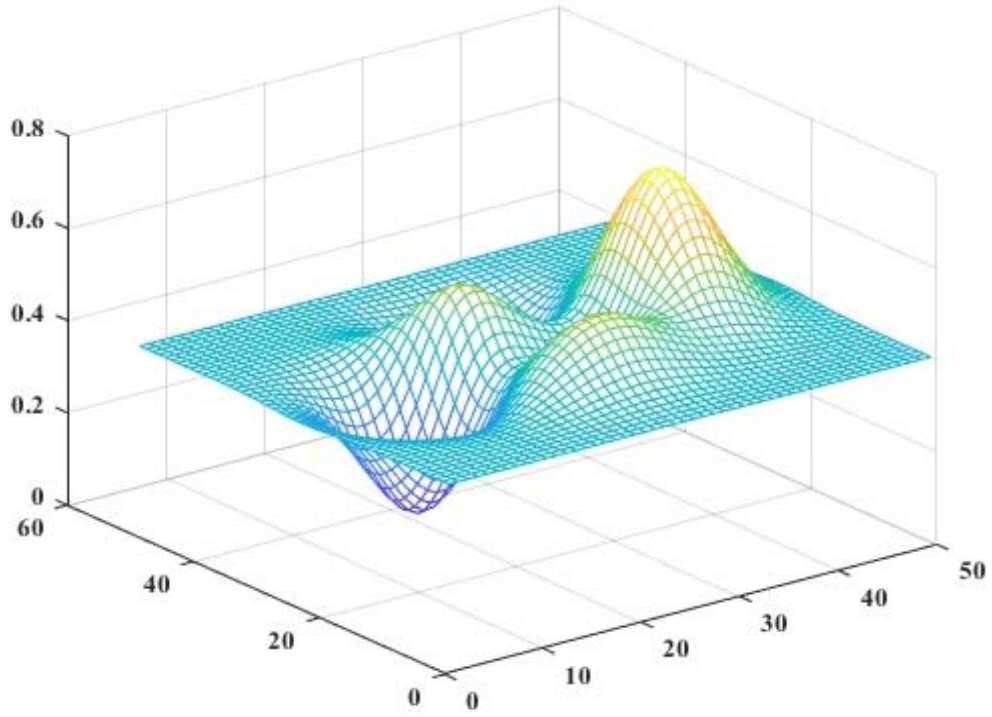


Рис. 3.14. Графік поверхні вихідних значень ризиків ІБ підприємства

Джерело: укладено автором

Результати обчислювальних експериментів показали, що вихідні залежності (3.21) – (3.24) можуть бути досить точно апроксимовані за допомогою ШНМ. Було встановлено, що при збільшенні числа нейронів більше восьми зростає складність та ступінь нелінійності вихідного відображення параметрів оцінки ризиків. При використанні ШНМ у процедурах АІБ необхідно врахувати ступінь довіри експерта до раніше сформованої навчальної вибірки. Якщо даних для навчання недостатньо або частина їх визнана недостовірними, то доцільно скоротити число нейронів. Це дозволяє не перенавчати ШНМ.

Також у результаті обчислювальних експериментів у середовищах Genie і Matlab було доведено, що пропонований підхід до оцінювання ризиків ІБ під час аудиту дозволяє точніше підібрати засоби захисту інформації для контурів РОМ. ШНМ застосовується для оцінки та прогнозування ризиків ІБ у ході аудиту і не тільки дозволяє ефективно підібрати контрзаходи захисту ІБ ОБІ, а й у цілому побудувати ефективну СУІБ, що адаптується до нових загроз. Зниження витрат становило не менше 15 % порівняно з методами оцінювання ризиків у процесі АІБ, які описані у працях [54–58].

Перспективою досліджень є імплементація розробленої ШНМ до складу СППР, яка може також використовуватися в ході АІБ ОБІ. Завданням СППР стане підтримка варіантів рішень, які дозволять адміністратору ІБ РОМ діяти на випередження. Наприклад, як превентивні заходи можна розглянути такі: зупинку або перезапуск серверів, перезапуск віртуальних машин і под.

Комбіноване використання апарату БМ та ШНМ дозволяє автоматизувати процедури АІБ, у тому числі для досить складних сценаріїв проведення атак на РОМ.

Список бібліографічних посилань

1. Lallie H. S., Shepherd L. A., Nurse J. R., Erola A., Epiphaniou G., Maple C., Bellekens X. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic // Computers & Security. 2021. № 105, 102248.

2. Miao Y., Chen C., Pan L., Han Q. L., Zhang J., Xiang Y. Machine Learning Based Cyber Attacks Targeting on Controlled Information: A Survey // arXiv preprint. URL: https://arxiv. org/abs/2102. 07969 (дата звернення звернення 22.06.2022).

3. Yamin M. M., Ullah M., Ullah H., Katt B. Weaponized AI for cyber attacks // Journal of Information Security and Applications. 2021. Vol. 57. 102722.

4. Golyash I., Sachenko S., Rippa S. Improving the information security audit of enterprise using XML technologies // In Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (2011, September). IEEE, 2011. Vol. 2. P. 795–798.

5. Steinbart P. J., Raschke R. L., Gal G., Dilla W. N. The influence of a good relationship between the internal audit and information security functions on information security outcomes // Accounting, Organizations and Society. 2018. № 71, P. 15–29.

6. Griffiths P. Where next for information audit? // Business Information Review. 2010. № 27 (4) P. 216–224.

7. Steinbart P. J., Raschke R. L., Gal G., Dilla W. N. The relationship between internal audit and information security: An exploratory investigation // International Journal of Accounting Information Systems. 2012. № 13 (3). P. 228–243.

8. Kaur R., Singh M. A survey on zero-day polymorphic worm detection techniques // IEEE Communications Surveys & Tutorials. 2014. № 16 (3). P. 1520–1549.

9. Steinbart P. J., Raschke R. L., Gal G., Dilla W. N. Information security professionals' perceptions about the relationship between the information security and internal audit functions // Journal of Information Systems. 2013. № 27 (2). P. 65–86.

10. Kayworth T., Whitten D. Effective information security requires a balance of social and technology factors // MIS Quarterly executive / Published 15 May 2012. URL : https://www. semantic-scholar. org/paper/Effective-Information-Security-Requires-a-Balance-Kayworth-Whitten/ f29f258b0508d8ceba0a8e3942656df294127784 (дата звернення 22.06.2022).

11. Jarison J., Morris L., Wilkinson C. The future of cyber security in internal audit. Disponibil online la www. crowe. com/-/media/Crowe/LLP/foliopdf/The-Future-of-Cybersecurity-in-IA-Risk-18000-002A-update.ashx. 2018.

12. Suduc A. M., Bîzoi M., Filip F. G. Audit for information systems security // Informatica Economica. 2010. № 14 (1). P. 43.

13. Herath H. S., Herath T. C. IT security auditing: A performance evaluation decision model // Decision Support Systems. 2014. № 57. P. 54–63.

14. Atymtayeva L. B., Bortsova G. K., Inoue A., Kozhakhmet K. T.. Methodology and ontology of expert system for information security audit // In The 6th International Conference on Soft Computing and Intelligent Systems, and The 13th International Symposium on Advanced Intelligence Systems (2012, November). IEEE : 2012. P. 238–243.

15. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. International Organization for Standardization, 2013. 23 p.

16. ISO/IEC 27000:2014. Information technology. Security techniques. Information security management systems. Overview and vocabulary. International Organization for Standardization, 2014. 31 p.

17. ISO/IEC 27004:2009. Information technology. Security techniques. Information security management systems. Measurement. International Organization for Standardization, 2009. 55 p.

18. ISO/IEC 27005:2011. Information technology. Security techniques. Information security management systems. International Organization for Standardization, 2011. 68 p.

19. ISO 19011:2011. Guidelines for auditing management systems. International Organization for Standardization, 2011. 44 p.

20. Roy Y. V., Mazur N. P., Skladannyi P. M. Аудит інформаційної безпеки – основа ефективного захисту підприємства // Кібербезпека: освіта, наука, техніка. 2018. № 1 (1). С. 86–93. URL : https://csecurity.kubg.edu.ua/index.php/journal/article/view/23 (дата звернення: 22.06.2022).

21. Башинська І. О. Основні порушники та загрози інформаційної безпеки промислових підприємств // Problems of social and economic development of business: Collective monograph. Montreal : Publishing house «BREEZE», 2014. P. 262–267.

22. Kryvoruchko O., Desiatko A., Synichuk O. Моделювання інформаційної системи проведення незалежного аудиту інформаційної безпеки. *Управління розвитком складних систем*. 2020. № 43. С. 67–75.

23. Aguarón J., Escobar M. T., Moreno-Jiménez J. M. Consistency stability intervals for a judgement in AHP decision support systems // European Journal of Operational Research. 2003. Vol. 145. № 2. P. 382–393.

24. De Wilde P. Neural network models: theory and projects // Springer Science & Business Media. 2013.

25. Lakhno V. et al. Information Security Audit Method Based on the Use of a Neuro-Fuzzy System. In: Silhavy R., Silhavy P., Prokopova Z. (eds) Software Engineering Application in Informatics. CoMeSySo 2021. Lecture Notes in Networks and Systems, vol 232. Springer, Cham.

26. Langner R. Stuxnet: Dissecting a cyberwarfare weapon // IEEE Security & Privacy. 2011. № 9 (3). P. 49–51.

27. Дзьобань О. П., Соснін О. В. Інформаційна безпека: нові виміри загроз, пов'язаних з інформаційно-комунікаційною сферою // Гуманітарний вісник Запорізької державної інженерної академії. 2015. № 61. С. 24–34.

28. Humphreys E. Information security management standards: Compliance, governance and risk management // Information security technical report. 2008. № 13(4). P. 247–255.

29. Kanatov M., Atymtayeva L., Yagaliyeva B. Expert systems for information security management and audit. Implementation phase issues // In 2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS, 2014, December). IEEE, 2014. P. 896–900.

30. Han D., Dai Y., Han T., Dai X. Explore Awareness of Information Security: Insights from Cognitive Neuromechanism // Computational Intelligence and Neuroscience. 2015. № 11. P. 11. https://dl.acm.org/doi/abs/10.1155/2015/762403 (дата звернення: 22.06.2022).

31. Andrade R., Torres J., Flores P. Management of information security indicators under a cognitive security model // In 2018 IEEE 8th annual computing and communication workshop and conference (CCWC, 2018, January). IEEE, 2018. P. 478–483.

32. Grediaga Á., Ibarra F., García F., Ledesma B., Brotóns F. Application of neural networks in network control and information security // In International Symposium on Neural Networks (2006, May). Berlin, Heidelberg : Springer, 2018. P. 208–213.

33. Mukkamala S., Janoski G., Sung A. Intrusion detection using neural networks and support vector machines // In Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (2002, May, Cat. No. 02CH37290). IEEE, 2002. Vol. 2. P. 1702–1707.

34. Kirta T., Kivimaab J. Optimizing it security costs by evolutionary algorithms // In Conference on Cyber Conflict Proceedings 2010. P. 145–160.

35. Lysenko S., Bobrovnikova K., Shchuka R., Savenko O. A cyberattacks detection technique based on evolutionary algorithms // In 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT). IEEE, 2020. P. 127–132.

36. Barankova I. I., Mikhailova U. V., Kalugina O. B. Analysis of the Problems of Industrial Enterprises Information Security Audit. In: Radionov A., Karandaev A. (eds) Advances in Automation. RusAutoCon 2019. Lecture Notes in Electrical Engineering, Springer, Cham, 2020. vol. 641.

37. Steinbart P. J., Raschke R. L., Gal G., Dilla W. N. The influence of a good relationship between the internal audit and information security functions on information security outcomes // Accounting, Organizations and Society. 2018. № 71. P. 15–29.

38. Mataracioglu T., Ozkan S. Governing information security in conjunction with COBIT and ISO 27001. arXiv preprint arXiv:1108.2150. 2011.

39. Steinbart P. J., Raschke R. L., Gal G., Dilla W. N. The relationship between internal audit and information security: An exploratory investigation // International Journal of Accounting Information Systems. 2012. № 13 (3). P. 228–243.

40. Montesino R., Fenz S. Information security automation: how far can we go? // In Sixth International Conference on Availability, Reliability and Security (2011, August). IEEE, 2011. P. 280–285.

41. Au C. H., Fung W. S. Integrating Knowledge Management into Information Security: From Audit to Practice // International Journal of Knowledge Management (IJKM). 2019. № 15 (1). P. 37–52.

42. Stafford T., Deitz G., Li Y. The role of internal audit and user training in information security policy compliance // Managerial Auditing Journal. 2018. № 33 (4). P. 410–424.

43. Pereira T. S. M., Santos H. A Security Framework for Audit and Manage Information System Security // In 2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (2010, August). IEEE, 2010. Vol. 3. P. 29–32.

44. Хох В. Д., Мелешко Є. В., Смірнов О. А. Дослідження методів аудиту систем управління інформаційною безпекою // Системи управління, навігації та зв'язку : зб. наук. пр. 2017. № 1 (41). С. 38–42.

45. Волот О. І. Інформаційна та кібернетична безпека сучасного підприємства: забезпечення та моделювання // Центрально-український наук. вісник. Економічні науки. 2019. № 3 (36). С. 238–247.

46. Аудит інформаційної безпеки на основі застосування нейро-нечіткої системи / В. Лахно, А. Блозва, Є. Часновський та ін. // Технічні науки та технології. 2021. № 3 (25). P. 125–137.

47. Казакова Н. Ф., Плешко Е. А., Айвазова К. Б. Міжнародна регламентація правового регулювання та стандартизації аудиту інформаційної безпеки // Вісник Східноукраїнського Нац. ун-ту імені Володимира Даля. 2013. № 15 (1). С. 172–181.

48. Юдін О. К., Зюбіна Р. В., Матвійчук-Юдіна О. В. Сучасні практики впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури // Наукоємні технології. 2019. № 1. С. 36–43.

49. Akhmetov B., Lakhno V., Akhmetov B., & Alimseitova Z. Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity // In Proceedings of the Computational Methods in Systems and Software (2018, September). Springer, Cham, 2018. P. 162–171.

50. Lois P., Drogalas G., Karagiorgos A., Thrassou A., Vrontis D. Internal auditing and cyber security: audit role and procedural contribution // International Journal of Managerial and Financial Accounting. 2021. № 13 (1). P. 25–47.

51. Roldán-Molina G., Almache-Cueva M., Silva-Rabadão C., Yevseyeva I., Basto-Fernandes V. A decision support system for corporations cybersecurity management // In 2017 12th Iberian Conference on Information Systems and Technologies (CISTI). IEEE, 2017. P. 1–6.

52. Calderon T. G., Cheh J. J. A roadmap for future neural networks research in auditing and risk assessment // International Journal of Accounting Information Systems. 2002. № 3 (4), P. 203–236.

53. Gaganis C., Pasiouras F., Doumpos M. Probabilistic neural networks for the identification of qualified audit opinions // Expert Systems with Applications. 2007. № 32 (1). P. 114–124.

54. Мельниченко О. В. Аудит інформаційної безпеки банку при роботі з електронними грошима. *Проблеми економіки*. 2013. № 4. С. 341–347.

55. Markowski A. S., Mannan M. S. Fuzzy logic for piping risk assessment (pfLOPA) // Journal of loss prevention in the process industries. 2009. № 22 (6). P. 921–927.

56. Grace A. M., Williams S. O. Comparative analysis of neural network and fuzzy logic techniques in credit risk evaluation // International Journal of Intelligent Information Technologies (IJIIT). 2016. № 12 (1). P. 47–62.

57. Mokhor V., Honchar S. F. The Idea of the Construction of the Algebra of Risks on the Basis of the Theory of Complex Numbers // Electronic modeling. 2018. № 40 (4). P. 107–111.

58. Mokhor V., Honchar S., Onyskova A. Cybersecurity Risk Assessment of Information Systems of Critical Infrastructure Objects // In 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T). IEEE, 2020. P. 19–22.

59. Akhmetov B. S., Lakhno V. A., Ydyryshbayeva M. B., Yagaliyeva B. E., Baiganova A. V., Akhanova M. B., Tashimova A. K. Application of bayesian networks in the decision support system during the analysis of cyber threats // Journal of Theoretical and Applied Information Technology. 2021. № 99 (4). P. 884–893.

60. US National Vulnerability Database. URL : https://nvd.nist.gov/

ПІСЛЯМОВА

Зростання ролі інформації у розвитку суспільства в цілому та економічних систем різного рівня зокрема призводить до необхідності з'ясування нових теоретико-методологічних засад та практичних завдань, пов'язаних з формуванням корпоративної інформаційної безпеки, які полягають у з'ясуванні та уточненні понятійно-категоріального апарату, вивчення механізмів захисту корпоративної інформації, оцінюванні їх економічної ефективності.

Ускладнення інформаційних потоків, засобів їх забезпечення, зростання обсягів інформації в системі прийняття управлінських рішень обумовило появу нового поняття «корпоративний інформаційний простір», який ми визначаємо як організовану систему інформації та інформаційних процесів корпорації, котра є станом та результатом її функціонування, способом її розвитку та представлення.

Корпоративний інформаційний простір впродовж існування та розвитку корпоративних структур пройшов складний процес еволюції, в межах якого нами виокремлено три принципові етапи: «паперовий», «автоматизований» і «мережевий». Останній етап, що триває до цього часу, характеризується глобальним характером, високим рівнем інтенсивності та швидкості поширення інформації, її «надлишковим» характером, зниженням витрат часу на оброблення та аналіз інформації, зростанням витрат на убезпечення інформаційного простору, суттєвим впливом на трансформацію бізнес-моделі, організаційної структури підприємства, способу виробництва товарів та послуг. Таким чином, можна говорити про значне посилення впливу корпоративного інформаційного простору на розвиток підприємства.

Корпоративний інформаційний простір має складну структуру, в межах якої нами виокремлено чотири принципові компоненти: суб'єкти, семантичну складову (інформаційний контент), інформаційну інфраструктуру, регламенти та норми. Центральним та системоутворювальним компонентом корпоративного інформаційного простору є його суб'єкти, серед яких варто виокремити первинний та вторинний рівні. Первинним суб'єктом 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 умовно поділяємо на інформаційні поля; інформаційний процес; віртуальну реальність; інформаційну культуру.

В умовах цифровізації суспільства, зростання вагомої ролі інформації як у житті людини, так і у функціонуванні підприємства в геометричній прогресії, збільшуються ризики втрати інформації, що потребує формування корпоративної інформаційної безпеки – стану захищеності інтересів підприємства від недобросовісних дій (умисних та неумисних) щодо корпоративної інформації, спрямованих на всі компоненти корпоративного інформаційного простору. З'ясовано роль та місце захисту корпоративної інформації у процесі формування інформаційної безпеки та економічної ефективності функціонування підприємства.

Корпоративне інформаційне поле характеризується важливими параметрами, зокрема: інтенсивністю інформаційного обміну, насиченістю інформаційних полів, рівнем цифровізації, цифровою компетентністю персоналу, рівнем корпоративної інформаційної культури, рівнем інноваційності КІП, захищеністю КІП та якістю його регламентації. Висока якість параметрів корпоративного інформаційного поля дає змогу на якісному рівні виконувати йому такі функції: інтегрувальну, комунікативну, актуалізуючу, соціальну, навчальну, інноваційну та акселеруючу. З іншого боку, виконання корпоративним інформаційним простором своїх функцій на якісно високому рівні дозволяє в цілому підвищувати результати діяльності за рахунок більш ефективного використання всього пулу ресурсів, а також вдосконалювати параметри корпоративного інформаційного простору.

Захист корпоративної інформації пов'язаний із захистом корпративного інформаційного поля від різноманітних загроз з метою збереження високої якості його параметрів та забезпечення можливості ефективно виконувати ним свої функції. З цією метою в роботі 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, які спрямовуються на порушення функціонування корпоративного інформаційного поля і передбачають їх ідентифікацію, аналіз, запобігання та нейтралізацію. Представлено

концепт-модель місця захисту корпоративної інформації у забезпеченні ефективного функціонування підприємства.

Захист корпоративної інформації потребує розроблення дієвих механізмів протидії загрозам інформаційній безпеці підприємства, які узгоджуватимуться з сучасними концептуальними положеннями ефективності функціонування економічних систем. На основі аналізу, узагальнення та систематизації сучасних підходів до тлумачення змісту економічної ефективності у дослідженні розмежовано поняття «економічна ефективність функціонування підприємства» та «економічна ефективність управління підприємством» і розглянуто видову трансформацію останньої.

Ґрунтуючись на систематизації основних характеристик поняття «управління» та підходів до його організації з позицій системного підходу визначено економічну ефективність управління підприємством як інтегровану характеристику ефективності (міри отриманого ефекту до ресурсів/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, в межах якої чільне місце посідає економічна ефективність захисту корпоративної інформації – міра економічного ефекту витрачених ресурсів на реалізацію системи заходів з ідентифікації, аналізу, запобігання та нейтралізації загроз порушення функціонування корпоративного інформаційного поля.

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

Зважаючи на те, що система корпоративної інформаційної безпеки спрямована на забезпечення стабільних фінансових результатів та стійкого розвитку підприємства, нарощення його вартості (тобто підпорядкована основній меті та завданням його економічної діяльності), формування цієї системи базується на теорії економічних механізмів та має бути інтегрованим у механізм

управління підприємством, включаючи не лише економічні важелі, а й економічні методи. Водночас широке застосування спеціалізованих інформаційних технологій потребує включення до складу такого механізму низки технічних методів.

Серед інструментів механізму формування корпоративної інформаційної безпеки вагому роль відіграє комплаєнс, який доцільно запроваджувати у формі «Risk based approach», що заснований на аналізі ризиків, в узгодженні з іншими інструментами формування корпоративної інформаційної безпеки. У межах технічних методів формування інформаційної безпеки варто виокремити методи моделювання корпоративної безпеки та автоматизовані системи управління інформаційними ризиками. Суб'єкт господарювання в процесі формування політики управління корпоративною інформаційною безпекою може обирати за основу будь-який з варіантів зазначених підходів, розробляти власний підхід, комбінувати елементи окремих технологій тощо.

Корпоративна інформаційна безпека може бути представлена сукупністю певним чином організованих та спільно використовуваних ресурсів, як-от технічні, технологічні, кадрові, інформаційні, і навіть організаційно-економічні. Загальний обсяг та структура цих ресурсів, система їх взаємодії дозволять відповісти на питання про здатність виробничої системи до досягнення тих чи інших цілей, тобто визначити її прогресивність. Запропонований варіант прогресивності корпоративної політики інформаційної безпеки відповідає такому критерію, завдяки якому корпоративна структура має можливість забезпечити своєчасне та якісне задоволення потреб суспільства, що розвиваються, з мінімальними сукупними витратами живої та уречевленої праці при обов'язковому дотриманні соціальних умов, вимог до стану довкілля та обмежень засобів розширення ресурсів корпорації.

Для оцінювання ефективності корпоративної інформаційної безпеки, що забезпечується на стратегічному рівні, доцільно застосовувати коефіцієнт рентабельності інвестицій у КІБ як співвідношення середньорічного відверненого збитку до середньорічного обсягу інвестицій у КІБ, частку програмних та технічних засобів, розроблених для цього підприємства. У межах оперативно-тактичного контуру управління як основні показники пропонується використовувати коефіцієнти продуктивності, рентабельності, віддачі інформаційної системи, які обчислюються за

показниками чистої виручки, чистого прибутку та відверненого збитку відповідно до середньорічної вартості володіння. Як допоміжні показники на оперативно-тактичному рівні пропонується оцінювати темпи зростання кількості інцидентів витоку конфіденційної інформації, заходів з поліпшення інформаційних процесів та порушення регламентів зберігання та передавання інформації. На основі зазначених показників пропонується до використання інтегральний показник економічної ефективності КІБ. Запропонований підхід до оцінювання економічної ефективності КІБ грунтується на поєднанні методів ТОС, інвестиційного аналізу, імітаційного моделювання, коефіцієнтного, динамічного та інтегрального аналізу, методу Ісікави, пропонує чітку послідовність та логіку застосування запропонованих показників, деталізованих за контурами управління, ієрархічністю, що дозволяє структурувати та автоматизувати процес оцінювання економічної ефективності КІБ, здійснювати його на постійній основі. Результати його застосування є базою для подальшого вдосконалення як самого процесу формування КІБ, так і підвищення його економічної ефективності.

За результатами проведеного дослідження запропоновано підхід до процедури формалізації ознакового функціонального подання неправомірних дій комп'ютерного зловмисника у ході реалізації функцій НСД до ресурсів ІС компаній та підприємств. Виконано формалізацію ієрархічної схеми формування множини ознак НСД до ресурсів ІС підприємства. Отримана ієрархічна структура може бути основою для подальшого синтезу інтелектуальної системи виявлення спроб НСД в умовах важкозрозумілих ознак або їх невеликої кількості. Це дасть змогу ефективно реалізувати первинну формалізацію неправомірних дій комп'ютерних зловмисників для подальшого математичного опису параметра ймовірності НСД, наприклад, на основі Марківських ланцюгів.

Запропоновано методологічний підхід, що дозволяє автоматизувати та систематизувати прояви ефекту захищеності інформації від витоків по технічних каналах. Доповнено імовірнісну модель виконання загроз, яка дає можливість на основі запропонованого програмного забезпечення залучати кількох експертів для оцінки актуальності загроз витоку інформації щодо ТКПІ в умовах динамічного вдосконалення ТЗР. Розроблене ПЗ у комплексі з програмним забезпеченням, яке призначене для

оцінки ризиків втрати інформації, дозволяє комплексно оцінити рівень захищеності ТКПІ підприємства. Розроблене ПЗ сприяє зниженню витрат на проведення вузькоспеціальних досліджень у питаннях щодо оцінювання актуальності загроз витоку інформації з ТКПІ в умовах динамічного вдосконалення ТЗР. Таким чином, було досягнуто основної мети роботи – автоматизувати процедуру оцінювання актуальності загроз витоку інформації з ТКПІ в умовах динамічного вдосконалення ТЗР та вдосконалити процес оцінювання захищеності приміщень підприємств шляхом використання релевантних оцінок експертів.

У процесі алгоритмізації процедур, пов'язаних з обробленням та аналізом подій ІБ у межах їх ЖЦ, та відповідно до принципу цілісності об'єкти захисту (зокрема, КІС підприємств) необхідно аналізувати у різних ракурсах. Такий аналіз починається з окремих компонентів об'єкта захисту та закінчується його аналізом загалом, у тому числі – зовнішнього середовища. Реалізація принципів цілісності та подібності подій ІБ у ході управління адаптивними параметрами процедур моніторингу та оброблення подій ІБ у межах їх ЖЦ полягає у побудові взаємних відображень між завданнями ІБ та відповідними методами їхнього вирішення. У цьому основну роль відіграють доступні дані, необхідні для реалізації потенціалу конкретного методу чи моделі у процесах оброблення та аналізу подій ІБ у межах їх ЖЦ. Керуючись подібними відображеннями, можна оптимізувати схеми моніторингу. За такої оптимізації важливо сконцентрувати увагу аналітика з інформаційної безпеки 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 інформаційної безпеки, включаючи процедури оброблення та аналізу подій ІБ у межах їх ЖЦ, відповідає принципам ієрархічної пов'язаності, цілісності та подібності подій інформаційної безпеки.

Запропоновано доповнення до способу організації процесу управління подіями інформаційної безпеки для підприємства. На відміну від наявних рішень, деталізований алгоритм підпроцесу «Оброблення подій». Ця деталізація має комплексний характер. Крім того, вона охоплює життєвий цикл події ІБ. Виконані дослідження дозволяють на практиці заповнити потенційні прогалини інформації під час створення системи управління

інформаційної безпеки підприємства. Додатковою перевагою запропонованого рішення є можливість задіяння цього підпроцесу як незалежного, що дає змогу спростити процедуру управління ІБ підприємства загалом і знизити витрати на її побудову для невеликих суб'єктів господарювання.

Встановлено, що оцінювати рівень інформаційної безпеки для об'єкта інформатизації доцільно на основі оцінювання результативності безлічі критеріїв методу аналізу ієрархій. Показано, що як метрики оцінювання можна використовувати як стандартні чисельні метрики ІБ, так і метрики, запропоновані експертами з інформаційної безпеки й погоджені з менеджментом ОБІ. З урахуванням цього запропоновано модифікований метод аналізу ієрархій, який відрізняється від стандартного, застосуванням апарату теорії нечітких множин та нейронних мереж, що дає можливість менеджменту приймати обґрунтовані управлінські рішення у сфері ІБ ОБІ. Отримані рішення спрямовані на підвищення не лише власне інформаційної безпеки об'єкта інформатизації, а й у кінцевому підсумку оптимізують систему управління ОБІ, скорочують витрати й підвищують ефективність бізнес-процесів ОБІ загалом. Показано, що застосування математичного апарату методу аналізу ієрархій та відповідного програмного забезпечення, зокрема розробленої інтелектуальної системи, дозволяє підвищити ступінь достовірності результатів проведення комплексного аудиту інформаційної безпеки ОБІ, причому це твердження справедливе як для процедур внутрішнього аудиту ІБ об'єкта інформатизації, так і для зовнішнього.

Доповнено метод аудиту інформаційної безпеки, заснований на автоматизації процедур аудиту шляхом залучення для оцінки ризиків ІБ апарату БМ та ШНМ. Показано, що така комбінація дозволяє оперативно в ході аудиту інформаційної безпеки визначати актуальні ризики ІБ об'єкта інформатизації. При цьому як вихідна інформація можуть використовуватися дані з датчиків/сенсорів різних апаратно-програмних засобів захисту інформації в сегментах РОМ ОБІ. Показано, що автоматизація процедур АІБ на основі застосування БМ та ШНМ дає змогу адміністратору інформаційної безпеки розподілених обчислювальних мереж своєчасно й динамічно реагувати на загрози.

Наукове видання

ЧУБАЄВСЬКИЙ Віталій Іванович

КОРПОРАТИВНА ІНФОРМАЦІЙНА БЕЗПЕКА

Монографія

Редактор О. Г. Пащенко
Комп'ютерне верстання Л. І. Власової
Дизайн обкладинки Г. В. Поліщук

Формат 60х84/16. Ум. друк. арк. 14,05. Тираж 300 пр. Зам. 242.

Видавець і виготовлювач
Київський національний торговельно-економічний університет
вул. Кіото, 19, м. Київ-156, Україна, 02156

Свідоцтво суб'єкта видавничої справи серія ДК № 7656 від 05.09.2022