МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова
праця на правах рукопису

ЧУБАЄВСЬКИЙ ВІТАЛІЙ ІВАНОВИЧ

330.131.5-049.65:[334.72:004.9

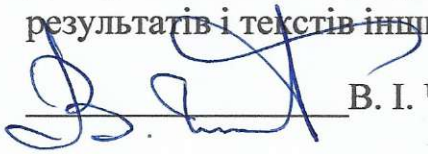
ДИСЕРТАЦІЯ

ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ СИСТЕМ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ

Спеціальність: 08.00.04 – економіка та управління підприємствами
(за видами економічної діяльності)
Галузь знань – економічні науки

Подається на здобуття наукового ступеня: доктора економічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.



_____В. І. Чубаєвський

Київ – 2023

АНОТАЦІЯ

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

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

У дисертації досліджено теоретико-методологічні засади та методичні підходи до формування економічно-ефективної системи захисту корпоративної інформації. За результатми дослідження визначено основні сутнісні характеристики корпоративного інформаційного простору: безперервний процес виробництва та споживання інформації, результат та спосіб пізнання дійсності, суб'єктність, системність та організованість, фактор розвитку суб'єкта та об'єкт управління та визначено його зміст як сукупність інформації та інформаційних процесів, яка є станом, засобом та результатом функціонування системи, чинником її розвитку та формою представлення. Виходячи із цього, визначено сутність корпоративного інформаційного простору як організовану систему інформації та інформаційних процесів корпорації, яка є станом та результатом її функціонування, способом її розвитку та представлення. На основі аналізу та узагальнення сучасних досліджень ідентифіковано три етапи еволюції корпоративного інформаційного простору: паперовий (до середини 70-х років), автоматизований (із середини 70-х років до початку 90-х років), мережевий (із початку 90-х по теперішній час). На сучасному етапі корпоративний інформаційний простір характеризується глобальністю, відсутністю фізичних меж зберігання інформації, високою інтенсивністю та швидкістю її поширення, надлишковістю, уразливістю та зростанням витрат на захист, посиленим впливом на трансформацію корпоративних бізнес-моделей. З'ясовано, що корпоративний інформаційний простір характеризується єдністю та взаємообумовленістю окремих елементів. У структурі корпоративного інформаційного простору запропоновано виокремлювати чотири принципові компоненти: суб'єкти, семантичну складову

(інформаційний контент), інформаційну інфраструктуру, регламенти та норми. Обгрунтовано зміст та склад окремих компонентів.

На основі аналізу та узагальнення сучасних досліджень визначено зміст корпоративної інформаційної безпеки як стан захищеності інтересів підприємства від недобросовісних дій (умисних та неумисних) щодо корпоративної інформації, що спрямовані на всі компоненти корпоративного інформаційного простору та доведено чіткий взаємозв'язок між захистом корпоративної інформації та досягненням високих економічних результатів функціонування підприємства, які і є відображенням його інтересів. Сформульовано концептуальне бачення місця захисту корпоративної інформації в забезпеченні ефективного економічного розвитку підприємства на основі доведеної взаємообумовлюючої залежності між параметрами та функціями корпоративного інформаційного простору; розширено перелік параметрів КІП такими характеристиками як рівень цифровізації КІП, цифрові компетентності персоналу, рівень інноваційності інформаційної інфраструктури, рівень корпоративної інформаційної культури, ступінь захищеності та якість регламентації КІП; ідентифіковано систему функцій КІП (інтегруюча, комунікативна, актуалізуюча, соціальна, навчальна, інноваційна, акселеруюча) та сформульовано авторське бачення сутності захисту корпоративної інформації як системи принципів, методів та процесів протидії загрозам інформаційній безпеці підприємства, які спрямовуються на порушення функціонування КІП і передбачають їх ідентифікацію, аналіз, попередження та нейтралізацію.

Представлено теоретичний концепт сутності економічної ефективності управління підприємством на основі нової авторської трактовки змісту «управління підприємством» як інтегральної характеристики сукупності функціональних підрозділів, управлінських процесів, управлінських рішень, управлінського персоналу, центрів фінансової відповідальності в межах єдиного корпоративного інформаційного простору та відповідно сформульованої її видової класифікації з визначеними сутністю та місцем у ній економічної ефективності захисту корпоративної інформації, що дозволило систематизувати основні

методичні підходи до оцінювання ефективності захисту корпоративної інформації. Отже, економічну ефективність захисту корпоративної інформації запропоновано визначати як міру економічного ефекту витрачених ресурсів на реалізацію системи заходів з ідетифікації, аналізу, попередження та нейтралізації загроз порушення функціонування корпоративного інформаційного поля.

На основі аналізу та розвитку наявного доробку визначено сутність концепції формування корпоративної інформаційної безпеки як систему поглядів на організацію та забезпечення такої безпеки, що відображається через обрану методологію формування, окреслені принципи та розроблений механізм забезпечення. Таким чином, ідентифіковано, що концепція формування корпоративної інформаційної безпеки має містити три принципові структурні компоненти: методологічну основу, принципи, механізм, які знаходяться в логічному зв'язку та підпорядкуванні. Відповідно до сформульованого бачення обґрунтовано авторську концепцію формування корпоративної інформаційної безпеки, що ґрунтується на позитивістській та нормативній економічних теоріях, поєднанні системного, процесного, проектного підходів в управлінні та концепції динамічних компетентностей, сформульованій системі принципів та механізмі забезпечення, що сприятиме більш комплексному розумінню проблем формування інформаційної безпеки та забезпеченню комплексності заходів щодо її забезпечення.

Доведено, що політика інформаційної безпеки корпорацій є елементом корпоративного управління і випливає із 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. З'ясовано, що послідовне узгодження політики інформаційної безпеки може бути досягнуте шляхом конвергенції корпоративної політики інформаційної безпеки з іншими бізнес-політиками організації в межах циклу стратегічного управління. У дисертації систематизовано та узагальнено напрями корпоративної

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

Вивчення сучасних підходів до оцінювання економічної ефективності корпоративної інформаційної безпеки дозволило зробити висновок про складність застосування єдиної наявної методики для формування вичерпного висновку щодо ефективності корпоративної інформаційної безпеки та виявити ряд проблем, які потребують вирішення, зокрема: відсутність чітко сформульованих принципів оцінювання та систематизації показників економічної ефективності та їх критеріальних значень, відсутність рекомендацій щодо логічної послідовності аналізу окремих показників та підходів до формування інтегрального або узагальнюючого показника економічної ефективності корпоративної інформаційної безпеки. З метою вирішення цих проблем у дисертації розроблено методологічний підхід до оцінювання економічної ефективності захисту корпоративної інформації, який включає: принципи оцінювання та систематизації показників; систему часткових показників економічної ефективності та критеріальну шкалу їх інтерпретації; узагальнюючу оцінку економічної ефективності захисту корпоративної інформації на основі поєднання інтегрального показника та показника прогресивності розвитку системи захисту корпоративної інформації (КІ), структурно-логічну послідовність етапів оцінювання, що створює основу для запровадження дієвих систем оцінювання економічної ефективності захисту корпоративної інформації. У межах зазначеного підходу пропонується також оцінювання ступеня досягнення максимально можливого прибутку корпоративної структур за рахунок визначення потенційних можливостей системи

захисту корпоративної інформації, який сприяє отриманню своєчасної та достовірної інформації як основи для прийняття та реалізації суб'єктами безпеки тактичних і стратегічних управлінських рішень та дозволяє надавати керівникам корпорацій комплексну оцінку ефективності управлінських дій щодо використання інноваційних технологій інформаційної безпеки на всіх ієрархічних рівнях організаційної структури управління.

Доведено, що з ускладненням сценаріїв проведення кібернетичних атак, особливо таргетованих, розширюється і простір ознак, що характеризують способи отримання несанкціонованого доступу до інформаційних ресурсів підприємств. Оскільки простір ознак несанкціонованого доступу постійно розширюється, навіть кваліфікованим експертам у сфері інформаційна безпека без підтримки спеціалізованих програмних продуктів при прийнятті рішення в подібних питаннях обійтися складно. Це зумовлює необхідність продовження досліджень у напрямі інтелектуалізації на основі ІТ процедури первинної формалізації неправомірних дій комп'ютерних зловмисників, які роблять спроби отримати несанкціонований доступ до ІС суб'єктів господарської діяльності. У дисертації розроблено методологічний підхід до процедури формалізації ознакового функціонального подання неправомірних дій комп'ютерного зловмисника в ході реалізації функцій несанкціонованого доступу до ресурсів ІС підприємств за рахунок формалізації ієрархічної схеми формування множини ознак несанкціонованого доступу до ресурсів ІС підприємства; отримана ієрархічна структура є основою для подальшого синтезу інтелектуальної системи виявлення спроб несанкціонованого доступу в умовах важкозрозумілих ознак або їх невеликого числа, що дозволяє ефективно реалізувати первинну формалізацію неправомірних дій комп'ютерних зловмисників для подальшого математичного опису параметра ймовірності несанкціонованого доступу.

Удосконалено методологічний підхід, що дозволяє автоматизувати та систематизувати прояви ефекту захищеності інформації від витоків технічними каналами шляхом доповнення ймовірнісної моделі виконання загроз, яка дозволяє на основі запропонованого програмного забезпечення (ПЗ) залучати кілька

експертів для оцінки актуальності загроз витоку інформації щодо ТКПІ в умовах динамічного вдосконалення ТЗР.

З’ясовано зростаючий тренд кількості та варіативності видів кібератак. Виявлено, що найбільш поширеними видами кібератак, з якими стикаються невеликі підприємства – це фішинг, вторгнення в мережу компанії, випадки ненавмисного витоку інформації, розкрадання пристроїв, помилкова конфігурація мережі та її захисту. З’ясовано, що в Україні найбільше від кібератак потерпають державні установи, промислові підприємства, медичні заклади, фінансові установи, заклади освіти і науки та та підприємства торгівлі. Спостерігається зростання інтересу менеджменту компаній до проблем захисту корпоративної інформації та практичного впровадження програм навчання персоналу діям при кібератаках.

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

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

Доведено, що в процесі оцінки ефективності функціонування СЗІ об’єкта господарювання найбільш доцільно застосовувати ймовірнісні методи. Відповідно до цих методів прийнятний для сторони захисту гарантований рівень ІБ

трансформуватиметься в довірчі ймовірності відповідних метрик захисту інформації та КБ ОБІ підприємства. Обгрунтовано методичні підходи до моделювання системи оцінювання рівня інформаційної безпеки (ІБ) для об'єктів інформатизації (ОБІ), яка на відміну від існуючих ґрунтується на методі аналізу ієрархій (МАІ) та дозволяє оцінювати її результативність за визначеними критеріями.

Обгрунтовано необхідність розроблення та впровадження дієвого організаційно-економічного забезпечення як основи практичної реалізації політики захисту корпоративної інформації. Розроблено методологічний підхід до формування організаційно-економічного забезпечення ефективного захисту корпоративної інформації як комплексу взаємоузгоджених елементів (заходів) різної спрямованості та частоти застосування, які перебувають у постійній взаємодії, виступають частиною економічного механізму інформаційної безпеки, реалізуються на різних контурах управління та інтегровані в систему загальнокорпоративного управління з метою досягнення визначених цілей та який на відміну від існуючих передбачає чітку систематизацію елементів за їх функціональним напрямом, можливістю впливу на КІБ, частотою застосування, контуром управління. Це дозволило окреслити систематизований комплекс практичних заходів із захисту корпоративної інформації, що підвищить обґрунтованість та ефективність їх запровадження в практичній діяльності. Обгрунтовано наукові підходи до створення моделі, що описує процедуру формалізації завдання оптимізації системи захисту інформації (СЗІ) суб'єкта господарської діяльності (підприємства), яка на відміну від існуючих передбачає математико-алгоритмічну та комп'ютерну підтримку процедури прийняття рішень у питаннях організаційно-економічного забезпечення ефективного захисту корпоративної інформації в контексті завдань менеджменту інформаційної безпеки (ІБ) підприємств. Запропонований підхід дає можливість стороні захисту максимально ефективно визначати параметри організаційного управління інфраструктурою СЗІ підприємства.

Розроблено та описано інтелектуальну систему оцінки загроз витоку інформації щодо ТКПІ (технічних каналів передачі інформації), в основу якої покладено метод аудиту інформаційної безпеки, заснований на автоматизації процедур аудиту шляхом залучення для оцінки ризиків інформаційної безпеки апарату Байєсовських мереж (БМ) та штучних нейронних мереж (ШНМ). Така система дозволяє підвищити ступінь достовірності результатів проведення комплексного аудиту ІБ ОБІ та комплексної оцінки ризиків, своєчасно реагувати на загрози адміністратору ІБ розподіленої обчислювальної мережі (РОМ). Сформульовано методичний підхід до процедури аудиту інформаційної безпеки (АІБ), який на відміну від існуючих забезпечує багатостороннє оцінювання інформаційної безпеки об'єктів інформатизації на основі поєднання стандартних чисельних та експертних метрик оцінювання ІБ, що дозволяє оперативно в ході аудиту інформаційної безпеки (АІБ) визначати актуальні ризики ІБ ОБІ та автоматизувати процедури АІБ на основі застосування Байєсовських мереж (БМ) і штучної нейронної мережі (ШНМ), а адміністратору ІБ розподіленої обчислювальної мережі (РОМ) своєчасно та динамічно реагувати на загрози.

Практична значущість отриманих результатів полягає в тому, що всі пропозиції доведено до практичних рекомендацій і може бути впроваджено в практику корпоративного управління. Результати наукового дослідження, що мають прикладний характер, набули практичного застосування в роботі Департаменту кіберполіції Національної поліції України, Ради Національної безпеки і оборони України, ТОВ «КАРМА ДІДЖИТАЛ ЛТД», Державної служби спеціального зв'язку та захисту інформації України, при викладанні дисциплін у Державному торговельно-економічному університеті.

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

ANNOTATION

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

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

The thesis examines the theoretical and methodological principles and methodological approaches to the formation of an economically efficient system of corporate information protection. According to the results of the study, the main essential characteristics of the corporate information space were determined: the continuous process of production and consumption of information, the result and way of knowing reality, subjectivity, systematicity and organization, the development factor of the subject and the object of management, and its content was determined as a collection of information and of information processes, which is the state, means and result of the functioning of the system, the factor of its development and the form of representation. Based on this, the essence of the corporate information space is determined as an organized system of information and information processes of the corporation, which is the state and result of its functioning, the way of its development and presentation. Based on the analysis and generalization of modern research, three stages of the evolution of the corporate information space have been identified: paper (until the mid-70s), automated (from the mid-70s to the beginning of the 90s), network (from the beginning of the 90s to the present time). At the current stage, the corporate information space is characterized by globality, the absence of physical boundaries of information storage, high intensity and speed of its dissemination, redundancy, vulnerability and the growth of protection costs, increased influence on the transformation of corporate business models. It was found that the corporate information space is characterized by the unity and interdependence of individual elements. In the structure of the corporate information space, it is proposed to distinguish four principle components: subjects, semantic component (information content), information infrastructure, regulations and norms. The content and composition of individual components are substantiated.

Based on the analysis and generalization of modern researches, the content of corporate information security is determined as a state of protection of the company's interests from unscrupulous actions (intentional and unintentional) in relation to corporate information aimed at all components of the corporate information space, and a clear relationship between the protection of corporate information and the achievement of high economic results of the operation of the enterprise, which are a reflection of its interests. A conceptual vision of the place of protection of corporate information in ensuring effective economic development of the enterprise is formulated based on the proven interdependence between the parameters and functions of the corporate information space (CIS); the list of CIS parameters has been expanded with such characteristics as the level of digitalization of CIS, digital competences of personnel, the level of innovativeness of information infrastructure, the level of corporate information culture, the degree of security and the quality of regulation of CIS; the system of CIS functions is identified (integrating, communicative, actualizing, social, educational, innovative, accelerating) and the author's vision of the essence of corporate information protection is formulated as a system of principles, methods and processes for countering threats to the information security of the enterprise, which are aimed at disrupting the functioning of CIS and provides for their identification , analysis, prevention and neutralization.

The theoretical concept of the essence of the economic efficiency of enterprise management is presented on the basis of the author's new interpretation of the meaning of "enterprise management" as an integral characteristic of a set of functional units, management processes, management decisions, management personnel, centers of financial responsibility within the framework of a single corporate information space and its correspondingly formulated species classification with determined by the essence and the place in it of the economic effectiveness of corporate information protection, which made it possible to systematize the main methodical approaches to evaluating the effectiveness of corporate information protection. Accordingly, the economic efficiency of corporate information protection is proposed to be determined as a measure of the economic effect of resources spent on the implementation of a system of measures for

identification, analysis, prevention, and neutralization of threats to the functioning of the corporate information field.

Based on the analysis and development of the existing work, the essence of the concept of the formation of corporate information security is defined as a system of views on the organization and provision of such security, which is reflected through the chosen methodology of formation, the outlined principles and the developed mechanism of provision. Thus, it was identified that the concept of forming corporate information security should contain three fundamental structural components: a methodologist ical basis, principles, mechanism, which are in logical connection and subordination. In accordance with the formulated vision, the author's concept of the formation of corporate information security, which is based on positivist and normative economic theories, a combination of system, process, project approaches in management and the concept of dynamic competences, a formulated system of principles and a provision mechanism, which will contribute to a more comprehensive understanding of the problems of the formation of information security safety and ensuring the comprehensiveness of measures to ensure it.

It is proven that the information security policy of corporations is an element of corporate governance and stems from strategic requirements for risk management and corporate governance. Information security of corporations must be implemented in accordance with business goals, which are characterized by a high level of dynamism, under the conditions of the need for continuous consistent coordination between the security policy and other areas of corporate business policy and strategies. It was found that the consistent coordination of the information security policy can be achieved by the convergence of the corporate information security policy with other business policies of the organization within the framework of the strategic management cycle. The dissertation systematizes and summarizes the directions of the corporate policy of information security through the justification of the dominant factors of forming its basis in the global business environment, highlighting such as: the creation of a single digital corporate business space, the increase in the speed of implementation of digital business strategies with a high level of technological deployment and intensity violations of the

stability of the corporate information protection system, on the basis of which, in contrast to the prevailing approaches, the need to increase the effectiveness of corporate information security policy due to its flexible response to changes in the strategic goals of corporate structures has been proven.

The study of modern approaches to evaluating the economic efficiency of corporate information security made it possible to conclude that it is difficult to apply the only available methodology to form a comprehensive conclusion on the effectiveness of corporate information security and to identify a number of problems that need to be solved, in particular: the lack of clearly formulated principles for evaluating and systematizing indicators of economic efficiency and their criterion values, lack of recommendations regarding the logical sequence of analysis of individual indicators and approaches to the formation of an integral or general indicator of the economic efficiency of corporate information security. In order to solve these problems, the dissertation developed a methodological approach to evaluating the economic effectiveness of corporate information protection, which includes: principles of evaluation and systematization of indicators; a system of partial indicators of economic efficiency and a criterion scale for their interpretation; a general evaluation of the economic efficiency of corporate information protection based on a combination of an integral indicator and an indicator of the progressivity of the CI protection system development, a structural and logical sequence of assessment stages, which creates the basis for the introduction of effective systems for evaluating the economic efficiency of corporate information protection. Within the limits of the mentioned approach, it is also proposed to assess the degree of achieving the maximum possible profit of corporate structures by determining the potential capabilities of the corporate information protection system, which contributes to obtaining timely and reliable information as a basis for the adoption and implementation of tactical and strategic management decisions by security subjects and allows managers to provide corporations, a comprehensive assessment of the effectiveness of management actions regarding the use of innovative information security technologies at all hierarchical levels of the organizational management structure.

It has been proven that as the scenarios of cyber attacks, especially targeted ones, become more complicated, the space of signs that characterize the methods of obtaining UA (unauthorized access) to the information resources of enterprises also expands. Since the space of features of UA is constantly expanding, even qualified experts in the field of IS (information systems) without the support of specialized software products when making decisions on such issues, it is difficult to get by. This makes it necessary to continue research in the direction of IT-based intellectualization of the procedure for the initial formalization of the illegal actions of computer criminals who are trying to obtain UA to the IS of business entities. The dissertation developed a methodological approach to the procedure of formalizing the characteristic functional presentation of illegal actions of a computer attacker in the course of implementing the functions of UA to enterprise IS resources due to the formalization of the hierarchical scheme of forming a set of signs of UA to enterprise IS resources; the obtained hierarchical structure is the basis for the further synthesis of an intelligent system for detecting UA attempts in difficult conditions skillful signs or a small number of them, which allows to effectively implement the primary formalization of illegal actions of computer attackers for the further mathematical description of the probability parameter of UA.

The methodological approach has been improved, allowing to automate and systematize the manifestations of the effect of protection of information against leaks through technical channels by adding a probabilistic model of threat execution, which allows, on the basis of the proposed software (software), to involve several experts to assess the relevance of threats of information leakage regarding TCIT (technical channels of information transmission) in conditions of dynamic improvement TMI (technical means of intelligence).

The growing trend of the number and variability of types of cyberattacks has been revealed. It was found that the most common types of cyberattacks faced by small businesses are phishing, intrusion into the company's network, cases of accidental information leakage, theft of devices, misconfiguration of the network and its protection. It has been found that in Ukraine, state institutions, industrial enterprises, medical institutions, financial institutions, scientific and educational institutions, and trade

enterprises suffer the most from cyber attacks. There is a growing interest of company management in the problems of protecting corporate information and the practical implementation of personnel training programs for actions in case of cyber attacks.

An approach to the organization of the information security (IS) event management process for the enterprise has been developed, which, unlike the existing ones, offers a complex detailing of the algorithm of the «Event processing» subprocess in accordance with the life cycle of IS events, which will allow in practice to fill potential information gaps when creating an enterprise IS management system , to implement this sub-process in an independent mode, to simplify the procedure for managing the IS of the enterprise as a whole and to reduce the costs of its construction for small enterprises.

An approach to adaptive monitoring of information security has been formulated, which includes procedures for processing and analyzing information security events within their life cycle, corresponds to the principles of hierarchical connection, integrity and similarity of IS events, which, unlike existing ones, is characterized by invariance in relation to the ways of implementing infrastructure solutions IS of the enterprise and, in particular, its CIS (corporate information systems). This allows, without changing the methodological toolkit, to scale this approach and adapt it to the ISMS (information security management systems) of various enterprises.

It has been proven that in the process of evaluating the effectiveness of the operation of the IPS (information protection systems) of the business object, it is most appropriate to use probabilistic methods. According to these methods, the guaranteed level of IS acceptable to the defense side will be transformed into the confidence probabilities of the relevant metrics of information protection and CS of IO (corporate security of informatization objects) enterprises. Methodical approaches to the modeling of the system for evaluating the level of information security (IS) for objects of informatization (IO), which, unlike the existing ones, are based on the method of analysis of hierarchies (MAH) and allow to evaluate its effectiveness according to defined criteria, are substantiated.

The need to develop and implement effective organizational and economic support as a basis for practical implementation of corporate information protection policy is

substantiated. A methodological approach to the formation of organizational and economic support for the effective protection of corporate information has been developed as a complex of mutually coordinated elements (measures) of different orientations and frequency of application, which are in constant interaction, are part of the economic mechanism of information security, are implemented on various management contours and are integrated into the system of general corporate management in order to achieve the specified goals and which, unlike the existing ones, provides for a clear systematization of elements according to their functional direction, the possibility of influencing the CIS, the frequency of application, and the control circuit. This made it possible to outline a systematized set of practical measures for the protection of corporate information, which will increase the validity and effectiveness of their implementation in practical activities. The scientific approaches to the creation of a model describing the procedure for formalizing the task of optimizing the information protection system (IPS) of an economic activity subject (enterprise) are substantiated, which, unlike the existing ones, provides mathematical-algorithmic and computer support for the decision-making procedure in matters of organizational and economic ensuring effective protection of corporate information in the context of information security (IS) management tasks of enterprises. The proposed approach enables the defense side to determine the parameters of the organizational management of the SSI infrastructure of the enterprise as efficiently as possible.

An intelligent system for assessing threats of information leakage regarding TCIT (technical channels of information transmission) has been developed and described, which is based on the information security audit method, based on the automation of audit procedures by involving the apparatus of Bayesian networks (BM) and artificial neural networks for the assessment of information security risks (ISR). This system allows to increase the degree of reliability based on the results of a complex IS audit of IO and a comprehensive risk assessment, respond in a timely manner to threats to the IS administrator of a distributed computing network (DCN). A methodical approach to the information security audit (ISA) procedure has been formulated, which, unlike the existing ones, provides a multi-faceted assessment of the information security of

informatization objects based on a combination of standard numerical and expert IS assessment metrics, which allows to quickly identify relevant issues during an information security audit (ISA) IS risks of IO and automate ISA procedures based on the application of Bayesian networks (BM) and artificial neural networks (ANN), and the IS administrator of a distributed computing network (DCN) to respond to threats in a timely and dynamic manner.

The practical significance of the obtained results lies in the fact that all proposals are reduced to practical recommendations and can be implemented in the practice of corporate management. The results of scientific research, which are of an applied nature, have gained practical application in the work of the Cyber Police Department of the National Police of Ukraine, the National Security and Defense Council of Ukraine, LTD «KARMA DIGITAL LTD», the State Service for Special Communications and Information Protection of Ukraine, in the teaching of disciplines in the State University of Trade and Economics.

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

Список опублікованих праць за темою дисертації

Наукові праці, у яких опубліковані основні наукові результати дисертації:

1. Чубаєвський В. І. Корпоративна інформаційна безпека : монографія / В.І. Чубаєвський. Київ : Держ. торг.-екон. ун-т, 2022. 272 с. (14 друк. арк.).
2. Чубаєвський В. Світова практика управління подіями інформаційної безпеки корпорацій. *Зовнішня торгівля: економіка, фінанси, право*. 2022. № 6. С. 73–82. (0,9 друк. арк.; наукове фахове видання України, категорія «Б»).
3. Чубаєвський В. І. Методичний підхід до оцінки економічної ефективності системи захисту корпоративної інформації. *Електронний журнал «Ефективна економіка»*. 2022. № 11. URL: https://nayka.com.ua/index.php/ee/article/view/730/738 (дата звернення: 21.11.2022). (0,6 друк. арк.; наукове фахове видання України, категорія «Б»).

4. Чубаєвський В. І. Прогресивність розвитку системи захисту корпоративної інформації. *Економіка та суспільство*. 2022. № 44. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1793 (дата звернення: 01.11.2022). (0,6 друк. арк.; наукове фахове видання України, категорія «Б»).
5. Чубаєвський В. Корпоративний інформаційний простір: сутність та еволюція. *Scientia Fructuosa (Вісник Київського національного торговельно-економічного університету)*. 2022. № 4. С. 84–97. (1,1 друк. арк.; наукове фахове видання України, категорія «Б»).
6. Чубаєвський В. І. Особливості формування системи захисту інформаційних ресурсів корпоративних структур. *Фаховий електронний науково-практичний журнал «Проблеми сучасних трансформацій. Серія: економіка та управління»*. 2022. № 5. URL: https://reicst.com.ua/pmt/article/view/2022-5-04-10/2022-5-04-10 (дата звернення: 01.11.2022). (0,5 друк. арк.; наукове фахове видання України, категорія «Б»).
7. Чубаєвський В. І. Методи управління корпоративною інформаційною безпекою. *Економіка та суспільство*. 2022. № 43. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1732 (дата звернення: 01.11.2022). (0,7 друк. арк.; наукове фахове видання України, категорія «Б»).
8. Chubaievskyi V., Tereshchenko E., Andryeyeva V., Stoianenko I. Model for assessing technological resources in the economic security of business in the process of European integration. *Information-analytical journal «Economics. Finances. Law»*. 2022. № 8. P. 13–16. (0,4 друк. арк.; особистий внесок автора: запропонована модель оцінки технологічних ресурсів економічної безпеки бізнесу – 0,1 друк. арк.; наукове фахове видання України, категорія «Б», Index Copernicus).
9. Lakhno V., Akhmetov B., Mohylnyi H., Chubaievskyi V., Kryvoruchko O., Desiatko A. Multi-criterial optimization composition of cyber security circuits based on genetic algorithm. *Journal of Theoretical and Applied Information Technologythis*. 2022. Vol. 100. № 7. P. 1996–2006. (0,9 друк. арк.; особистий внесок автора:

запропонована методика багатокритеріальної оптимізації витрат на систему захисту інформації об'єкта інформатизації, яка полягає в застосуванні генетичного алгоритму VEGA (Vector Evaluated Genetic Algorithm) – 0,1 друк. арк.; Scopus).

10. Chubaievskyi V., Blakyta H., Matusova O., Adamenko V., Hamula I. Assessing the state of the corporate information area in Ukraine. *Міждисциплінарні дослідження складних систем = Interdisciplinary Studies of Complex Systems* : Збірник наукових праць. Київ : Вид-во НПУ імені М. П. Драгоманова, 2022. № 20. С. 35–45. (1,0 друк. арк.; особистий внесок автора: запропоновано методичний інструментарій оцінки стану корпоративної інформаційної сфери країни – 0,2 друк. арк.; Web of Science).
11. Lakhno V., Bereke M., Adilzhanova S., Chubaievskyi V., Desiatko A., Palaguta K. Genetic algorithm for solving the problem of scaling a cloud-oriented object of informatization. *Journal of Theoretical and Applied Information Technologythis link is disabled*. 2022. Vol. 100. № 6. P. 1693–1705. (1,2 друк. арк.; особистий внесок автора: запропоновано генетичний алгоритм розв’язання задачі масштабування хмароорієнтованого об’єкта інформатизації – 0,2 друк. арк.; Scopus).
12. Lakhno V., Blozva A., Kasatkin D., Chubaievskyi V., Tyshchenko D., Brzhanov R. Experimental studies of the features of using waf to protect internal services in the zero trust structure. *Journal of Theoretical and Applied Information Technologythis*. 2022. Vol. 100. № 3. P. 705–721. (1,8 друк. арк.; особистий внесок автора: досліджено використання WAF у захисті внутрішніх сервісів у структурі Zero Trust – 0,3 друк. арк.; Scopus).
13. Chubaievskyi V., Blakyta H., Bogma O., Shtuler I., Batrakova T. Protection of information resources as an integral part of economic security of the enterprise. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetuthis*. 2022. № 4. P. 117–122. (0,5 друк. арк.; особистий внесок автора: обґрунтовано модель побудови системи захисту інформації підприємств – 0,1 друк. арк.; наукове фахове видання України, категорія «А», Scopus, Index Copernicus).

14. Akhmetov B., Lakhno V., Chubaievskyi V., Kaminskyi S., Adilzhanova S., Ydyryshbayeva M. Automation of Information Security Risk Assessment. *International Journal of Electronics and Telecommunicationsthis*. 2022. Vol. 3. № 68. P. 549–555. (0,6 друк. арк.; особистий внесок автора: розроблено метод аудиту інформаційної безпеки для розподільної числової мережі об'єкта інформатизації – 0,1 друк. арк.; Scopus).
15. Чубаєвський В., Десятко А., Криворучко О., Лахно В., Блозва А., Місюра М. Застосування СППР у завданнях організаційно-економічного забезпечення захисту інформації. *Інформаційні технології та суспільство*. 2022. № 2(4). С. 107–116. (0,6 друк. арк.; особистий внесок автора: описано процедури формалізації завдання оптимізації системи захисту інформації – 0,1 друк. арк.; наукове фахове видання України, категорія «Б»).
16. Чубаєвський В. І., Жук Т. В. Економічна ефективність інформаційної безпеки підприємств торгівлі. *Scientia Fructuosa (Вісник Київського національного торговельно-економічного університету)*. 2022. № 1. С. 106–117. (1,0 друк. арк.; особистий внесок автора: обґрунтовано вибір методів оцінки економічної ефективності інформаційної безпеки для підприємств торгівлі – 0,5 друк. арк.; наукове фахове видання України, категорія «Б»).
17. Чубаєвський В. І., Богма О. С., Сілакова Г. В. Методика оцінки ефективності систем захисту корпоративної інформації вітчизняних підприємств. *Економічний простір*. 2022. № 177. С. 56–61. (0,6 друк. арк.; особистий внесок автора: запропоновано інтегральну методику оцінювання рівня ефективності системи захисту корпоративної інформації підприємства, яка передбачає розрахунок інтегральних показників за кожною виділеною складовою системи захисту корпоративної інформації підприємства й загального інтегрального показника – 0,2 друк. арк.; наукове фахове видання України, категорія «Б»).
18. Чубаєвський В. Стратегічні орієнтири формування корпоративної політики інформаційної безпеки. *Причорноморські економічні студії*. 2021. Вип. 72. (Ч. 2). С. 24–30. (0,4 друк. арк.; наукове фахове видання України, категорія «Б»).

19. Lakhno V., Akhmetov B., Mazaraki A., Chubaievskyi V., Desiatko A. Methodology for assessing the effectiveness of measures aimed at ensuring information security of the object of informatization. *Journal of Theoretical and Applied Information Technologythis*. 2021. Vol. 14. № 99. P. 3417–3427. (1,0 друк. арк.; особистий внесок автора: запропонована методика розрахунку показників від інвестиційних заходів у рамках підвищення метрик ІБ ОБІ – 0,2 друк. арк.; Scopus).
20. Чубаєвський В., Лахно В., Ахметов Б., Криворучко О., Касаткін Д., Десятко А., Литовченко Т. Оптимізації резерву обладнання для інтелектуальних автоматизованих систем. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2021. Т. 2. № 14. С. 87–99. (0,7 друк. арк.; особистий внесок автора: запропоновано алгоритми для нейромережевого аналізатора кібербезпеки – 0,1 друк. арк.; наукове фахове видання України, категорія «Б»).
21. Чубаєвський В., Лахно В., Криворучко О., Касаткін Д., Десятко А., Блозва А., Гусєв Б. Методика мінімізації витрат на побудову багатоконтурної системи захисту на основі генетичного алгоритму. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2021. Т. 1. № 13. С. 16–28. (1,1 друк. арк.; особистий внесок автора: обґрунтовано оптимальні параметри компонентів СЗІ з урахуванням обраних експертом пріоритетних метрик кібербезпеки ОБІ – 0,3 друк. арк.; наукове фахове видання України, категорія «Б»).
22. Чубаєвський В., Лахно В., Криворучко О., Касаткін Д., Десятко А., Блозва А. Ефективність методики розрахунку показників інвестицій в системи інформаційної безпеки об’єктів інформатизації. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2021. Т. 4. № 12. С. 96–107. (1,0 друк. арк.; особистий внесок автора: обґрунтовано можливість і необхідність отримання необхідних даних, що сприяють достовірній оцінці ефективності заходів, спрямованих на підвищення інформаційної безпеки компанії – 0,2 друк. арк.; наукове фахове видання України, категорія «Б»).
23. Чубаєвський В., Волосович С. Безпека корпоративної інформації в екосистемі FinTech. *Foreign trade: Economics, Finance, Law*. 2021. Т. 119. № 6. С. 98–108.

(0,8 друк. арк.; особистий внесок автора: проаналізовано подвійну природу кібербезпеки, що одночасно є складовою FinTech і забезпечує захист корпоративних інформаційних систем учасників екосистеми FinTech – 0,4 друк. арк.; наукове фахове видання України, категорія «Б»).

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

Опубліковані праці апробаційного характеру:

25. Lakhno V., Kasatkin D., Desiatko A., Chubaievskyi V., Tsuitsuira S., Tsuitsuira M. Indicators Systematization of Unauthorized Access to Corporate Information / Rajakumar G., Du K. L., Vuppalapati C., Beligiannis G. N. (eds) *Intelligent Communication Technologies and Virtual Mobile Networks :* Lecture Notes on Data Engineering and Communications Technologies. Singapore : Springer, 2023. Vol. 131. P. 569–580. (0,8 друк. арк.; особистий внесок: запропоновано підхід до процедури формалізації ознакового функціонального подання неправомірних дій комп'ютерного зловмисника під час реалізації функцій несанкціонованого доступу до ресурсів інформаційних систем компаній та підприємств – 0,1 друк. арк.; Scopus).
26. Чубаєвський В. І. Особливості оцінки економічної ефективності інвестування в об'єкти інформаційної безпеки корпорацій. *Сучасні проблеми економіки та бізнесу* : матеріали XII Міжнародної науково-практичної конференції (Київ, 10–11 листопада 2022 р.). Київ : НАУ, 2022. С. 220–222. (0,1 друк. арк.).
27. Чубаєвський В. І. Реалізація методичного підходу до оцінки економічної ефективності системи захисту корпоративної інформації. *Сучасні тренди соціально-економічних перетворень та інтелектуалізації суспільства в умовах сталого розвитку* : тези доповідей Міжнародної науково-практичної

конференції (10 листопада, м. Запоріжжя). Запоріжжя : НУ «Запорізька політехніка», 2022. С. 372–374 (0,1 друк. арк).

28. Lakhno V., Mazaraki A., Kasatkin D., Kryvoruchko O., Khorolska K., Chubaievskyi V. Models and Algorithms for Optimization of the Backup Equipment for the Intelligent Automated Control System Smart City. *Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems* : Proceedings of ICICCT 2022 / Editors: G. Ranganathan, Xavier Fernando, Álvaro Rocha. Singapore : Springer, 2022. Vol. 383. P. 749–762. (1,0 друк. арк.; особистий внесок автора: запропоновано моделі та алгоритми оптимізації кібербезпеки інтелектуальної автоматизованої системи управління Smart City – 0,1 друк. арк.; Scopus).
29. Chubaievskyi V. Directions of assessment of technological resources of economic security of business in the process of European Integration. *Стратегічні орієнтири розвитку економіки, фінансів, обліку і права* : збірник тез доповідей міжнародної науково-практичної конференції (Полтава, 30 липня 2022 р.). Полтава : ЦФЕНД, 2022. С. 17–19. (0,2 друк. арк.).
30. Lakhno V., Kozlovskyi V., Klobukov V., Chubaievskyi V., Tyshchenko D. Software Package for Information Leakage Threats Relevance Assessment. *Lecture Notes in Networks and Systemsthis* : Computer Science On-line Conference / Conference Paper. 2022. Vol. 503. P. 290–301. (1,0 друк. арк.; особистий внесок автора: запропоновано методологічний підхід, який дозволяє автоматизувати та систематизувати прояви ефекту захищеності інформації від витоків по технічних каналах передачі – 0,2 друк. арк.; Scopus).
31. Lakhno V., Malyukov V., Kryvoruchko O., Chubaievskyi V., Misiura M., Pashorin V. Methodology for placing components of a video surveillance system for smart city based on a composite cost optimization model. *Lecture Notes in Networks and Systemsthis* : Computer Science On-line Conference / Conference Paper. Springer, Cham, 2022. Vol. 501. P. 13–23. (0,8 друк. арк.; особистий внесок автора: розроблено новий клас білінійних диференціальних ігор в нечіткій постановці,

що можуть бути застосовані до фізичних систем захисту в корпоративному середовищі – 0,1 друк. арк.; Scopus).

32. Lakhno V., Akhmetov B., Chubaievskyi V., Desiatko A., Palaguta K., Blozva A., Chasnovskyi Y. Information security audit method based on the use of a neuro-fuzzy system. *Proceedings of the 5th Computational Methods in Systems and Software 2021*. Springer, Cham, 2021. P. 171–184. (1,4 друк. арк.; особистий внесок автора: запропоновано модифікований метод аналізу ієрархій, на основі застосування апарату теорії нечітких множин та нейронних мереж – 0,2 друк. арк.; Scopus).
33. Чубаєвський В. І., Франчук Т. М. Проблеми захисту персональних даних в електронно-інформаційному середовищі. *Кібергігієна. Кібербезпека. Безпека держави* : матеріали наукових семінарів (м. Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. Київ : Київ. нац. торг.-екон. ун-т, 2020. С. 34–36. (особистий внесок автора: запропоновано методи діагностування загроз несанкціонованого доступу до персональних даних – 0,1 друк. арк.).
34. Чубаєвський В. І., Терешенко Е. Ю. Особливості моніторингу оцінки інформаційної безпеки України. *Інформаційно-аналітичне забезпечення управління фінансово-економічною безпекою держави, регіону, суб'єктів господарювання в умовах COVID-19* : матеріали X Міжнар. наук.-практ. конф., Харків, 18-19 листопада 2021 року / Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2021. С. 294–297. (особистий внесок автора: визначено склад показників системи моніторингу оцінки інформаційної безпеки – 0,1 друк. арк.).
35. Чубаєвський В., Криворучко О., Десятко А. Оцінка якості програмного забезпечення інформаційно-управляючих систем. *Глобалізаційні виклики розвитку національних економік* : тези доповідей II Міжнар. наук.-практ. конф. (Київ, 19 жовтня 2021 р.) / відп. ред. А. А. Мазаракі. Київ : Київ. нац. торг.-екон. ун-т, 2021. С. 278–281. (особистий внесок автора: оцінка захищеності програмного забезпечення інформаційно-управляючих систем – 0,1 друк. арк.).
36. Лахно В., Ахметов Б., Чубаєвський В., Криворучко О., Десятко А., Пашорін В. Оцінювання ефективності заходів щодо забезпечення інформаційної безпеки

об’єкта інформатизації. *Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні 2021* : збірник матеріалів IX Міжнар. наук.-практ. інтернет конф., м. Київ, 13–14 трав. 2021 р. Київ : НУБіП України, 2021. С. 45–48. (особистий внесок автора: обґрунтування системи показників для оцінювання ефективності заходів щодо забезпечення інформаційної безпеки об’єкта інформатизації – 0,1 друк. арк.).

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

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 4

ВСТУП 6

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ 23

1.1. Корпоративний інформаційний простір: еволюція контенту та форм організації 23

1.2. Захист корпоративної інформації як детермінанта ефективного розвитку підприємства 39

1.3. Видова трансформація економічної ефективності управління підприємством 53

Висновки до розділу 1 75

Список використаних джерел до розділу 1 78

РОЗДІЛ 2. МЕТОДОЛОГІЧНІ ОСНОВИ УПРАВЛІННЯ КОРПОРАТИВНОЮ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ 86

2.1. Концепція формування корпоративної інформаційної безпеки 86

2.2. Методологічні засади формування корпоративної політики інформаційної безпеки 114

2.3. Систематизація показників оцінки економічної ефективності управління корпоративною інформаційною безпекою 135

Висновки до розділу 2 155

Список використаних джерел до розділу 2 159

РОЗДІЛ 3. МОДЕЛІ ТА ТЕХНОЛОГІЇ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ 174

3.1. Систематизація ознак несанкціонованого доступу до корпоративної інформації 174

3.2. Програмний комплекс для оцінки актуальності загроз витоку інформації 185

3.3. Моделювання ефективності інвестицій на формування системи захисту корпоративної інформації 198

Висновки до розділу 3 214

Список використаних джерел до розділу 3 215

РОЗДІЛ 4. ЕКОНОМІЧНА ДІАГНОСТИКА СИСТЕМ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ 224
4.1. Оцінка інформаційної безпеки в Україні та світі 224
4.2. Аналіз діючої практики управління інформаційною безпекою на підприємствах 237
4.3. Оцінка економічної ефективності системи захисту корпоративної інформації 248
Висновки до розділу 4 268
Список використаних джерел до розділу 4 269
РОЗДІЛ 5. МЕТОДИ ПІДВИЩЕННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ 277
5.1. Організаційно-економічне забезпечення ефективного захисту корпоративної інформації 277
5.2. Методика аудиту інформаційної безпеки підприємства 288
5.3. Вдосконалення оцінки ризиків інформаційної безпеки підприємства в автоматизованих системах захисту корпоративної інформації 302
Висновки до розділу 5 311
Список використаних джерел до розділу 5 313
ВИСНОВКИ 322
ДОДАТКИ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЕМ – Event Management (управління подіями)

АІБ – аудит інформаційної безпеки

АС – автоматизовані системи

БМ – байєсовські 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 передачі інформації

ТСЗІ – технічні системи захисту інформації

ШНМ – штучна нейронна мережа

ВСТУП

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

За оцінками експертів станом на 2023 рік 70% людства буде користуватись Інтернетом. Це вагома ознака розвитку глобального інформаційного суспільства, що вимагає розробки та запровадження системних підходів кіберзахисту як на корпоративному, так і на державному рівнях. Практика останніх років засвідчує висхідний тренд вартості кіберзлочинів з одного боку, та низьку спроможність традиційних заходів кібербезпеки щодо їх стримування та запобігання.

Яскравим прикладом таких загроз є наймасштабніша 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 загальні збитки в масштабах країни могли складати 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, протидії кібератакам, що

потребує розроблення нових рішень та підходів, які відповідають не тільки реаліям сьогодення, але й мають значний потенціал розвитку, ураховуючи сучасні тенденції ІТ-галузі в цілому.

Актуальність зазначеної проблематики підкреслює 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 України за один місяць війни вже сталося майже втричі більше хакерських атак різного виду, ніж за аналогічний період минулого року. Найпопулярнішими видами атак залишаються фішингові розсилання, розповсюдження шкідливого програмного забезпечення. Атакують, насамперед, державні установи, фінансовий, оборонний сектор, операторів зв'язку, місцеві органи влади, логістичні компанії, медіа. І ця тенденція має зростаючий тренд.

Так, за даними Євростат, у 2019 році 93 % підприємств ЄС із чисельністю персоналу понад 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, статистичні спостереження щодо запровадження підходів із забезпечення інформаційної безпеки підприємствами України наразі відсутні. Водночас стан інформаційної безпеки України опосередковано демонструє її місце у глобальному та національному індексах кібербезпеки. Так, у 2018 році Україна посіла 54 місце серед 180 країн у глобальному рейтингу кібербезпеки, посиливши свою позицію на 2 пункти, у 2020 році – 25 місце серед 160 країн у рейтингу національного індексу кібербезпеки. Це свідчить про певне покращення систем захисту інформації в Україні, проте і вказує на наявний потенціал та необхідність запровадження заходів із посилення інформаційної безпеки.

Нині Україна посідає чільне місце серед країн, що пропонують якісні ІТ-послуги сертифікованими фахівцями, що вказує на високий потенціал в сфері розробки та розгортання сучасних програм захисту від кібер-атак. 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 щодо питань подолання наслідків кібератак на критично важливу інформаційну інфраструктуру і виявлення причин та обставин таких інцидентів. CERT-UA також допомагає усунути загрози безпеці приватного сектору України та іноземних партнерів. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» (2017), CERT-UA та Центр реагування на кіберзлочини координують заходи, спрямовані на оперативне реагування на кібератаки, а також контролюють упровадження контрзаходів, що передбачають мінімізацію уразливості систем зв'язку.

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

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

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 в 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 неї 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 наразі «Цифровий компас ЄС до 2030» в межах Проєкту стратегії сталого розвитку «Європа-2030».

Питання розвитку інформаційного суспільства та забезпечення інформаційної безпеки в Україні регламентуються рядом нормативно-правових актів, зокрема: Конституцією, Законом України «Про Концепцію Національної програми інформатизації», Воєнною доктриною, Законом «Про інформацію», Законом «Про телекомунікації», Стратегією кібербезпеки України тощо. Наразі обґрунтовано проєкт Закону України «Про цифровий порядок денний України» в межах проєкту Стратегії «Україна-2030».

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

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

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

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

Більшість дослідницьких зусиль іноземних учених зосереджені на використанні мережевого трафіка для створення моделей прогнозування. Ці дослідження представлені в роботах таких учених, як: Е. Понтес, А. Гуельфі, С. Кофуджі, А. Сільва. Інші дослідники, такі як Д. Бансал, С. Софат, П. Чакраборті, П. Хадіві, Б. Льюіс, А. Махендиран, Дж. Чен, П. Батлер, Э. Нсозі, С. Мекару, Дж. Браунштейн будують кіберпрогнозування за допомогою статистичного та алгоритмічного моделювання.

Не дивлячись на досить потужний пласт досліджень з проблематики інформаційної безпеки, наразі відсутні комплексні міждисциплінарні розвідки, які б окреслювали методологію та практичний інструментарій формування ефективних систем захисту корпоративної інформації, які б забезпечували з одного

боку дієвий захист інформації (убезпечували виток інформації, вихід із ладу комунікаційних засобів тощо), а з іншого – формували б 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. Відповідно, саме на обґрунтування теоретико-методологічних засад формування ефективних (із т. з. досягнення цілей захисту та цільових показників економічної ефективності) систем інформаційної безпеки спрямоване дане дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано відповідно до плану науково-дослідних робіт Державного торговельно-економічного університету. Результати досліджень наведено в темах: «Системи оцінювання економічної ефективності захисту корпоративної інформації» (термін виконання – II кв. 2021р. – III кв. 2024 р., номер державної реєстрації 0121U110908) запропоновано інтегральну методику оцінювання рівня ефективності системи захисту корпоративної інформації підприємства, яка передбачає розрахунок інтегральних показників за кожною виділеною складовою системи захисту корпоративної інформації підприємства й загального інтегрального показника; обґрунтовано шкалу інтерпретації рівня ефективності системи захисту корпоративної інформації підприємства за запропонованою методикою; розроблено підходи до математико-алгоритмічної та комп'ютерної підтримки процедури прийняття рішень у задачі організаційно-економічного забезпечення ефективного захисту корпоративної інформації; запропоновано методику багатокритеріальної оптимізації витрат на систему захисту корпоративної інформації, яка полягає в застосуванні генетичного алгоритму VEGA (Vector Evaluated Genetic Algorithm) (довідка № 1999/24 від 14.11.2022); «Цифрова трансформація торговельно-економічної та туристичної систем України» (№717/20; термін виконання – 01.06.2021 – 31.12.22; замовник – МОНУ; підстава для проведення НДР – наказ МОНУ від 16.04.2021 № 434), де

запропоновано методи оцінки економічної ефективності інформаційної безпеки для підприємств торгівлі; систематизовано особливості оцінки економічної ефективності інформаційної безпеки з урахуванням особливостей діяльності оптово-роздрібних підприємств; розроблено підходи до вирішення проблем захисту персональних даних в електронно-інформаційному середовищі торговельно-економічної та туристичної сфер України; запропоновано генетичний алгоритм розв'язання задачі масштабування хмароорієнтованого об'єкта інформатизації в торговельно-економічній та туристичній сферах (довідка № 2005/20 від 15.11.2022).

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

Для досягнення поставленої мети визначено такі завдання:

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

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

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

– обґрунтувати Концепцію формування корпоративної інформаційної безпеки;

– систематизувати види корпоративних політик інформаційної безпеки;

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

– обґрунтувати комплекс ознак несанкціонованого доступу до корпоративної інформації;

– розробити програмний комплекс для оцінки актуальності загроз витоку інформації;

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

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

– провести аналіз діючої практики управління інформаційною безпекою на підприємствах;

– оцінити економічну ефективність систем захисту корпоративної інформації в Україні;

– розробити організаційно-економічне забезпечення ефективного захисту корпоративної інформації;

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

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

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

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

Методи дослідження. Для вирішення поставлених у роботі завдань використані загальнонаукові й прикладні методи дослідження, взаємопов’язані та послідовно застосовані для забезпечення загальної логіки, зокрема, порівняльний, структурний та логіко-історичний (для дослідження сутності, еволюції та особливостей корпоративного інформаційного простору, ролі захисту корпоративної інформації в забезпеченні розвитку підприємства, дослідженні видової трансформації економічної ефективності управління підприємством п.1.1, 1.2, 1.3.); системно-функціональний метод (для розроблення концепції формування системи корпоративної інформаційної безпеки, методологічних засад формування політики захисту корпоративної інформації, систематизації показників оцінювання економічної ефективності захисту корпоративної інформації п.2.1, 2.2, 2.3); методи

системного аналізу, теоретичного узагальнення та синтетичних оцінок (для обґрунтування механізму формування корпоративної інформаційної безпеки, формування принципів оцінки та розроблення інтегрального показника економічної ефективності захисту корпоративної інформації п.2.1, 2.3); теорії ймовірності і математичної статистики (для оцінювання довірчих інтервалів математичного сподівання нормального розподілу випадкової величини інтенсивності кібератак (р. 3); методи порівняння, математичні та статистичні методи аналізу, анкетного опитування (для оцінки тенденцій зміни рівня інформаційної безпеки України, аналізу діючої практики захисту корпоративної інформації на підприємствах України та оцінки його ефективності р. 4); метод аналізу ієрархій (MAI), метод нечітких правил, теорія Байєсовських мереж (БМ), елементи нечіткої логіки (НЛ), алгоритми штучних нейронні мережі (ШНМ) (для розроблення моделей оцінювання рівня безпеки корпоративної інформації (р. 5).

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

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

вперше:

– обґрунтовано авторську концепцію формування корпоративної інформаційної безпеки, що ґрунтується на позитивістській та нормативній

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

– розроблено методологічний підхід до оцінювання ефективності захисту корпоративної інформації, який включає: принципи оцінювання та систематизації показників; систему часткових показників ефективності та критеріальну шкалу їх інтерпретації; узагальнюючу оцінку ефективності захисту корпоративної інформації на основі поєднання інтегрального показника та показника прогресивності розвитку системи захисту КІ, структурно-логічну послідовність етапів оцінювання, що створює основу для запровадження дієвих систем оцінювання ефективності захисту корпоративної інформації;

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

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

ризиків, своєчасно реагувати на загрози адміністратору ІБ розподіленої обчислювальної мережі (РОМ);

удосконалено:

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

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

– концептуальне позиціонування захисту корпоративної інформації в забезпеченні ефективного розвитку підприємства на основі доведеної взаємообумовлюючої залежності між параметрами та функціями корпоративного інформаційного простору (КІП); розширено перелік параметрів КІП такими характеристиками як рівень цифровізації КІП, цифрові компетентності персоналу, рівень інноваційності інформаційної інфраструктури, рівень корпоративної інформаційної культури, ступінь захищеності та якість регламентації КІП; ідентифіковано систему функцій КІП (інтегруюча, комунікативна, актуалізуюча, соціальна, навчальна, інноваційна, акселеруюча) та сформульоване авторське бачення сутності захисту корпоративної інформації як системи принципів, методів та процесів протидії загрозам інформаційній безпеці підприємства, які спрямовуються на порушення функціонування КІП і передбачає їх ідентифікацію, аналіз, попередження та нейтралізацію, що поглиблює теоретичні основи функціонування КІП та формує підґрунтя для побудови систем управління ним;

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

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

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

– організаційно-економічне забезпечення ефективного захисту корпоративної інформації як комплексу взаємоузгоджених елементів (заходів) різної спрямованості та частоти застосування, які перебувають у постійній взаємодії, виступають частиною економічного механізму інформаційної безпеки, реалізуються на різних контурах управління та інтегровані в систему загальнокорпоративного управління для досягнення визначених цілей та який на відміну від існуючих передбачає чітку систематизацію елементів за їх

функціональним напрямом, можливістю впливу на КІБ, частотою застосування, контуром управління. Це дозволило окреслити систематизований комплекс практичних заходів із захисту корпоративної інформації, що підвищить обґрунтованість та ефективність їх запровадження в практичній діяльності;

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

набули подальшого розвитку:

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

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

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

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

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

Практичне значення одержаних результатів дисертаційної роботи полягає в тому, що теоретичні і методологічні положення доведені до рівня конкретних методик і рекомендацій щодо підвищення економічної ефективності систем захисту корпоративної інформації, можуть бути використані в практичній діяльності підприємств у процесі реалізації систем захисту інформації, а також органами державної влади – під час реалізації державної політики, вдосконалення

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

Положення, висновки та пропозиції дисертаційної роботи застосовано в освітньому процесі Державного торговельно-економічному університеті під час викладання дисциплін «Економічна безпека підприємства», «Економічна діагностика підприємства», «Архітектура та проєктування програмного забезпечення», «Хмарні та GRID технології», «Комп'ютерні мережі» та в навчально-методичному процесі під час підготовки навчального посібника,

збірників тестових завдань, програм, робочих програм, опорних конспектів лекцій (довідка № 2000/22 від 14.11.2022).

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

Апробація результатів дисертації. Основні положення і результати досліджень, викладені в дисертаційній роботі, доповідались і отримали схвалення на 12 міжнародних і всеукраїнських науково-практичних конференціях та наукових семінарах: 4th International Conference on Innovative Data Communication Technologies and Application (ICIDCA 2022) (м. Коїмбатур, Індія, 3–4 листопада 2022 р.), Міжнародна науково-практична конференція «Стратегічні орієнтири розвитку економіки, фінансів, обліку і права» (м. Полтава, 30 липня 2022 р.), 6th International Conference on Inventive Communication and Computational Technologies (ICICCT – 2022) (м. Тамілнад, Індія, 12–13 травня 2022 р.), 11th Computer Science On-line Conference 2022 (Чехія, 26–30 квітня 2022 р.), 4th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2022) (м. Тірунелвелі, Індія, 10–11 лютого 2022 р.), International Conference on Computational Intelligence and Data Analytics (ICCIDA – 2022) (м. Гайдарабад, Індія, 8–9 січня 2022 р.), X Міжнародна науково-практична конференція «Інформаційно-аналітичне забезпечення управління фінансово-економічною безпекою держави, регіону, суб'єктів господарювання в умовах COVID-19» (ХНУМГ ім. О. М. Бекетова, м. Харків, 18–19 листопада 2021 р.), II Міжнародна науково-практична конференція «Глобалізаційні виклики розвитку національних економік» (КНТЕУ, м. Київ, 19 жовтня 2021 р.), 5th Computational Methods in Systems and Software 2021 (Чехія, 13–15 жовтня 2021 р.), IX Міжнародна науково-практична Інтернет-конференція «Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2021» (НУБіП України, м. Київ, 13–14 травня 2021 р.), IV Міжнародна науково-практична конференція

проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS) (Київський національний університет імені Тараса Шевченка, м. Київ, 15–16 квітня 2021 р.), Наукові семінари «Кібергігієна. Кібербезпека. Безпека держави» (КНТЕУ, м. Київ, 27 листопада 2020 р.).

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

Обсяг та структура роботи. Дисертаційна робота складається із вступу, п’яти розділів зі списками використаних джерел до кожного з них, висновків та додатків. Повний обсяг дисертації становить 371 сторінка, із них основна частина займає 300 сторінок. Дисертація містить 34 таблиці, 36 рисунків, 4 додатки, списки використаних джерел включають загалом 440 найменувань (без врахування праць здобувача).

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ

1.1. Корпоративний інформаційний простір: еволюція контенту та форм організації

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

У роботах В. Домарьова [9], С. Мельниченко [10], М. Чумаченко [11], М. Денисенко, І. Колос [12], А. Батюка, З. Двуліт [13], В. Іванової [14] вивчаються теоретико-методологічні основи та прикладні аспекти створення та 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 [17]. Вивченню його феномена та розвитку завжди приділялась особлива увага з боку філософів, соціологів, культурологів та згодом економістів у контексті дослідження ресурсного

потенціалу окремих економічних систем. Із часом та розвитком інформаційного суспільства увага науковців до функціонування та трансформації інформаційного простору лише зростає, з огляду на посилення ролі інформації, як в житті окремого індивіда, так і у функціонуванні економічних систем різного рівня. Не дивлячись на потужний пласт наукових досліджень у різних галузях науки на сьогоднішній день відсутні однозначні трактовки поняття «інформаційний простір», підходи до його структуризації, а відтак і методи регламентації та управління ним.

Так, М. Яковенко на основі дослідження та узагальнення філософських трактовок 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].

З даних 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.

Г. Ньюбі 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.

М. Слюсаревський у межах авторської «реляційної теорії інформаційного простору» розглядає інформаційний простір як стан (і водночас результат) перманентної взаємодії процесів виробництва та споживання інформації, тобто інформаційний простір розглядається 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 характеризувати 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 автора, 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. У якості такого суб'єкта може виступати як особистість, так і соціальна група, організація, підприємство або навіть державний орган – тобто будь-які користувачі інформаційних технологій [20].

Так, на основі вищезазначеного можна виокремити таку важливу сутнісну ознаку інформаційного простору як безперервність процесу виробництва та споживання інформації, тобто наявність постійної комунікації між суб'єктами.

До вищезазначених сутнісних характеристик інформаційного простору нами пропонується додати наступну характеристику «інформаційний простір є фактором 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. Відтак інформаційний простір є важливим об'єктом управління, адже його формування та функціонування має сприяти економії ресурсів, підвищенню ефективності функціонування системи, її виживанню та розвитку [73].

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, 73]

На основі узагальнення та розвитку сучасних підходів можна таким чином 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»** [73].

Задля 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 відносить 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 [21, 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 трактовка корпорації в міжнародному праві є схожою до терміна «корпоративне підприємство в українському правовому полі». Такого підходу дотримується і переважна більшість авторів, що займаються розвідками у сфері корпоративного управління. Так, 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 і вкладених інвестицій [23]. Аналогічну трактовку цього терміна надають українські наковці О. Арєф'єва та Н. Васюткіна [24]. Використовуючи поняття «корпоративний» надалі ми будемо дотримуватися саме такого змістовного навантаження терміна «корпорація», розуміючи під нею правову форму бізнесу, що відрізняється і відокремлена від конкретних осіб, які ними володіють.

Таким чином, розуміння понять «інформаційний простір» та «корпорація» дозволяє в наступний спосіб визначити поняття **корпоративного інформаційного простору – організована система інформації та інформаційних процесів корпорації, яка є станом та результатом її функціонування, способом її розвитку та представлення** [73].

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

Як слушно зазначає С. 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 в усіх сферах діяльності людини сучасних інформаційно-комунікаційних технологій, які істотно змінюють не тільки спосіб виробництва товарів і послуг, але 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 наш погляд, можна визначити етапи його еволюції так, як наведено в табл. 1.1.

Таблиця 1.1

Етапи еволюції корпоративного інформаційного простору

Назва етапу	Період	Основні ознаки
«Паперовий» (до широкого використання у практиці ПЕОМ)	До середини 70-х років	-локальність -обмеженість -низька інтенсивність поширення -високі витрати часу на формування на обробку інформації
«Автоматизований» (після винаходу та широкого запровадження у практику ПЕОМ)	Із середини 70-х років до початку 90-х років	-локальність -обмеженість -низька інтенсивність поширення -скорочення витрат часу на формування на обробку інформації
«Мережевий» (після початку широкого використання Інтернету в комерційних цілях)	Із початку 90-х років по теперішній час	-глобальність -відсутність фізичних меж зберігання інформації -висока інтенсивність та швидкість поширення -«надлишковість» та складність вибору релевантної інформації -низькі витрати часу на формування, обмін та обробку інформації -зростання витрат на захист інформації -посилений вплив інформаційного простору на трансформацію бізнес-моделі, організаційної структури тощо

Джерело: складено автором [73]

Так, за останні 50 років відбулася суттєва трансформація корпоративного інформаційного простору. З особливою інтенсивністю трансформаційний процес відбувався останні 30 років після широкого застосування Інтернету. Якщо до цього корпоративний інформаційний простір носив локальний характер, характеризувався високими витратами на збір та обробку інформації, тоді як уже із середини 90-х років XX-го сторіччя інформаційний простір став носити глобальний характер, спостерігається високий рівень інтенсивності та швидкості поширення інформації: будь-яка інформація може бути поширена або знайдена «в один клік»; дуже часто інформація носить «надлишковий» характер, потребує відбору. Водночас суттєво знижуються витрати часу на обробку та аналіз інформації та зростають – на убезпечення інформаційного простору. 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 посилення ролі корпоративного інформаційного простору в розвитку підприємства [73].

Так, на думку 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 підприємства [26].

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

Так, для сучасного корпоративного інформаційного простору характерна 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.

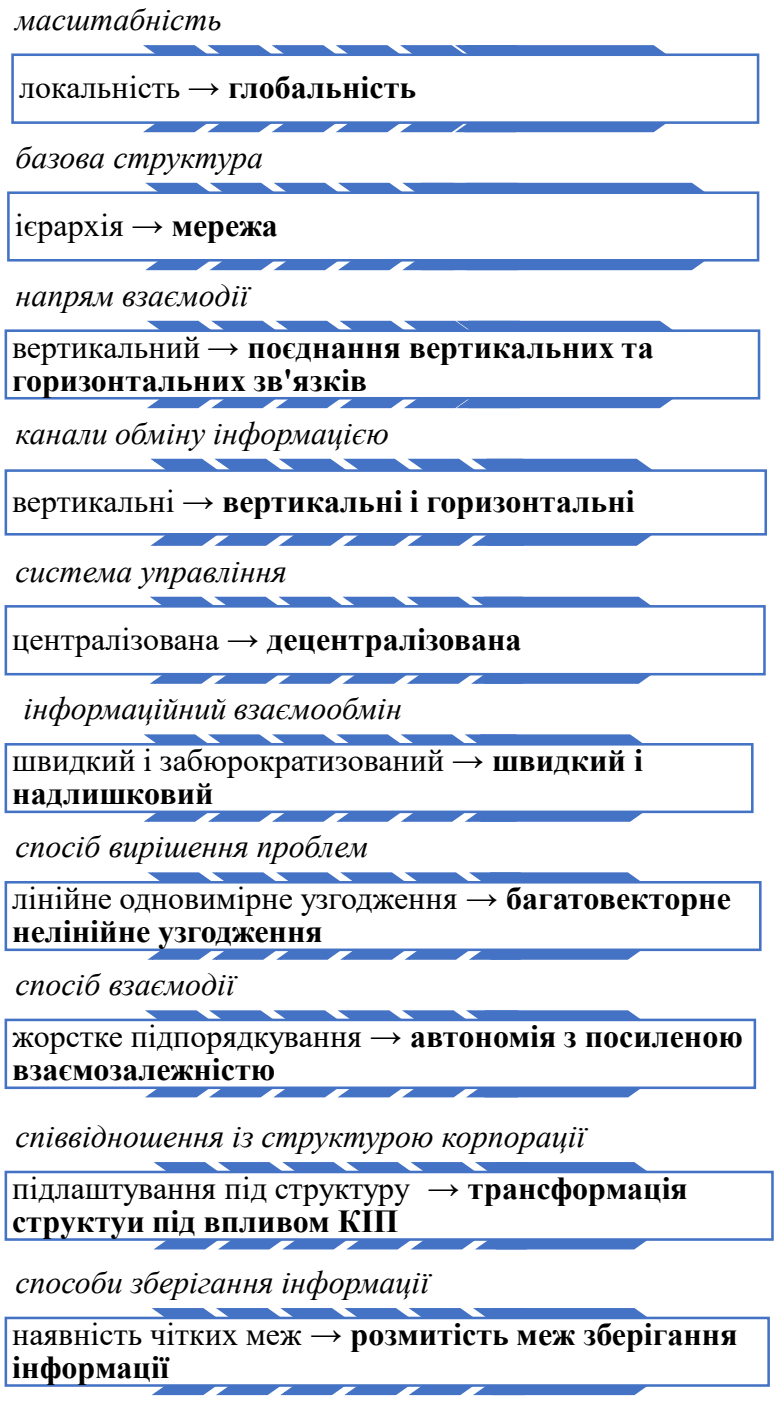


Рис. 1.2. Тенденції розвитку корпоративного інформаційного простору на сучасному етапі його еволюції

Джерело: розвинено автором на основі [26]

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 зберігалася фізично в межах підприємства, то зараз знаходиться в різних місцях і виходить за межі «офісу» (у відокремлених сервісних центрах, на «хмарних» сервісах тощо). Таким чином, під впливом розвитку корпоративного інформаційного простору спостерігається трансформація структури самої корпорації: її межі розмиваються, формуються сучасні мережеві організаційні структури, що носять більш демократичний, гнучкий та адаптивний характер.

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

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

1. **Інформаційна інфраструктура** – середовище, що забезпечує можливість збору, зберігання, передавання, автоматизованої обробки та поширення інформації в 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 [27].

2. **Інформаційні ресурси** на машинних носіях, а також розподілені по вебсайтах у мережі Інтернет. Інформаційні ресурси можуть бути державними та недержавними та знаходитися у власності громадян, органів державної влади, органів місцевого самоврядування, підприємств, організацій, установ та громадських об’єднань. Мають місце наступні 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 дозволяє різко скоротити споживання решти видів ресурсів, що в кінцевому результаті призводить до значної економії сил та засобів [27].

3. **Засоби та методи прикладної математики**, під якими розуміють алгоритми та програмні засоби, що забезпечують функціонування апаратних платформ (систем) [27].

4. **Організаційні заходи**, що забезпечують функціонування компонентів інформаційного простору [27].

5. **Правові методи (норми)**, під якими розуміють інформаційне законодавство, міжнародні угоди та інші національні та міжнаціональні правові акти [27].

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

Це одна з найширших трактовок компонентного складу інформаційного простору. Якщо застосувати зазначений підхід до корпоративного інформаційного простору, логічним є висновок щодо відсутності в його складі ринку інформаційних технологій. Проте, на нашу думку, дискусійним є віднесення до складу інформаційного простору системи організаційних заходів, оскільки вони є результатом управлінської дії на його стан та результати функціонування.

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

– інформаційні ресурси, що містять дані, відомості та знання, зафіксовані на відповідних носіях інформації [28];

– організаційні структури, що забезпечують функціонування та розвиток єдиного інформаційного простору, зокрема, збір, обробку, зберігання, розповсюдження, пошук і передачу інформації [28];

– засоби інформаційної взаємодії громадян і організацій, що забезпечують їм доступ до інформаційних ресурсів на основі відповідних інформаційних

технологій, що включають програмно-технічні засоби і організаційно-нормативні документи [28].

Так, 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 відносити і такі підрозділи і які, на нашу думку, є елементом забезпечення функціонування корпоративного інформаційного простору.

О. 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 у просторі інформації, не залежно до її форми і стану, що знаходиться 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 [29];

– інформаційний потік – сукупність інформації, що переміщується в інформаційному просторі через канали комунікації. Інформаційні потоки можуть протікати як усередині окремих інформаційних сфер, 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 [29].

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, що забезпечує інформаційну взаємодію користувачів, а також задоволення їх інформаційних потреб [29].

Слушною, на нашу думку, є пропозиція О. Кузьміної щодо виділення окремим компонентом структури 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 і 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].

Дійсно, 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 представлятися в певному вигляді, який відповідає інтересам компанії щодо формування іміджу, реалізації політик в інших сферах діяльності, «акцентуючи увагу» на певних здобутках і позитивних рисах.

Проте авторка не конкретизує місце даного компоненту інформаційного простору серед інших його складових.

Якщо з двоаспектною трактовкою інформаційного простору О. Кузьміною в цілому можна погодитись, 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;

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

Так, по-перше, зміст інформаційної системи у трактовці авторки 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 вузька трактовка компонентної структури корпоративного інформаційного простору. Так, Л. Матвєєва під корпоративним інформаційним простором розуміє сукупність інформаційних систем і технологій, зокрема таких як ERP, CRM, BPM та інших подібних систем і відповідних модулів [30]. Подібний 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, обробки інформації. До неї автори відносять АСУ, АСУ ТП та САПР.

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

Важливо не лише визначити складові компоненти корпоративного інформаційного простору, але 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. Науменко пропонується авторська концепт-модель структури інформаційного простору на основі діаграми Дж. Венна, де центральним компонентом є користувач, який використовує інформаційні ресурси. Компонентами моделі інформаційного простору автор пропонує виділяти інформаційні засоби взаємодії, системи обробки 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 [73].

Центральним та системоутворюючим компонентом 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 [73].

Наступним компонентом є семантична складова, тобто сам інформаційний контент, який умовно поділяємо на:

– інформаційні поля;

– інформаційний процес;

– віртуальну реальність;

– інформаційну культуру.

Так, погоджуючись із думкою О. Кузьміної, під інформаційним полем розуміємо сукупність усієї зосередженої в корпоративному просторі інформації, безвідносно до її форми і стану, що знаходиться окремо як від об'єкта відображення, так і від суб'єкта сприйняття [29].

Корпоративне інформаційне поле складається з великої сукупності різнорідної інформації, яку в найбільш узагальненому вигляді можна класифікувати таким чином (табл. 1.2.):

Таблиця 1.2

Класифікація інформації корпоративного інформаційного поля

Класифікаційна ознака	Види інформації
За предметною областю	-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 зовнішнє середовище) -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 [73]

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 одностороннім або зустрічним рухом інформації: вербально, письмово, за допомогою різноманітних техніко-технологічних засобів [73].

Таким чином, інформаційний потік можна визначити як сукупність розподіленої в часі та за обсягом інформації, що рухається в перебігу комунікації за різними каналами комунікації [73].

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

Важливим компонентом семантичної складової вважаємо корпоративну інформаційну культуру, яка є складним утворенням та віддзеркалює корпоративну філософію комунікацій і містить формальну і 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 і детермінує у взаємодії з іншими ресурсами ефективність функціонування економічної системи.

Важливим компонентом корпоративного інформаційного простору є інформаційна інфраструктура, яка складається з технічних засобів збору, обробки, зберігання, передачі, поширення та технологічних засобів (програмних продуктів). Якість та інноваційність інформаційної інфраструктури суттєво детермінує ефективність інформаційного процесу та в цілому впливає на ефективність функціонування підприємства [73].

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, передачі та обробки інформації [73].

Таким чином, корпоративне інформаційне поле – це складне багатокомпонентне утворення, окремі компоненти якого перебувають у взаємообумовлюючому зв'язку.

1.2. Захист корпоративної інформації як детермінанта ефективного розвитку підприємства

Інформатизація суспільства, проникнення інформаційно-комунікативних технологій (далі – ІКТ) в усі сфери суспільного буття є основною передумовою переходу від індустріального до постіндустріального суспільства. Цей процес носить глобальний та водночас нерівномірний характер. 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 визначається одним з пріоритетних напрямів державної політики» [33].

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 із 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 інформації 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 [33].

Відповідно до згаданого Закону саме реалізація завдань розвитку інформаційного суспільства дозволить 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 в суспільному житті, прийнятті відповідних рішень органами державної влади та органами місцевого самоврядування [33].

Водночас в умовах цифровізації суспільства, зростаючої ролі інформації як в житті людини, так і у функціонуванні підприємства, у 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 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. Уже аксіоматичною визнана залежність результатів функціонування, досягнення цілей від рівня економічної безпеки та її інформаційної складової. У наукових дослідженнях зустрічаються різні тлумачення поняття «інформаційна безпека».

Так, О. Сороківська, В. Гевко під інформаційною безпекою підприємства розуміють суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [34]. 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. Хофмана, інформаційна безпека – це стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації [35].

На думку О. Горбатюка, інформаційна безпека являє собою стан захищеності потреб в інформації особистості, суспільства і держави, за якого забезпечується їх існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. [36].

Подібне тлумачення інформаційної безпеки надається більшістю авторами, зокрема В. Богуш [37]. Загалом воно відповідає вітчизняному законодавчому тлумаченню цього поняття, згідно з яким інформаційна безпека визначається як 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 [33].

Переважна більшість науковців та 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) щодо корпоративної інформації, що спрямовані на всі компоненти корпоративного інформаційного простору. Відтак можна відслідкувати чіткий взаємозв’язок між захистом корпоративної інформації та досягненням високих результатів функціонування підприємства, які і є відображенням його інтересів (див. рис. 1.3).

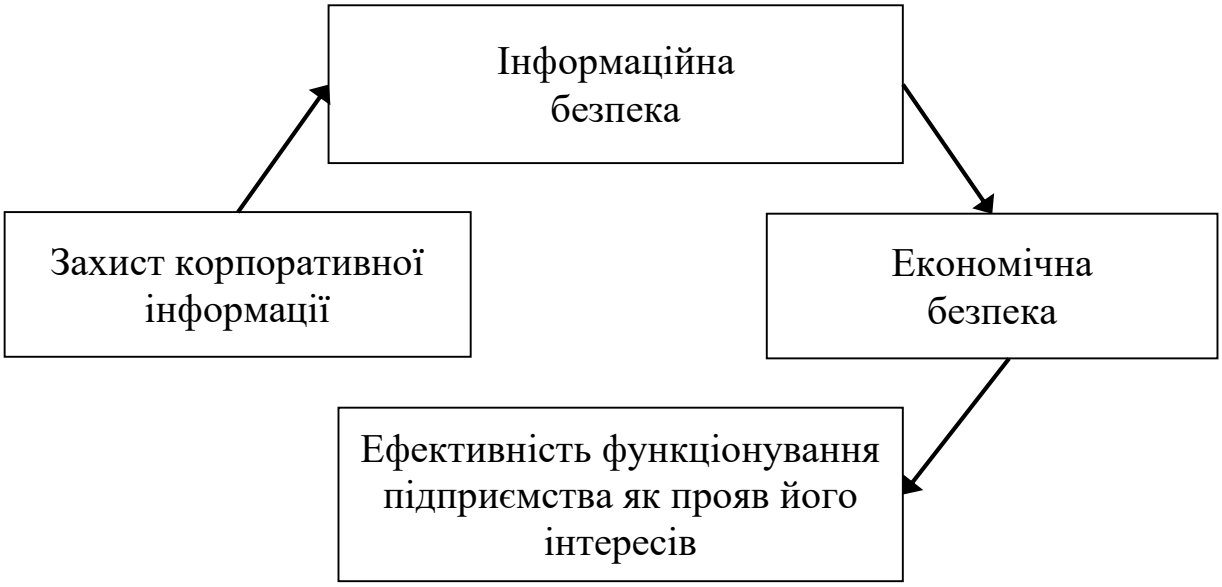


Рис. 1.3. Логіка взаємозв'язку захисту корпоративної інформації та ефективності функціонування підприємства

Джерело: складено автором

Розглянемо більш детально механізм зазначеного вище логічного зв'язку між захистом корпоративної інформації та ефективністю функціонування підприємством.

Так, корпоративний інформаційний простір характеризується рядом параметрів. У сучасних наукових дослідженнях наразі 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 у просторі» [38]. 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 полі підприємства. «У процесі обміну відбувається збільшення інформації за рахунок крос-взаємодії інформаційного фактору їх суб'єктів і, отже, можна зробити висновок про незворотний характер зростання інформації як умови і результату еволюції систем» [38].

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

4. Цифрова компетентність персоналу, яка може вимірюватися його вмінням користуватися сучасними інформаційними технологіями.

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

6. Рівень корпоративної інформаційної культури, який характеризує ступінь поваги та дотримання задекларованої філософії інформаційних комунікацій підприємства як у середині нього, так і із 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 у середині підприємства, так і з суб'єктами зовнішнього середовища.

Зазначені параметри перебувають у тісному взаємозв'язку, тобто один із параметрів може впливати на його інші параметри. Так, 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 визначених 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. Переважна більшість науковців до числа таких відносить такі [39, 40 та ін.]:

– інтегруюча – 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 і 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:

– інтегруюча – 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 та цілей підприємства в зовнішньому середовищі шляхом реалізації ним

інформаційної політики та актуалізація цілей і завдань підприємства, їх трансляція для внутрішніх користувачів інформації;

– соціальна – інформаційний простір трансформує підприємство і змінює характер та зміст його соціально-економічних відносин;

– навчальна – корпоративний інформаційний простір створює середовище 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. 1.4.

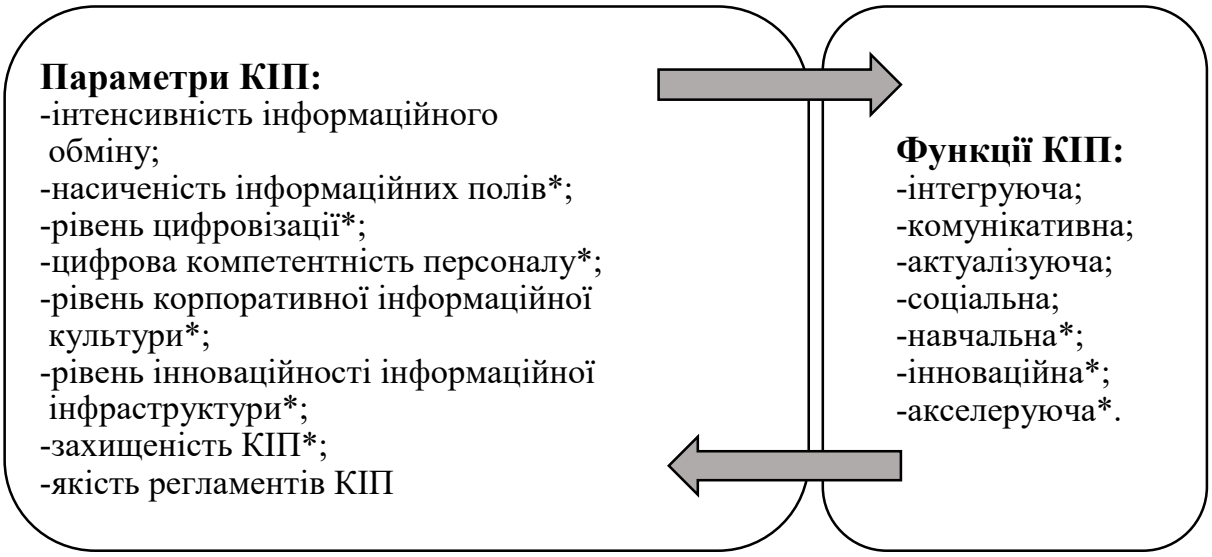


Рис. 1.4. Взаємозв'язок параметрів та функцій корпоративного інформаційного поля

Джерело: складено та розвинено автором за [39, 40 та ін]

** запропоновано автором*

Висока якість параметрів корпоративного інформаційного поля дозволяє на якісному рівні виконувати йому свої функції. 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 обсягу ресурсів, а також вдосконалювати параметри корпоративного інформаційного простору.

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

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 і повноти інформації і програмного забезпечення. Доступність – це забезпечення доступності інформації і основних послуг для користувача в потрібний для нього час [41].

Таким чином, усі 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, радіотехнічні, хімічні та інші канали;

– 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 [42].

В. Ліпкан пропонує класифікувати загрози інформаційній безпеці відповідно до загальної класифікації загроз національній безпеці: 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 [43].

Натомість А. Логінов визначає загрози як:

• розкриття інформаційних ресурсів;

• порушення цілісності інформаційних ресурсів;

• збій у роботі обладнання [44].

Л. Євдоченко задля вироблення рекомендацій щодо організації дієвих форм і методів забезпечення інформаційної безпеки 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) [45].

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 (із шахрайською метою);

• користувач отримує несанкціонований доступ з однієї мережі до іншої [46].

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 збереження; 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 [47].

А до навмисних: 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) розробка 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 [47].

Узагальнюючи та розвиваючи зазначені підходи, пропонуємо таку класифікацію загроз інформаційній безпеці підприємства (табл. 1.3). Варто відзначити, що зазначену класифікацію не слід вважати сталою. Інтенсивний розвиток інформаційних технологій, тенденції цифровізації суспільства в цілому і бізнесу, зокрема, призводять до постійного зростання інтенсивності та видів загроз.

Таблиця 1.3

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 загрози -внутрішні загрози
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 ймовірності -з середнім рівнем ймовірності -з низьким рівнем ймовірності
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 -негативний інформаційний вплив -негативні наслідки застосування інформаційних технологій -несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації
За наявністю умислу:	-умисні -випадкові

Закінчення табл. 1.3

Класифікаційна ознака	***Види загроз***
За проявом та правовими наслідками	-злочин -шахрайство -хуліганство
За типом	-програмні -апаратні -інші
За метою	-оперативні -тактичні -стратегічні

Джерело: розвинено за [33, 43, 46, 47, 48, 49]

** запропоновано автором*

Водночас погоджуємося з тезою О. Золотар та І. Трубіна про важливе теоретико-прикладне значення класифікації загроз інформаційній безпеці. «Вона обумовлена потребою внутрішньологічної 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 в розробці методів аналізу цих загроз, перевірки її достовірності, виявлення шляхів їх нейтралізації» [50]. Тобто розуміння, уміння ідентифікувати, аналізувати загрози інформаційній безпеці, розробляти шляхи їх запобігання, нейтралізації лежить в основі захисту корпоративної інформації.

Таким чином, **захист корпоративної інформації пропонуємо визначати як систему принципів, методів та процесів протидії загрозам інформаційній безпеці підприємства, які спрямовуються на порушення функціонування корпоративного інформаційного поля і передбачає їх ідентифікацію, аналіз, запобігання та нейтралізацію**.

Узагальнюючи викладений вище матеріал, можна таким чином представити концепт-модель місця захисту корпоративної інформації в забезпеченні ефективного функціонування підприємства (рис. 1.5).

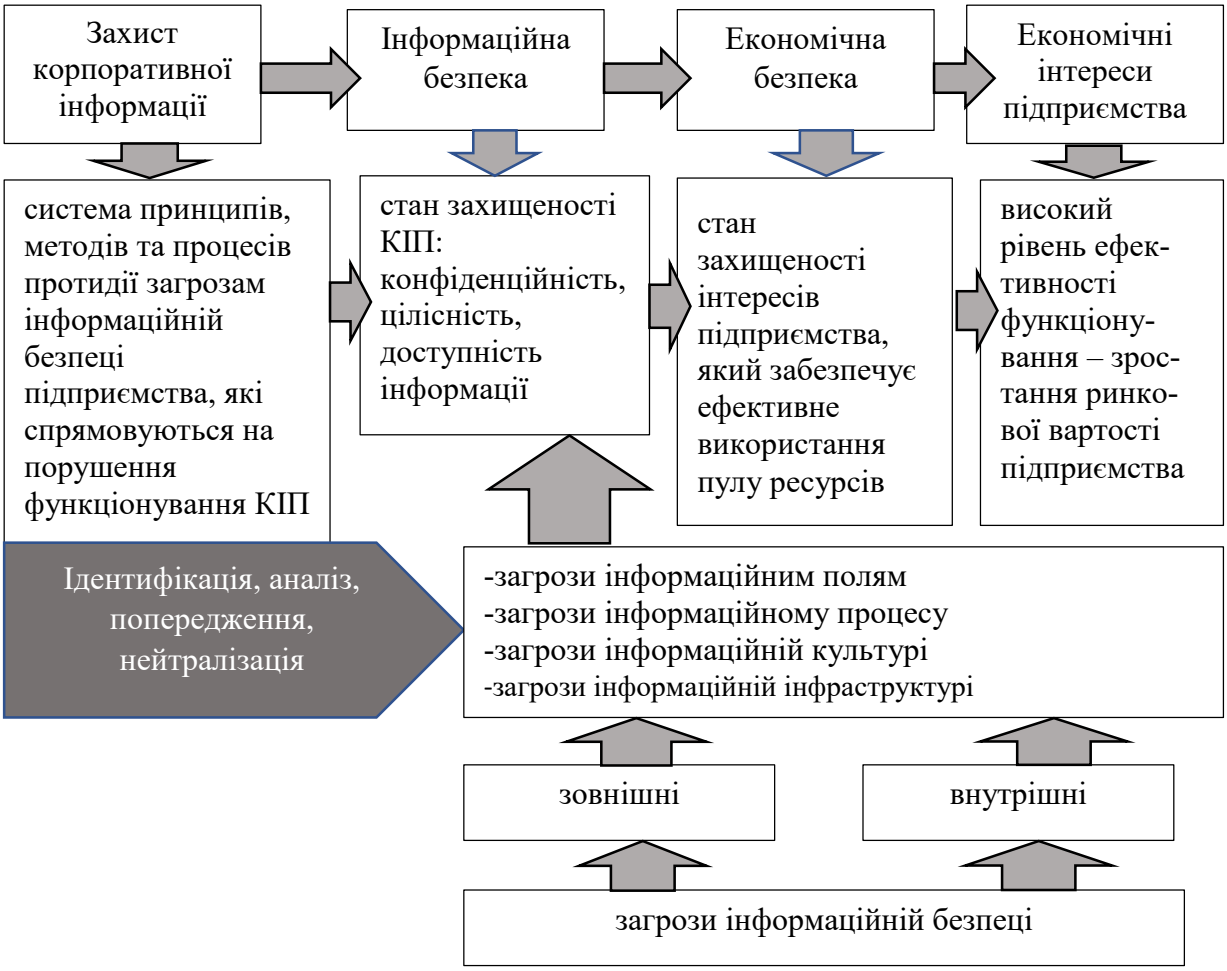


Рис. 1.5. Концепт-модель місця захисту корпоративної інформації в забезпеченні ефективного функціонування підприємства

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.

1.3. Видова трансформація економічної ефективності управління підприємством

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.

Не дивлячись на значні доробки з дослідження проблематики ефективності, наразі відсутній єдиний підхід до трактовки 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, що забезпечують усі види діяльності підприємства. Таким чином, очевидною є значимість ефективності управління в 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 [51]:

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

– виробництво продукту певної вартості при найменших витратах ресурсів;

– міру витрат підприємства на досягнення поставлених цілей.

Варто зазначити, що остання трактовка більш близька за змістом до поняття «результативність», дослідження якої вже виокремилось в окремий напрям [51–55]. Таким чином, доходимо до висновку, що ефективність усе ж таки характеризує

співвідношення між певними економічними результатами функціонування підприємства та використаними для їх одержання ресурсами або 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 урахування альтернативних витрат.

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

Наразі виокремлюються різні види ефективності.

Так, за характером здійснюваних витрат розрізняють ефективність усіх 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 слід відносити до всієї сукупності ресурсів чи лише її спожитої частини. Сьогодні єдиної думки із цього приводу серед науковців немає. Тому погоджуємося з думкою про доцільність застосування обох видів ефективності.

Поширеним є поділ економічної ефективності за видами діяльності. Проте за цією класифікаційною ознакою окремі науковці при визначенні видів ефективності орієнтуються на види діяльності, що регламентуються стандартами бухгалтерського обліку та фінансової звітності підприємств [51], а інші деталізують на основі функціональних напрямів управління [52, 53, 54]. Нам імпонує перша точка зору, проте ми повною мірою не погоджуємося із трактовкою змісту цих видів ефективності, що запропоновані С. Лобовим. Відповідно, за цією

ознакою варто виокремити такі види економічної ефективності та їх таке змістовне навантаження:

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

– ефективність інвестиційної діяльності, яка 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. Проте єдина позиція щодо видів ефективності за цією класифікаційною ознакою відсутня, а ті, що пропонуються в літературі, мають фрагментарний характер [51–55]. Ми пропонуємо виокремлювати за цією ознакою види ефективності за бізнес-процесами верхнього рівня, зокрема:

– економічна ефективність основних бізнес-процесів, під якою варто розуміти 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 деталізуватися за видами бізнес-процесів різних рівнів.

Варто відзначити, 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 сходяться на думці щодо доцільності класифікації видів ефективності за умовами оцінювання, виокремлюючи реальну, розрахункову та умовну ефективність. Так, під реальною ефективністю розуміють 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 [52].

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 [51, 52, 54, 55].

Окремі науковці класифікують економічну ефективність за ступенем збільшення ефекту, пропонуючи розрізняти первісну та мультиплікаційну ефективність. Необхідність такого поділу видів ефективності, на думку науковців, викликана тим, що в результаті здійснення тих чи інших заходів може спостерігатися як одноразовий ефект, так і мультиплікаційний. Мова про мультиплікаційний ефект може йти тоді, коли початковий ефект повторюється й примножується на різних рівнях даного підприємства, а також поширюється на інші підприємства та організації [51, 52, 54, 55].

У наявних наукових підходах зустрічається класифікація економічної ефективності за метою визначення, у межах якої розрізняють абсолютну та порівняльну ефективність. Абсолютна ефективність характеризує загальну або питому (у 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 (напрямку діяльності) порівняно з іншими варіантами [51, 52, 54].

Н. Архіпов пропонує класифікувати економічну ефективність за стейкхолдерами, виокремлюючи ефективність для власників, для кредиторів, для постачальників, для персоналу тощо [55]. Погоджуємося з доцільністю такого підходу, особливо в умовах актуальності запровадження стейкхолдерського підходу у практику корпоративного управління, який вважають умовою стійкого

зростання. Він пропонує класифікувати економічну ефективність за обраними критеріями оцінювання, поділяючи на максимальну, мінімальну та цільову (оптимальну) [55]. Зазначений підхід вважаємо доречним, він є важливою характеристикою, у тому числі результату управлінської діяльності.

До вищезазначених видів 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 за оцінюваними показниками відповідає середньоринковим оцінкам, а висока – перевищує рівень середньоринкових показників. Зазначені види важливі для розуміння місця підприємства в конкурентному середовищі та розробленні заходів щодо підвищення його конкурентоспроможності.

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. Такий вид ефективності характеризується зростанням її індикаторів за рахунок запровадження різноманітних управлінських, технологічних, товарних, продуктових інновацій тощо.

Так, узагальнюючи наявні підходи, можна таким чином представити класифікацію видів економічної ефективності підприємства (табл. 1.4).

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 знаходиться в полі зору науковців, адже завжди актуальним лишається питання для власників, чи ефективно менеджмент компанії здійснює управління, для топ-менеджерів – чи

ефективно здійснюють свої функції менеджери нижчих ланок, якими будуть фінансові результати діяльності та показники ефективності його функціонування якщо підвищити рівень якості менеджменту?

Таблиця 1.4

Види економічної ефективності підприємства

Класифікаційна ознака	Види ефективності
характер здійснюваних витрат	ресурсна, витратна
вид діяльності	операційної діяльності, інвестиційної діяльності, фінансової діяльності
вид бізнес-процесу (БП)	основних БП, допоміжних БП, обслуговуючих БП
рівень оцінювання	підприємства, бізнес-одиниці, структурного підрозділу
ступінь збільшення ефекту	первісна, мультиплікаційна
мета визначення	абсолютна, порівняльна
стейкхолдер	власників, кредиторів, персоналу, постачальників, клієнтів
умови оцінювання	реальна, потенційна, розрахункова
критерій оцінювання	максимальна, мінімальна, цільова (оптимальна)
досягнутий рівень*	низька, середня, висока
основний фактор-акселератор формування*	досягнута за рахунок сприятливого зовнішнього середовища, за рахунок спрямованих управлінських дій

Джерело: узагальнено та розвинено за [51–55]

** запропоновано автором*

Не дивлячись на значну кількість публікацій, що спрямовані на дослідження цієї проблематики, наразі відсутні одностайні підходи, як до визначення змісту «економічної ефективності управління», так і виокремлення її видів. Водночас спостерігається неоднозначність трактувань ефективності управління та варіативність показників її оцінювання.

На сьогоднішній день у науковій літературі склалося 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 [56].

Другий підхід трактує ефективність управління як відносну міру результативності управлінських витрат (витрат на управління) [57]. Зазначений підхід є дещо вужчий попереднього, 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 слід 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: фінансові витрати на утримання керуючої системи, затрати часу на виконання певних операцій і всього процесу управління [58].

Четвертий підхід тлумачить ефективність управління як ступінь досягнення цілей управління діяльністю підприємства [58]. Погоджуючись із тим, що досягнення цілей є важливим завданням системи управління підприємством, на нашу думку, зазначене тлумачення ближче до поняття «результативність управління», адже економічна ефективність передбачає розуміння того, наскільки витратним було досягнення цілей.

П'ятий підхід трактує ефективність управління як ефективність управлінських рішень, а відтак її оцінка грунтується на ідентифікації цілей та критеріїв. Так, за наявності кількох цілей Л. Христенко рекомендує привести різні

цілі до єдиної оцінки та визначити ефективність кожного рішення за всіма цілями, обираючи при цьому найбільш ефективний варіант [59].

Шостий підхід трактує ефективність управління як ефективність управлінської праці. Погоджуємося з думкою Р. Вечерковські, що дане 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 [57].

Сьомий підхід розглядає економічну ефективність управління крізь призму відносної ефективності заходів на вдосконалення управління [58]. 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 трактовок поняття «економічна ефективність управління підприємством», насамперед, демонструє його комплексність та складність, яка обумовлюється складністю самого поняття «управління підприємством». Не випадково вивченню його змісту, методологічних засад формування присвячено значний науковий доробок [51–58].

У сучасних дослідженнях науковці описують різні аспекти цього поняття, зокрема:

1. Управління як мистецтво застосовувати накопичений досвід на практиці, спираючись на концепції, теорії, принципи, форми і методи, що лежать у його основі, для того, щоб члени колективу спрямовували свої зусилля на досягнення її цілей в умовах найбільш повного розкриття потенціалу колективу [60].

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 [60].

3. Управління як процес, що відображає прагнення інтегрувати всі види діяльності за рішенням управлінських проблем в єдиний ланцюг. Управління при цьому представляється як динамічно змінюючі у просторі та часі, пов'язані між собою управлінські функції, метою яких є вирішення проблем і завдань навчального закладу [60].

4. Управління як функція, яка реалізується через виконання ряду управлінських дій (функцій управління) – планування, організація, розпорядження, координація, контроль, мотивація, керівництво, комунікації, дослідження, оцінки, прийняття рішень, підбір кваліфікованих фахівців, представництво, ведення переговорів, укладення угод на освітні послуги [60].

5. Управління як вид практичної діяльності [61], який потребує спеціальної підготовки, набуття певних знань та компетентностей і передбачає виконання набору рутин.

6. Управління як орган чи апарат [61], який формується з певних організаційних структур, персоналу, який займається управлінською діяльністю.

7. Управління як соціальний інститут сучасного суспільства [61], існування якого ґрунтується на людській взаємодії, комунікації та кооперації та спрямоване на задоволення важливих суспільних запитів. Особливо ця грань управління посилюється в умовах відділення інституту власності від інституту управління.

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

Ситуаційний підхід – спосіб мислення відносно 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 даного підходу до управління сприяє більш ефективному

досягненню мети особливо на крупних підприємствах із великою кількістю поставлених до вирішення завдань [62].

Таким чином, ситуаційний підхід – це застосування методів адаптації на зміну факторів внутрішнього та зовнішнього середовища. 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 прикладання 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» [60].

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. Управління підприємством за функціонального підходу здійснюється як єдиним цілим за допомогою розпоряджень, наказів та дозволів, при цьому чим вищим є рівень управління, тим відповідальніші рішення на ньому приймаються [63]. Таким чином, на нижні рівні ієрархії делегуються лише повноваження щодо прийняття найменш значущих рішень. У цілому кожен структурний підрозділ за такої системи управління функціонує відокремлено, автономно від інших; рівень взаємодії між підрозділами визначається поділом праці та обміном матеріальними продуктами.

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 дозволяє усунути відособленість підрозділів і посадових осіб, розглядати діяльність у системі менеджменту якості не в статиці, а в динаміці, коли діяльність у 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 [60].

Системний підхід, який розглядає підприємство як систему, елементи якої взаємозв'язані між собою, дозволяє ефективно управляти всією системою на основі налагодженої роботи кожного з елементів. Системний підхід в управлінні базується на загальній теорії систем [62].

Системний підхід в теорії менеджменту визначає організацію як сукупність взаємопов'язаних елементів, які орієнтовані на досягнення єдиної кінцевої цілі 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 їх 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 та здійснення вибору; кількісна оцінка цілей та засоби їх досягнення, заснована на всебічній оцінці всіх можливих і планованих результатів діяльності [64].

Так, у найбільш узагальненому вигляді з позицій системного підходу під управлінням підприємством розуміють 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 [65]. Системний

підхід є найбільш комплексним, по суті об'єднує всі аспекти управління, які виокремлюються в інших підходах.

Виходячи із зазначених аспектів управління, як явища та підходів до його здійснення, його можна описати таким чином (рис. 1.6).

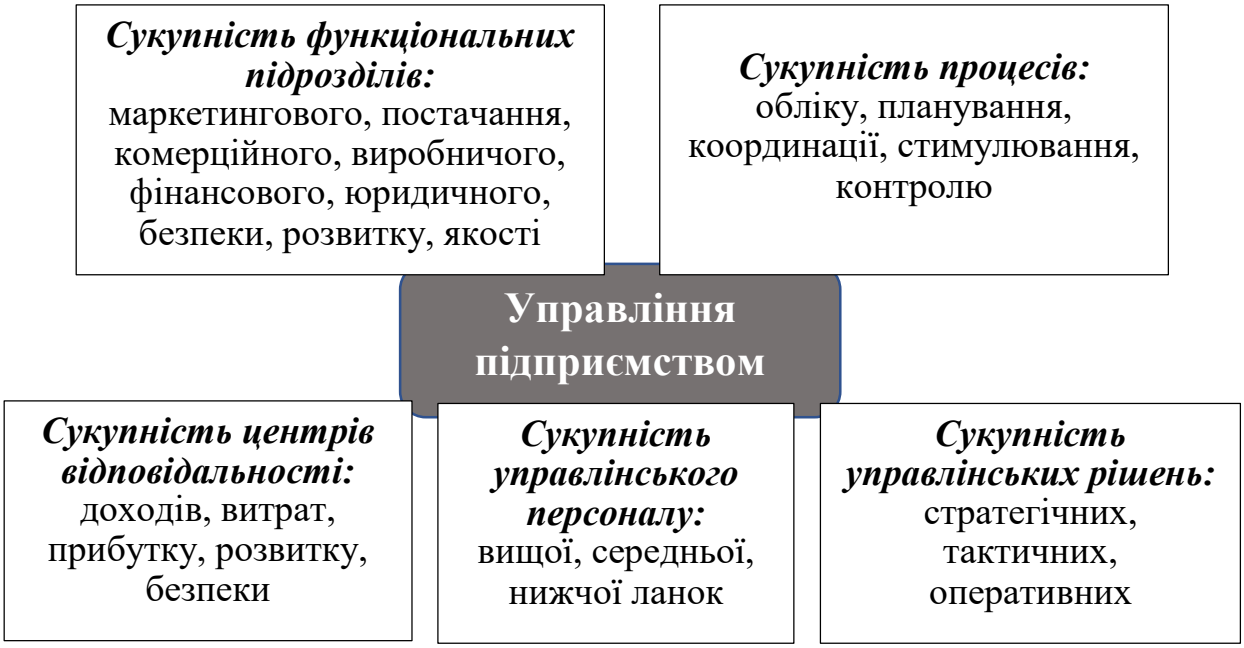


Рис. 1.6. Характеристики управління підприємством

Джерело: складено автором

Так, управління підприємством ґрунтується на певній організаційній структурі, яка передбачає виокремлення функціональних підрозділів, дивізіонів тощо. 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 і 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 із різною відповідністю часовому горизонту: стратегічних, тактичних, оперативних.

З розвитком та популяризацією системи контролю поширеним явищем стало виокремлення на підприємствах центів відповідальності, які можуть «накладатися» певним чином на функціональну структуру підприємства. Таким чином, управління можна також характеризувати як сукупність центрів відповідальності. Зазвичай, у літературі виокремлюють центри доходів, витрат, прибутку, розвитку. Ми пропонуємо додати до цього переліку центр безпеки, зважаючи на постійне нарощення загроз інтересам підприємства, високий рівень відхилення від середнього значення 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**.

Виходячи із цього, можна виокремити такі види економічної ефективності управління підприємством за елементами управління підприємством: **ефективність структурних підрозділів управління; ефективність процесів управління; ефективність центрів відповідальності; ефективність управлінського персоналу; ефективність управлінських рішень** та деталізувати їх таким чином (див. табл. 1.5).

Таблиця 1.5

Класифікація видів економічної ефективності управління підприємством

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

Джерело: складено автором

Так, окрім зазначених вище видів економічної ефективності управління підприємством за елементами управління підприємством, пропонуємо додати до них види ефективності за метою визначення та досягнутим рівнем, які пропонувалися у видовій класифікації економічної ефективності функціонування підприємства. Адже саме ці види ефективності дозволяють з одного боку

ідентифікувати достатність зусиль у вдосконаленні системи управління та здійснювати їх порівняльну оцінку.

Окремі види ефективності також можна деталізувати на більш локальні (прості) види. Зокрема, економічну ефективність окремих структурних підрозділів можна класифікувати на види 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 ефективності служби безпеки (рис. 1.7).

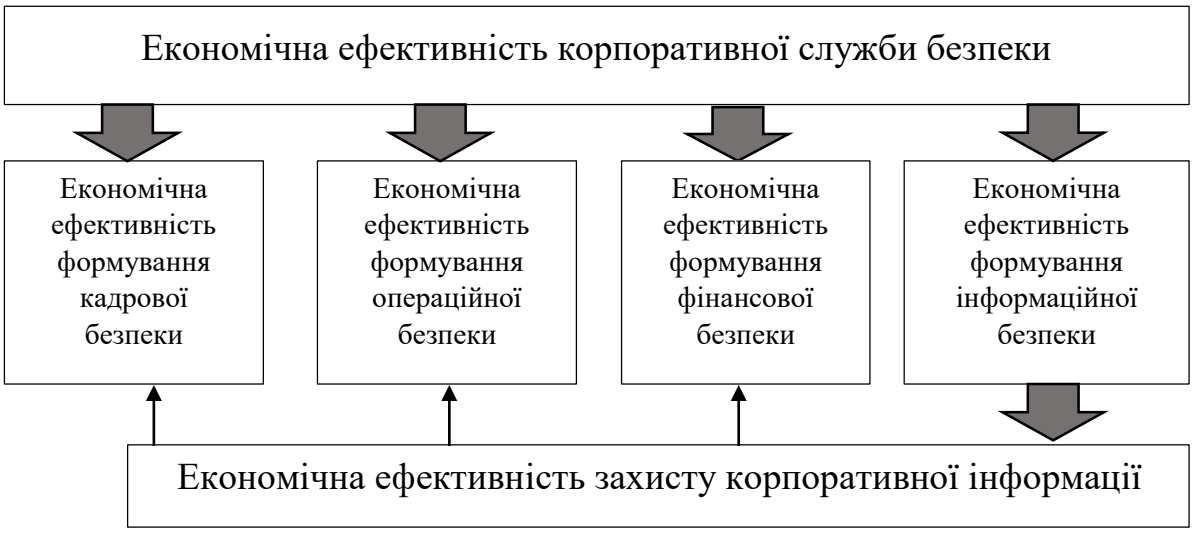


Рис. 1.7. Види економічної ефективності корпоративної служби безпеки

Джерело: складено автором

Так, виходячи з логічного зв'язку між захистом корпоративної інформації та формуванням інформаційної безпеки, її впливу на досягнення та збереження економічної безпеки (що розглянуто в п.1.2), бачимо особливе місце економічної ефективності захисту корпоративної інформації у формуванні економічної ефективності інформаційної безпеки та її інших видів, що повинні забезпечуватися корпоративною службою безпеки. Будучи важливим підвидом економічної ефективності формування інформаційної безпеки, економічна ефективність захисту корпоративної інформації суттєво впливає на ефективність формування кадрової, операційної, фінансової безпеки, адже в корпоративному

інформаційному просторі зберігається та передається інформація з різних предметних областей.

На сьогоднішній день у спеціалізованій літературі відсутнє визначення поняття «економічна ефективність захисту корпоративної інформації». Виходячи з нашого розуміння змісту понять «захист корпоративної інформації» (що розкривається у п.1.2) 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, запобігання та нейтралізації загроз порушення функціонування корпоративного інформаційного поля.

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 уразливим для сучасних загроз.

Відповідно до загальноприйнятої думки, характерної для більшості фахівців в області інформаційної безпеки (ІБ), сформувалася думка, що інвестування в ІБ і її концепція для конкретного об’єкта інформатизації (ОБІ) будуть ефективним, якщо забезпечити виконання вимог державних нормативних документів і стандартів. Така думка сформувалася на основі, єдиної загальновизнаної методики оцінки економічного ефекту від інвестування в ІБ ОБІ [66, 67]. Зауважимо, що в даному 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 [68].

Складність оцінювання реального ефекту від інвестування в захист корпоративної інформації (ЗКІ) обумовлюється досить великим переліком специфічних для сектору захисту інформації та кібернетичної безпеки чинників. Загалом відзначимо лише істотний вплив на ефективність інвестування в ЗКІ таких

факторів як: 1) постійно мінливий ландшафт кіберзагроз; 2) різноваріантність стратегії і тактики атакуючої сторони (комп'ютерних зловмисників); 3) швидкий розвиток технічних засобів ЗКІ і кібербезпеки (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'єктах інформатизації (ОБІ). Саме ця обставина дає можливість об'єктивно оцінювати ефективність їх застосування, а, отже, і результативність інвестицій у ЗЗКІ на ОБІ [69, 70].

Додаткова складність при оцінюванні ефективності інвестування в ЗКІ ОБІ пов'язана з невизначеністю результатів функціонування ЗЗКІ. На етапі проєктування ЗЗКІ присутні фактори невизначеності. Наприклад, пов'язані з тим, що може скластися така ситуація, при якій сторона захисту ОБІ витратить сотні тисяч грошових од. або навіть мільйони на захист від складних націлених кібератак, а атакуючій стороні часто досить удатися до невеликих за витратами («інвестицій у кібератаку») методів соціальної інженерії. Така тактика застосування методів соціальної інженерії в ряді випадків допомагала обходити найсучасніші ЗЗКІ [71]. Таким чином, під час реалізації проєктів у сфері ЗКІ рівень функціональності ЗЗКІ може знизиться. Отже, з позиції методології моделювання ефективності інвестування в ЗКІ ряд функціональних метрик ЗЗКІ не може бути тотожно вираженим і описаним 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 і т. ін.). Цей рівень у більшості випадків залежить від розміру потенційного запобігання шкоди для інформаційних масивів ОБІ. У такому випадку 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 [74].

Справжня вартість захисту корпоративної інформації складається з витрат на запобігання кібератак (програмне забезпечення; навчання цифрової грамотності працівників; на організацію системи безпеки, мотиваційної політики та корпоративної культури) і на ліквідацію наслідків від кібератак (викуп, відновлення операційних процесів, репутації) [74].

Втрати підприємства у разі успішної кібератаки:

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

2. По-друге, якщо кібератака зловмисників мала успіх, 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, у свою чергу, веде до зниження конкурентоспроможності підприємства [74].

3. По-третє, незалежно від того, яке рішення приймають керівники підприємств – 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 знижує конкурентні можливості підприємства [74].

4. По-четверте, викрадення бази даних зловмисниками може бути пов'язане не тільки з особистими даними клієнтів, але й з конфіденційною інформацією підприємства. Оприлюднення цих даних призведе до втрати конкурентних переваг компанії. Конфіденційна інформація контрагентів також опиняється під загрозою

оприлюднення, що, у свою чергу, призведе до штрафів, санкцій, судових витрат [74].

5. По-п’яте, викрадення, шифрування даних призводить до порушення бізнес-процесів підприємства. Але не менш важливим є втручання в закупівельні, збутові та інші бази за видами діяльності підприємства і їх пошкодження, що може супроводжуватися іншою формою кіберзагрози, наприклад вірусною атакою. Тимчасова втрата доступу до платіжної системи банку, бухгалтерських, кур’єрських програм та іншого призводить до тимчасової дезорієнтації та уповільнення основних бізнес-процесів і, як наслідок, – зниження обсягу виручки від реалізації та інших ключових показників діяльності підприємства [74].

6. По-шосте, стосунки з інвесторами. Як правило, крупні 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 за розміром підприємства, у 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 [74].

Економічний ефект захисту корпоративної інформації сучасні автори розраховують через темп зміни доходу (прибутку), відвернений збиток. Розрахунок обох показників є складним [74].

Методику розрахунку темпів зміни доходу (прибутку) можна поділити на два підходи через розрахунок: по-перше, приросту доходу (прибутку); по-друге, недоотриманої суми доходу (прибутку).

Розрахунок приросту доходу (прибутку) залежить від наявності достатнього рівня ІБ 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 вимагає своєї системи оцінки. Розрахунок недоотриманої суми доходу (прибутку) може розраховуватися через

імовірність настання кібератаки або є результатом фактичної кібератаки. Розрахунок показника ймовірності настання кібератаки 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 в разі успішної кібератаки [74].

Методика розрахунку економічного ефекту через відвернений збиток передбачає аналіз усіх 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 [74].

Можливості сучасних методик, які використовуються для оцінки економічної ефективності, представлено в табл. 1.6.

Дані табл. 1.6 відображають можливість кожного із методів визначати складові економічної ефективності захисту корпоративної інформації. З огляду на сутність економічної ефективності, насамперед, необхідно звернути увагу на методики, які дозволяють оптимізувати (мінімізувати) витрати на ІБ.

AIE передбачає оцінку ефективності інвестицій в технології безпеки з використанням експортних оцінок якісних показників. У цьому разі важливу роль відіграють особисті якості експертів (знання, досвід) [74].

Використання *AIE* доволі складне і вимагає звернення до компанії-консультанта. Застосування методики *PM* дозволяє оптимізувати витрати в режимі реального часу, але оцінка і прийняття рішень покладено на керівника і залежить від його особистих якостей. Метод *ROV* є трудомісткім і обмеженим у використанні, застосовується на стадії проєктування [74].

Таблиця 1.6

Методики оцінки економічної ефективності захисту корпоративної інформації

Назва методики	Оптимізація витрат	Визначення результату	Максимізація результату	Оцінка ризиків	Розробка 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 [66–72, 74]

Застосування *BSC* передбачає розроблення унікальних критеріїв: залежно від стратегії підприємства, показників оцінки задаються планові значення показників. Через те, що ІБ є допоміжною системою, виникає ряд проблем у побудові збалансованої моделі. Стратегічні показники підприємства, пов'язані з основною діяльністю, необхідно пов'язати з показниками інформаційної безпеки. *ABC*-метод є орієнтованим на виробничу і логістичну систему підприємства, пов'язаний із визначенням і розподілом витрат [74].

Аналіз можливостей розглянутих методів визначення розміру витрат і результату, оцінки економічної ефективності дозволяє зробити такі висновки [74]:

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

– метод *Customer Index* найбільше 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 аналізу і мінімізації витрат на підприємстві, але для визначення результату необхідно застосовувати принаймні ще одну методику;

– метод *DCF* носить комплексний підхід при оцінюванні інвестиційних витрат, ураховує 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, проте суттєво обмежена щодо оцінювання ризиків;

– модель *NPV* орієнтована на врахування інтересів інвесторів, повною мірою дозволяє оцінювати витрати та ефект;

– методи імітаційного моделювання та генетичного алгоритму максимально гнучкі та націлені на врахування ризиків при визначенні витрат та ефекту;

– наведені методи базуються на аналізі даних попередніх періодів (сталого розвитку) і під впливом пандемії *COVID-19* і пов'язаних із цим карантинних обмежень 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.

Висновки до розділу 1

1. Зростання ролі інформації в 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.

2. 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, яка є станом та результатом її функціонування, способом її розвитку та представлення.

3. Корпоративний інформаційний простір упродовж існування та розвитку корпоративних структур пройшов складний процес еволюції, у межах

якого нами виокремлено три принципові етапи: «паперовий», «автоматизований» і «мережевий». Останній етап, що триває і на теперішній час, характеризується глобальним характером, високим рівнем інтенсивності та швидкості поширення інформації, її «надлишковим» характером, зниженням витрат часу на обробку та аналіз інформації, зростанням витрат на убезпечення інформаційного простору, суттєвим впливом на трансформацію бізнес-моделі, організаційної структури підприємства, способу виробництва товарів та послуг. Таким чином, можна говорити про значне посилення впливу корпоративного інформаційного простору на розвиток підприємства.

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

5. В умовах цифровізації суспільства, зростаючої ролі інформації як в житті людини, так і у функціонуванні підприємства, у 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, що спрямовані на всі компоненти корпоративного інформаційного простору. З'ясовано роль та місце захисту корпоративної інформації у процесі формування інформаційної безпеки та економічної ефективності функціонування підприємства.

6. 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 дозволяє на якісному рівні виконувати йому свої функції: інтегруючу, 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 обсягу ресурсів, а також удосконалювати параметри корпоративного інформаційного простору.

7. Захист корпоративної інформації пов’язаний із захистом корпоративного інформаційного поля від різноманітних загроз із метою збереження високої якості його параметрів та забезпечення можливості ефективно виконувати ним свої функції. Із 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 в забезпеченні ефективного функціонування підприємства.

8. 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 в дослідженні розмежовано поняття «економічна ефективність функціонування підприємства», «економічна ефективність управління підприємством» та розглянуто видову трансформацію останньої.

9. Виходячи із систематизації основних характеристик поняття «управління», підходів до його організації з позицій системного підходу визначено економічну ефективність управління підприємством як інтегровану характеристику ефективності (міри отриманого ефекту до ресурсів / понесених витрат) функціонування всіх його підсистем: функціональних підрозділів, центрів відповідальності, процесів, управлінських рішень, управлінського персоналу, яка суттєво детермінує ефективність функціонування підприємства. Таким чином, представлено деталізовану класифікацію видів економічної ефективності управління підприємством, у межах якої чільне місце посідає економічна ефективність захисту корпоративної інформації – міра економічного ефекту витрачених ресурсів на реалізацію системи заходів з ідентифікації, аналізу, запобігання та нейтралізації загроз порушення функціонування корпоративного інформаційного поля.

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

Основні результати розділу опубліковані у наукових працях автора: [1, 5, 10, 13, 16, 23] – відповідно до списку опублікованих праць за темою дисертації на початку роботи.

Список використаних джерел до розділу 1

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. N. Y. : Bantam, 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. S. Soft Power: The Means To Success In World Politics. N. Y. : PublicAffairs, 2005. 191 p.
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 / В.В. Домарев. К. : ООО «ТИД Diasoff», 2002. 686 с.
10. Мельниченко С. В. Інформаційні технології в туризмі: теорія, методологія, практика : монографія. К. : Київ. нац. торг.-екон. ун-т, 2007. 493 с.
11. Чумаченко М. Г. Економічний аналіз : навч. посіб. / М.Г. Чумаченко. К. : КНЕУ, 2001. 540 с.
12. Денисенко М. П. Інформаційне забезпечення ефективного управління підприємством / М.П. Денисенко, І.В. Колос // Економіка та держава. 2006. № 7. С. 19–24.
13. Батюк А. Є. 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 / Валентина Іванова // 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 Національного університету оборони України імені Івана Черняховського. 2013. № 3(49). С. 26–32.

17. Яковенко М. Інформаційний простір: філософські аспекти формування поняття / Марина Яковенко // Вісник Національного університету «Львівська політехніка». 2011. № 692: Філософські науки. С. 22–27.
18. Зв'язки з громадськістю як інструмент маркетингових комунікацій / 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 в суспільстві. Психолого-педагогічні проблеми сучасної освіти. Харків. 1999. 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. New York and Geneva: UNCTAD, United Nations, 2007.
23. Reich R. B. The Work of Nations: Preparing Ourselves for 21st Century Capitalism. NY, 1992. 331 p.
24. Ареф'єва О. В. Корпоративне управління: еволюція, становлення, розвиток: Монографія / О.В. Ареф'єва, Н.В. Васюткіна. К.: Ліра-К, 2013. 180 с.
25. Довгий С. О. Інститут телекомунікацій і глобального інформаційного простору [Електронний ресурс] / С.О. Довгий. 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.
28. Розвиток інформаційного простору як запорука вдосконалення управління державою власним гуманітарним капіталом / І. М. Кармелюк // 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 [Електронний ресурс]. 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. 2019. №14. С. 186–192.
32. Скороварова Є. Концепція комунікації Н. Лумана [Електронний ресурс] / Є. Скороварова // Ученые записки Таврического национального университета им. В. И. Вернадского. URL: http://snphilcultpolsoc.crimea.edu/arhiv/2013/uch_24_1_2_filosof/008skvor.pdf (дата звернення 10.06.2022).
33. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 р. № 537-V. Дата оновлення 06.02.2007. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 13.06.2022).
34. Сороківська О. А., Гевко В. Л. Інформаційна безпека підприємства: нові загрози та перспективи // Вісник Хмельницького національного університету. 2010. № 2. Т. 2. С. 32–35.
35. 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.

36. Горбатюк О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть / О.М. Горбатюк // Вісник Київського університету імені Т. Шевченка. 1999. Вип. 14 : Міжнародні відносини. С. 46–48.
37. Богуш В. Інформаційна безпека держави / В. Богуш, О. Юдін; [Гол. ред. Ю.О. Шпак]. К.: «МК-Прес», 2005. 432 с.
38. Науменко Н. Ю. Особливості конкретизації методології формування інформаційного простору регіональних соціально-економічних систем // Modern Economic. №14. 2019. С. 186-192.
39. Кузьміна О. М. Актуалізація формування єдиного інформаційного середовища організації // Східна Європа: Економіка, Бізнес та Управління. № 5(16). 2018. С. 289-292.
40. Дубняк К. А. Інформаційний простір: структура та функціональні параметри // Держава та регіони. Серія «Соціальні комунікації». №4 (24). 2015. С. 21-25.
41. Близнюк І. М. Інформаційна безпека України та заходи її забезпечення / І.М. Близнюк // Науковий вісник Національної академії внутрішніх справ України. 2008. № 5. С. 206-214.
42. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. [Чинний від 1997.01.01]. Вид. офіц. Київ: Держстандарт України, 1996. 7 с.
43. Ліпкан В. А. Національна безпека України : навч. пос. / Володимир Ліпкан. Київ: КНТ, 2009. 576 с.
44. Логінов А. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : дис. на здобуття наукового ступеня кандидата юридичних наук : 12.00.07 / А.В. Логінов. Національна академія внутрішніх справ України. К., 2005.
45. Євдоченко Л. О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації : автореф. дис. на здобуття наук. ступеня канд. наук з держ. упр. : 25.00.01 / Л.О. Євдоченко. – Львів, 2011. 24 с.

46. Макарова М. В. Електронна комерція: посібник для студентів вищ. навч. закладів / М.В. Макарова. К.: Видавничий центр «Академия», 2002. 272 с.
47. Погребняк А. В. Технології комп'ютерної безпеки : монографія / А.В. Погребняк. Рівне: МЕГУ, 2011. 117 с.
48. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник / В.Л. Бурячок, Г.М Гулак, В.Б. Толубко. К.: ТОВ «СІК ГРУП УКРАЇНА», 2015. 449 с.
49. Литвинов В. В. Моделювання та аналіз безпеки розподілених інформаційних систем: навч. пос. [для студ. спец. 121 «Інженерія про- грамного забезпечення»] / В.В. Литвинов, В.В. Казимир, І.В. Стеценко та ін. Чернігів: Чернігів. нац. технол. ун-т, 2016. 254 с.
50. Золотар О. О., Трубін І. О. Класифікація загроз інформаційній безпеці // Інформація і право. № 3(9). 2013. С. 105–112.
51. Лобов С. П. Сучасні концепції економічної ефективності діяльності та ефективності управління підприємством [Електронний ресурс] / С.П. Лобов // Ефективна економіка. 2015. №4. URL: http://www.economy.nayka.com.ua/?op=1&z=4011 (дата звернення: 15.06.2022).
52. Братанич М. В. Визначення сутності економічної ефективності та класифікація її видів / М.В. Братанич, Т.В Полозова // Економіка промисловості. 2010. № 4. С. 153–155. URL: http://nbuv.gov.ua/UJRN/econpr_2010_4_26 (дата звернення: 15.06.2022).
53. Говорушко Т. А. Ефективність як економічна категорія / Т.А. Говорушко // Наукові праці НУХТ. 2007. № 20. С. 74–76.
54. Економіка підприємства: підручник / за заг. ред. С.Ф. Покропивного. 2-ге вид., перероб. та доп. Київ : КНЕУ, 2005. 528 с.
55. Архіпов Н. М. Види ефективності операційної діяльності підприємства торгівлі // Науковий вісник Ужгородського національного університету. Серія «Міжнародні економічні відносини та світове господарство». 2018. Випуск 18. Ч. 1. С. 21–25.

56. Синицына Т. А. Оценка эффективности системы управления промышленным предприятием: целевой подход: дис. канд. экон. наук: спец. 08.06.01 «Экономика, организация и управление предприятиями» / Т.А. Синицына. Одесса: ОГЭУ, 2004. 187 с.
57. Вечерковски Р. З. Управление знаниями при формировании конкурентных преимуществ предприятия : дис. канд. экон. наук: спец. 08.06.01 «Экономика, организация и управление предприятиями» / Р.З. Вечерковски. Луганск : ВНУ им. В. Даля, 2004. 216 с.
58. Щеглова О. Ю., Судакова О. І., Лаже М. В. Ефективність управління підприємством та підходи до її визначення // Науковий вісник Ужгородського національного університету. 2017. Вип.12. Ч. 2. С. 186–189.
59. 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)» / Л.М. Христенко. Луганск: ВНУ ім. В. Даля, 2007. 192 с.
60. Кононова І. В. Аналіз підходів до управління підприємством у сучасних умовах // Прометей. № 1(40). 2013. С. 146–151.
61. Поканевич Ю. В. Управління як складна багатовимірна категорія // Вісник ЖДТУ. 2009. № 1(47). URL: http://nbuv.gov.ua/portal/Soc_gum/Vzhdtu_econ/2009.1/44.pdf (дата звернення: 15.06.2022).
62. Харченко В. А. Системний підхід до стратегічного управління підприємством / В.А. Харченко // Економічний вісник Донбасу. 2013. № 1. С. 157–160.
63. Семон Б. Й. 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).
64. Дідур К. М. Системний підхід до управління підприємством та персоналом підприємства / К.М. Дідур // Ефективна економіка. 2012. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=1079 (дата звернення: 15.06.2022).

65. Устенко А. О. Система управління підприємством // Вісник Прикарпатського університету. Економіка. 2014. Випуск X. С. 96-103.
66. 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.
67. 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.
68. 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.
69. Chronopoulos M., Panaousis E., Grossklags J. An options approach to cybersecurity investment // IEEE Access, 2017. № 6, P. 12175–12186.
70. 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.
71. 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.
72. Frolick M. N., Ariyachandra T. R. Business Performance Management: One Truth // Information Systems Management. 2006. № 23(1). P. 41–48.
73. Чубаєвський В. Корпоративний інформаційний простір: сутність та еволюція // Scientia Fructuosa (Вісник Київського національного торговельно-економічного університету). 2022. № 4. С. 84–97.
74. Чубаєвський В. І. Методичний підхід до оцінки економічної ефективності системи захисту корпоративної інформації // Електронний журнал «Ефективна економіка». 2022. № 11. URL: https://nayka.com.ua/index.php/ee/article/view/730/738 (дата звернення: 21.11.2022).

РОЗДІЛ 2
МЕТОДОЛОГІЧНІ ОСНОВИ УПРАВЛІННЯ КОРПОРАТИВНОЮ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

2.1. Концепція формування корпоративної інформаційної безпеки

Нагальна актуальність та необхідність ефективного захисту корпоративної інформації, доведена в попередньому розділі дослідження, вимагає розроблення та запровадження ефективних програм та інструментів захисту корпоративної інформації. Відтак, корпоративний сектор потребує формування власного концептуального бачення такого захисту.

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

З огляду на те, що концепція на думку дослідників істотно відрізняється від теорії не тільки своєю незавершеністю, але й недостатньою верифікацією [1], розглядається як сурогатна форма теорії, головне призначення якої полягає в інтеграції певного масиву знання, наразі відсутнє єдине чітке бачення структурних елементів концепції.

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

Так, 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]

Так, відповідно до цього документу, «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 із боку сторонніх суб'єктів [3].

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 відображатись і на концепції корпоративної інформаційної безпеки.

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

Так, М. 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 наш погляд, 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 думку В. Кононовича та М. Тардаскіна концепція інформаційної безпеки викладає систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації та інформаційних ресурсів [9]. Такий підхід, на наше переконання, є більш строгим із точки зору загальнонаукової трактовки терміна «концепція», проте містить певну тавтологію. Адже концепція за своєю

суттю є системою поглядів. Натомість логічна структура концепції має розкривати крізь призму яких структурних елементів транслюються ці погляди. На нашу думку, найкращим чином така трансляція відбувається шляхом окреслення обраних методологічних підходів, що покладаються в основу концепції, що відповідає загальнонауковій трактовці цього терміна.

На думку Ю. 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 наш погляд, 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 через обрану методологію формування, окреслені принципи та розроблений механізм забезпечення. Таким чином, концепція формування корпоративної інформаційної безпеки містить три принципові структурні компоненти: методологічна основа, принципи, механізм, які знаходяться в логічному зв’язку та підпорядкуванні (див. рис. 2.1).

Рис. 2.1. Елементи концепції формування корпоративної інформаційної безпеки

Джерело: розроблено автором

Так, на наш погляд, базовим елементом концепції є саме її методологічна основа. Саме вона індивідуалізує концепції корпоративної інформаційної безпеки на різних підприємствах та в наукових дослідженнях. Адже саме обрана методологічна база обумовлює принципи та механізм формування корпоративної інформаційної безпеки. Виходячи з того, що, на наше переконання, забезпечення інформаційної корпоративної безпеки з одного боку має ґрунтуватися на строго окреслених наукових засадах, а з іншого боку носити суто прагматичний характер,

вважаємо за потрібне в межах компоненту «методологічна база» виокремити два підрівні «метаметодологія» та «підходи до управління».

Метаметодологія визначає загальні філософські основи пізнання світу та окремих явищ та процесів. Так, серед наявних загальнонаукових та філософських концепцій пізнання світу, яка останнім часом стала мейнстрімом в економічній методології, у тому числі, є позитивізм, який пройшов уже 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 [11].

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

Таким чином, позитивізм в економічній теорії ґрунтується на філософії позитивізму, що визнає в якості джерела 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 наш погляд, може виступати основою формування концепції корпоративної інформаційної безпеки, адже захист корпоративної інформації потребує постійного 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 виступає нормативна методологія. Так, С. Мочерний визначає нормативну економічну теорію як теорію, у якій аналіз окремих економічних явищ або процесів, національної економіки загалом дається на основі оцінок ученого з погляду інтересів окремих соціальних верств, груп, населення країни або загальнолюдських інтересів з урахуванням їх справедливого або несправедливого характеру [12].

Словник економічних термінів під нормативною економічною теорією розуміє теорію, яка здатна не тільки пояснити економічні явища і події, але 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 виходячи із 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 власне й описує бажаний (ідеальний) стан об’єкта.

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

Інший підрівень методології – підходи до управління – спрямований на конкретизацію метаметодології і 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, урахування найбільш істотних рис системи, якими, на думку Б. Холод є:

а) наявність різних елементів, складових системи;

б) наявність взаємозв'язку елементів системи;

в) наявність мети, що є початком системи, що пов'язує і визначає взаємодію елементів [14].

Таким чином, під системою автор розуміє 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 [15]:

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 спрямовують систему на високий рівень організації і що дають 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 і 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, оцінка бізнес-процесів дозволяють оптимізувати їх вартість, якісні параметри, адаптуватися до змін зовнішнього середовища, забезпечуючи стійкість системи та її фінансових результатів. Фокусування уваги на бізнес-процесах підприємства пов'язаний з процесним підходом.

М. 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 дійсно дозволяє вдосконалювати бізнес-модель підприємства, шукати слабкі місця в 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.

Реалізація окремих заходів щодо вдосконалення бізнес-процесів захисту корпоративної інформації часто потребує серйозних фінансових витрат, носить інноваційний характер. Ці заходи реалізуються як інвестиційні проєкти, які спрямовані на модернізацію інформаційної інфраструктури тощо. Відтак 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 реалізацію рішення унікального завдання в заданий термін із заданими ресурсами. Основними особливостями проєктного управління є: розгляд проєкту як унікальної комбінації процесів; зосередження прав і відповідальності за досягнення результатів проєкту в 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 проєкту процесів [17].

При 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 кроці 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 20-го сторіччя до концепцій ключових компетентностей, динамічних здібностей (90-ті роки 20-го ст.) та концепції ресурсних переваг (2000-ні 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.

Погоджуємося 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, ряд науковців пропонують вважати ще одним фактором виробництва. Більше того, з поширенням використання інформаційних технологій у діяльності соціально-економічних систем інформація починає розглядатися як основа для отримання ресурсів вищого порядку – знань.

Знання є невіддільними від людини і вони визначають можливості використання будь-яких матеріальних та нематеріальних ресурсів із 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. 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 в центрі уваги попередніх концепцій стратегічного управління [19].

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

Незважаючи на відмінності у визначеннях і незалежно від галузевих, функціональних і технологічних особливостей організаційних здатностей, у сучасній літературі є консенсус із приводу їх загальних характеристик, якими прийнято вважати [18]:

– 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 новітній трактовці Д. Тіса динамічні здатності організації містять чотири організаційні вміння [23]:

– рутинизовані процеси управління інноваціями і 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) [23].

На думку авторів концепції, динамічні здатності можливо 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. Однак 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, що її вона сприйняла або успадкувала [19-23].

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, конфіденційності інформації, а в цілому посилюють позицію підприємства за всіма видами активів.

Так, 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 і адекватність заходів 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

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 усього 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 передачі 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 має, насамперед, не порушувати зазначені принципи та сприяти, таким чином, формуванню національної інформаційної безпеки.

Наразі в наукових дослідженнях відсутній єдиний підхід до визначення принципів формування корпоративної інформаційної безпеки.

Так, І. Маркіна пропонує дотримуватися таких принципів формування корпоративної інформаційної безпеки: законність, дотримання балансу інтересів особи, суспільства і держави; системність; плановість; комплексність; безперервність; взаємна відповідальність суб'єктів забезпечення інформаційної безпеки, їх взаємодія; спадкоємність і безперервність удосконалення; розумна достатність; персональна мінімізація повноважень; наукова обґрунтованість і

технічна реалізація; обов’язковість контролю; превентивний характер проведення заходів 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 дослідників [25–37].

На наш погляд, зазначені принципи варто доповнити такими:

Принцип креативності та інноваційності, який полягає в 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 світі інформаційної безпеки, що сприятиме в цілому більш конкурентоздатній позиції по активах.

Принцип економічної ефективності, який передбачає забезпечення порівняльності 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 виступає 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 мають розглядатися в комплексі зі станом інших видів ресурсів.

Принцип ризик-орієнтованості, який передбачає дослідження інформаційних загроз у контексті вивчення ризиків підприємства. Таким чином, 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 підтримання інформаційної безпеки мають лежати в межах діючого правового поля
дотримання балансу інтересів особи, суспільства и держави	заходи убезпечення інформації мають відповідати принципам національної інформаційної безпеки, не порушувати прав та інтересів окремих осіб (працівників, клієнтів тощо) та максимально захищати корпоративний інформаційний простір
системність	заходи убезпечення інформації мають узгоджуватися та оцінюватися з позицій впливу та можливих наслідків на всі підсистеми підприємства
плановість	підприємство повинно мати чітку стратегію та оперативно-тактичний план розробки та реалізації заходів убезпечення інформації
комплексність	заходи убезпечення мають охоплювати всі елементи корпоративного інформаційного поля
безперервність	заходи убезпечення інформації мають відбуватися на постійній основі
взаємна відповідальність суб'єктів забезпечення інформаційної безпеки, їх взаємодія	усі суб'єкти забезпечення корпоративної інформаційної безпеки мають діяти узгоджено та відповідально, дотримуватися встановлених регламентів та нести відповідальність за якість та результати своїх рішень
розумна достатність	заходи убезпечення мають відповідати ресурсним можливостям підприємства та потенційним загрозам інформаційній безпеці
персональна мінімізація повноважень	дотримання балансу повноважень, що забезпечує можливість захисту інформації в умовах звільнення відповідального працівника та уникнення персональних ризиків
обов'язковість контролю	постійний моніторинг і контроль інформаційного поля та заходів з його убезпечення
превентивний характер проведення заходів інформаційної безпеки щодо заходів інших видів безпеки	заходи інформаційної безпеки мають носити переважно попереджувальний характер
*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

Закінчення табл. 2.1

Принцип	Стисла характеристика
*ситуативність та адаптивність**	швидке корегування стратегій захисту інформації залежно від ситуації
*інтегрованість**	управління корпоративною інформаційною безпекою має інтегруватися в загальну систему управління
*ризик-орієнтованість**	управління корпоративною інформаційною безпекою має бути повністю узгоджена та гармонізована з системою ризик-менеджменту на підприємстві

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

** запропоновано автором*

Наступним 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 у економіці був створений Л. Гурвіцем, Р. Майєрсоном та Е. Маскіном, за що у 2007 році вони отримали Нобелівську премію з економіки за «видатний вклад 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 в центр; центр отримує всю інформацію і розраховує майбутній результат; центр оголошує результат. Таким чином, було доведено можливість і необхідність механістичного підходу до управління економічними системами.

Словник-довідник під редакцією С. Мочерного надає 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].

В. 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. Пономаренко, О. Ястремська, В. Луцковський та ін. визначають його як сукупність форм, структур, методів та засобів управління, які 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. У 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), механізм 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. Разом із цим 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], дозволив нам таким чином представити механізм формування корпоративної інформаційної безпеки (див. табл. 2.2).

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

Таблиця 2.2

Елементи механізму формування корпоративної інформаційної безпеки

Елемент	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; ІТ-служба; Юридична служба; Топ-менеджери; відповідальні за процеси та центри фінансової відповідальності; окремі особи, що мають доступ до конфіденційної інформації
Мета	Забезпечення реалізації економічних інтересів підприємства шляхом захисту корпоративної інформації
Завдання	Забезпечення цілісності, конфіденційності 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; - контроль 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;

Закінчення табл. 2.2

Елемент	Стисла характеристика
Методи впливу (*продовж.*)	*Економічні (продовж.)*: - метод експертних оцінок; - метод дисконтованого грошового потоку; - метод індексу дохідності; - метод чистої приведеної вартості; - сценарний підхід; - метод імітаційного моделювання; - метод нечітких множин; - метод Ісікави; -метод генетичних алгоритмів
	Організаційно-правові: - моделювання бізнес-процесів; - комплаєнс; - формування регламентів та положень
	Технічні: *-методи моделювання інформаційної 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 [151]

Зміст окремих економічних методів широко висвітлюється в літературі, тому окреслимо лише можливу сферу їх застосування в процесі управління корпоративною інформаційною безпекою в контексті реалізації основних функцій (табл. 2.3).

Таблиця 2.3

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

Джерело: розроблено автором [149, 151]

Організаційно-правові методи включають в себе моделювання бізнес-процесів, у 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 [44] про те, що класифікація самих методів на структурні та об'єктні є доволі умовною, оскільки найбільш розвинуті методи використовують елементи обох підходів.

Серед найбільш поширених методів моделювання бізнес-процесів можна виокремити: метод функціонального моделювання SADT (IDEF0); метод моделювання процесів IDEF3; моделювання потоків даних DFD; метод ARIS; метод Ericsson-Penker; метод технології Rational Unified Process [44] (див. табл. 2.4).

Таблиця 2.4

Найбільш поширені методи моделювання бізнес-процесів підприємства

Метод	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, використовується для моделювання послідовності виконання дій і їх взаємозалежностей у межах процесу. Метод отримав визнання серед системних аналітиків як доповнення до методу функціонального моделювання IDEF0 Основою моделі IDEF3 є 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 відображається 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 у вихідні і виявлення зв'язків між цими процесами

Закінчення табл. 2.4

Метод	Коротка характеристика
ARIS (Architecture of Integrated Information System)	Комплекс засобів аналізу і моделювання діяльності підприємства. Його методичну основу складає 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 методу Ericsson-Penker створили свій профіль UML для моделювання бізнес-процесів – Ericsson-Penker Business Extensions, увівши набір стереотипів, які описують основні категорії бізнес-моделі: процеси, ресурси, правила і цілі діяльності підприємства
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); моделі бізнес-аналізу (Business Analysis Model) Модель бізнес-процесів представляє собою розширення моделі варіантів використання (Use Case) UML шляхом введення набору стереотипів – Business Actor (стереотип діючої особи) та Business Use Case (стереотип варіанта використання). Діючими особами можуть бути акціонери, замовники, постачальники, партнери, потенційні клієнти, місцеві органи влади, зовнішні системи, співробітники тих підрозділів організації, діяльність яких не враховується в 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 [45–57]

Моделювання бізнес-процесів є основою для їх оптимізації, оцінювання вартості, удосконалення бізнес-моделі, зокрема в частині формування корпоративної інформаційної безпеки.

Важливе місце в системі захисту корпоративної інформації посідає розроблення та запровадження різноманітних внутрішніх стандартів та регламентів роботи з інформацією. Насамперед, варто зазначити, що політика підприємства в

сфері інформаційної безпеки має відповідати діючій 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), Доктрина інформаційної безпеки України: Указ Президента України від 25.02.2017 р. № 47/2017, Стратегію національної безпеки і оборони України. Таким чином, внутрішні регламенти та стандарти не повинні вступати в протиріччя з діючими нормами вищезазначених нормативних актів.

Крім того, серед зовнішніх регламентних документів варто відзначити доцільність застосування стандартів якості у сфері захисту інформації, які носять рекомендаційний характер, проте можуть бути досить корисними в розробці і 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 які посилається ISO/IEC 17799:2005.

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

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

Термін «комплаєнс» – відносно новий у діловому середовищі України та на теперішній час використовується в основному в фінансово-банківській сфері. У 2005 р. Базельський комітет з банківського нагляду опубліковано документ «Дотримання законів, правил і рішень регулюючих органів і організація цієї діяльності в банках» (Compliance and the compliance function in banks) [58]. На підставі цього документа 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 області бухгалтерського обліку та аудиту), а з іншого – закони України не вимагають від підприємств створювати внутрішні системи контролю і програми виконання встановлених правил. Тому за великим рахунком запровадження комплаєнсу є ініціативою підприємства. Зазвичай його впровадження є ініціативою самого підприємства. Його наявність у компанії завжди виступає свідченням високої корпоративної культури, прозорості та інноваційності в системі запровадження інструментів та технологій управління. Водночас варто зазначити, що в сучасній практиці комплаєнс запроваджують не лише кредитно-фінансові установи, а і підприємства інших секторів економіки і ця тенденція посилюється [60–70].

У широкому сенсі під комплаєнсом слід розуміти частину системи управління / контролю в організації, пов’язану з ризиками невідповідності, недотримання вимог законодавства, нормативних документів, правил і стандартів наглядових органів, галузевих асоціацій та саморегулюючих організацій, кодексів поведінки тощо. Такі невідповідності в кінцевому підсумку можуть мати наслідком застосування юридичних санкцій або санкцій регулюючих органів, фінансові або репутаційні (іміджеві) втрати як результат невідповідності законам, загальноприйнятим правилам і стандартам [71].

Здебільшого комплаєнс фокусується на дотриманні належних стандартів поведінки на ринку, управління конфліктами інтересів, справедливе ставлення до клієнтів і забезпечення сумлінного підходу при консультуванні клієнтів. Проте в

сучасній практиці до сфери комплаєнс відносяться також специфічні області, серед яких належне 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 та передачі інформації, порушення національного законодавства у 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», застосований на дотриманні норми, яка передбачає мінімальний рівень організації комплаєнсу в банку – виконується тільки те, що імперативно вимагає закон.

2. «Risk based approach», заснований на аналізі ризиків. Саме такий підхід рекомендується іноземним банкам як національними регуляторами, так і міжнародними структурами (Compliance and the compliance function in banks), є домінуючим в Європі. В Україні він також рекомендований для впровадження центральним банком, однак, на жаль, в українській банківській практиці є менш поширеним, ніж підхід, заснований на нормі [71].

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

Третьою групою методів формування інформаційної безпеки є технічні, у межах яких варто виокремити методи моделювання корпоративної безпеки та автоматизовані системи управління інформаційними ризиками. Стисла характеристика цих методів наводиться в табл. 2.5 та 2.6.

Таблиця 2.5

Характеристика методів моделювання корпоративної інформаційної безпеки

Метод	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; має прив'язку до рівня інтеграції, на якому знаходиться об'єкт і суб'єкт
Модель Clark-Wilson (CW)	у повній мірі 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 дозволяє запобігти або виправити більшість нелегальних дій, що здійснюються зсередини 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 підтримання 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 допустити багато помилок при адмініструванні
Модель Адепт-50	модель безпеки, 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 методик загроз, для приватного сектору користувачів та уряду; передбачає використання матриці, яка формується на основі використання показників: ступінь доступу, система реалізації програмних додатків, наполегливість, ескалація привілеїв, ухилення від захисту, доступ до довірених даних, відкриття, додатків дії, збір, управління та адміністрування, ексфільтрація, вплив
«Модель алмазу» (Diamond Model)	базується на аналізі 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 конструкцій вищого рівня, таких як пов'язання подій разом у потоки діяльності та подальше злиття подій потоків у групи інформаційної активності. 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

Закінчення табл. 2.5

Метод	Коротка характеристика
«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, інші механізми все ще можуть забезпечити необхідний рівень безпечності для захисту системи. Включає безліч компонентів: персонал (людей), технологію, операційну систему, моніторинг та різні аспекти захисту як ключові компоненти забезпечення інформаційного захисту. Ці організаційні шари важко перевести в конкретні технологічні шари захисту, і вони залишають такі сфери, як моніторинг безпеки та показники

Джерело: систематизовано автором за [72–82]

Таблиця 2.6

Характеристика автоматизованих методів управління інформаційними ризиками

Метод	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 по контрзаходах і володіє універсальністю і адаптованістю під профілі різних організацій. Розроблено програмні продукти, що реалізують цю методику	Вимагає спеціальної підготовки і високої кваліфікації аудитора, процес є досить трудомістким і може обраховуватись місяцями безперервної роботи аудитора, не дозволяє створювати власні шаблони звітів або модифікувати існуючі; припускає використання лише методів зниження рівня ризиків ІБ, такі способи управління ризиками, як «уникнення» або «прийняття», не розглядаються
CORAS	Дозволяє створювати звіти про результати аналізу шляхом моделювання ризику. Інформаційні системи розглянуто як складні комплекси з урахуванням людського фактора, а не тільки на основі використовуваних технологій	Програмний продукт, що реалізує цю методологію, є безкоштовним і не потребує значних ресурсів для установки; методика проста у використанні і не вимагає спеціальних знань	Не передбачена періодичність проведення оцінювання ризиків і оновлення їх величин; не дозволяє оцінити ефективність інвестицій у заходи безпеки та знайти баланс між необхідними заходами

Закінчення табл. 2.6

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 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
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 нанесенню шкоди підприємству шляхом порушення корпоративної інформаційної безпеки.

2.2. Методологічні засади формування корпоративної політики інформаційної безпеки

У сучасних умовах розвитку корпорацій ландшафт питань забезпечення інформаційної безпеки корпорацій перемістився з вузькоспрямованого технічного питання до стратегічного фундаментального завдання перспективного розвитку бізнесу. Головною метою корпоративної політики інформаційної безпеки є забезпечення безперервності бізнесу та зменшення збитків шляхом запобігання та нивилювання негативного прояву інцидентів безпеки.

Отже, досягенення головної мети корпоративної політики інформаційної безпеки обумовлює об'єктивну необхідність формування безпечних корпоративних інформаційних систем та зміцнення національної безпеки країни за рахунок впровадження системи захисту корпроративної інформації до системи корпоративного управління. Визначаючи систему захисту корпоративної інформації, як одну з основних складових системи корпоративного управління, доцільно зазначити, що вона є інструментом забезпечення стійкого, динамічного та збалансованого розвитку вітчизняних корпорацій.

Політика інформаційної безпеки корпорацій є елементом корпоративного управління і випливає із 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 досягнуто шляхом конвергенції корпоративної політики інформаційної безпеки з іншими бізнес-політиками політики організації в межах циклу стратегічного управління [147].

Питання формування ефективної корпоративної політики інформаційної безпеки в різних її аспектах досліджували багато вітчизняних та зарубіжних науковців. Але ж не зважаючи на значну кількість праць, слід констатувати факт

відсутності уніфікованого термінологічного узагальнення політики інформаційної безпеки та механізмів її реалізації, що активізує дискусії науковців стосовно систематизації політики інформаційної безпеки та методичного інструментарію її впровадження як на рівні держави, так і на рівні корпорацій [147].

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 [89].

Відповідно до Закон 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» [90]. Отже, інформаційна система інтегрує інформаційні ресурси про особливості стану, напрями 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 слід зазначити, що більшість науковців розглядають її тільки через склад її компонентів, без виділення в окрему категорію зазначеного терміна [147].

В. Домарєв та О. Гордієнко характеризують політику інформаційної безпеки як набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз [91].

І. Анікін, В. Глова та А. Нігматулліна визначають політику інформаційної безпеки як набір норм, правил і практичних рекомендацій, що регламентують процес обробки інформації, виконання яких забезпечує захист від заданої множини загроз [92].

На думку А. Страхарчука і В. Страхарчука, політика інформаційної безпеки – це набір законів, правил і практичних рекомендацій, на базі яких здійснюється керування, захист і розподіл критичної інформації в системі. [93].

Є. Бодюл пропонує під політикою інформаційної безпеки розуміти науково обґрунтовану систему поглядів на визначення основних напрямів, умов і порядку практичного вирішення задач інформаційного захисту організацій та установ від протиправних дій [94].

За визначенням Ю. Хохлачової, політика інформаційної безпеки – це сукупність керівних принципів, правил, процедур фактичних прийомів, якими об’єкт керується у своїй діяльності [95].

М. Бондаренко, О. Потій, І. Горбенко та ін. характеризують політику інформаційної безпеки як сукупність правових і морально-етичних норм, правил, адміністративних, організаційних заходів і технічних, програмних і криптографічних засобів, направлених на захист інформаційної інфраструктури організації від випадкового і навмисного втручання в процес її функціонування [96].

На думку А. Нашинець-Наумової, політика інформаційної безпеки – це сукупність нормативних документів, які встановлюють порядок забезпечення безпеки інформації на конкретному підприємстві, а також вимоги з підтримки цього порядку [97].

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

З. Валіулліна та О. Черевко визначають, що в умовах сучасних глобалізаційних процесів інформаційна безпека корпорацій є пріоритетним напрямом соціально-економічного розвитку держави. При цьому автор обґрунтовує необхідність впровадження в діяльність корпорацій заходів законодавчого, економічного; програмно-технічного та адміністративно-управлінського характеру, комплексний влив яких дозволить створити

інформаційно безпечний корпоративний простір [98]. При цьому формування системи комплексного захисту інформаційних ресурсів повинна бути забезпечена, насамперед, за рахунок системи створення механізмів власного забезпечення, спрямованих на її реалізацію не тільки в повсякденних умовах, але і в ситуаціях, що потребують швидкої адаптації до нових викликів сучасності [99].

Погоджуючись із вищезазначеними думками, А. Нашинець-Наумова визначає доцільність та необхідність впровадження системи перманентних заходів також для реалізації систематичного моніторингу стану захисту корпоративної інформації та формування оптимальної моделі функціонування системи її забезпечення шляхом створення необхідних організаційно-економічних та правових механізмів формування розвитку і забезпечення ефективного використання інформаційних ресурсів корпорації [97, С. 60].

О. Жабинець при розробці політики інформаційної безпеки визначає доцільність прийняття заходів, спрямованих на захист активів компаній від будь-якої зміни, розкриття чи знищення, а також із метою забезпечення конфіденційності, цілісності та доступності інформації. [100].

Так, М. Шилов та І. Жевелєва акцентують увагу на необхідності впровадження в діяльність корпорацій комплексу заходів та засобів контролю, які б дозволили здійснювати систематичне управління безпекою та ризиками [101].

В. Бакай та В. Зима обґрунтовують думку про те, що в умовах розповсюдження глобалізаціних процесів саме ефективна політика інформаційної безпеки є пріоритетним механізмом забезпечення системи економічної безпеки підприємства. Автори наголошують на тому, що саме корпоративна політика 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» [102].

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

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

Тому зміну парадигми корпоративної політики інформаційної безпеки для зміни її вектора від внутрішньо-орієнтованого захисту інформації до стратегічного погляду, який враховує міжорганізаційний рівень, є об'єктивно необхідним та доцільним. Зміна 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 стейкхолдерів, які приймають рішення та відповідальні за забезпечення ефективної політики інформаційної безпеки організації на стратегічному рівні [147].

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 передачі інформації на міжорганізаційному рівні [103].

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» [104]. Автори наголошують на необхідності узгодження оцінки зовнішніх інформаційних загроз із фінансово обґрунтованим комплексом внутрішніх контрзаходів, включаючи необхідні допоміжні політики та процедури. Отже, політика інформаційної безпеки розглядається як ключовий інструмент впливу на зовнішнє бізнес-середовище організації шляхом ретельного відбору засобів внутрішнього контролю [147].

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» [105]. Дослідження корпоративної політики інформаційної безпеки цими авторами доводить її міцний зв'язок з організаційним стратегічним планом корпорації. Саме стратегічна політика інформаційної безпеки дозволить корпораціям запобігти існуючих та потенційних загроз інформаційним ресурсам у час, просторі і в процесі прийняття управлінських рішень [147].

К. Хонг та ін. стверджують, що саме врахування стратегічного підходу до формування корпоративної політики інформаційної безпеки дозволяє розширити її функціонал та зорієнтуватися на управлінні ризиками та надзвичайними ситуаціями [106].

У. Флорес та інші зарубіжні вчені розглядають корпоративну політику інформаційної безпеки як динамічний процес забезпечення захисту корпоративної інформації, який реалізується зацікавленими особами [107].

Отже, корпоративна інформаційна політика інформаційної безпеки є ключовим елементом загальної бізнес-стратегії корпорації, який включає адекватну підтримку її стратегічного розвитку, згуртованість інформаційних систем і бізнесу та координацію зусиль з інформаційної безпеки [147].

Функціонування сучасних корпоративних структур в умовах динамічного бізнес-середовища змушує перманентно враховувати та приймати нові технології. Саме технологічний вплив обумовлює необхідність формування стратегічного вектора розвитку корпорацій з урахуванням ключових викликів, що обумовлюють необхідність зміни напрямів їх діяльності (табл. 2.7).

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 [108].

Таблиця 2.7

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 із безпекою
	Зростання безпосереднього впливу кібератак на бізнес, що вимагає 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

Така тенденція 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 вимагає розробку та впровадження відповідних регулюючих механізмів [147].

По-друге, через всебічне впровадження інформаційних технологій у бізнес інциденти з інформаційною безпекою, що викликають порушення стійкості функціонування корпорацій, безпосередньо впливають на прогресивність розвитку бізнесу корпорацій [109]. Кібератаки обмежують, насамперед, продуктивність діяльності корпорацій, їх інноваційні можливості та обмежують конкурентні переваги. Це призводить до зменшення кола бізнес-партнерів, фінансових та репутаційних збитків [110].

Крім того, зарубіжні науковці виявили кореляцію між інцидентами інформаційної безпеки та ефективністю діяльності корпорацій [111]. Факт виникнення порушення інформаційної безпеки негативно впливає на ринкову вартість, коливається від 1 до 2,1 відсотка [112]. Зростання впливу кібератак на безпеку та ринкову вартість корпорацій змушують керівників корпорацій здійснювати постійний пошук альтернативних механізмів їх мінімізації.

По-третє, цифровізація вимагає 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 їх безпеки та конфіденційності [113]. Запорукою збереження та відтворення потенціалу цільової аудиторії корпорацій є формування нормативно-правової бази, що регламентує та забезпечує права всіх стейкхолдерів бізнесу, таким чином, ще більше стимулюють ці очікування. Крім того, слід зазначити, що в умовах сучасного цифрового середовища корпорації функціонують як цифровий ланцюг поставок, а не як окремі бізнес-одиниці [114]. Такий механізм їх функціонування обумовлює виникнення ризиків інформаційної безпеки за межами корпорацій, розширюючи завдання щодо розроблення відповідного методичного інструментарію формування ефективної корпоративної політики інформаційної безпеки, яка має бути зосереджена на створені прозорого міжорганізаційного захисту інтересів усіх зацікавлених осіб.

Стратегічні зміни, зумовлені впровадженням інформаційних технологій та формуванням єдиного цифрового корпоративного бізнесу-простору, виявили потребу в оновленому підході до розробки методичних засад систематизації видів

корпоративних політик інформаційної безпеки, які б ураховували 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 ступеню 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 [115].

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

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

– зв'язністю всіх структурних підрозділів корпорацій: економічна, механічна, енергетична, інформаційна залежність між ними;

– структурністю: якісно визначена та відносно стійка впорядкованість між підрозділами та відносинами корпорацій;

– взаємодією: між елементами всередині корпоративної системи та із зовнішнім середовищем;

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

– складністю: виявляється у взаємному неоднозначному впливі різноманітних факторів.

Корпоративні структури складаються із 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 в табл. 2.8.

Таблиця 2.8

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 із 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 відносяться до класу складних динамічних систем.

Отже, на сьогод важливим для корпоративних структур є розробка такої стратегії інформаційної безпеки, яка забезпечувала б гнучкість корпоративних структур в умовах економічної, соціальної та політичної динаміки і сприяла б можливості прийняття ефективних рішень на основі адаптивних підходів в управлінні корпоративними структурами.

Звідси 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 [116].

Тепер корпораціям доводиться не лише боротися з бізнес-середовищем, яке характеризується конкуренцією, динамічністю за своєю природою та економічними проблемами; вони також повинні боротися з ландшафтом інформаційної безпеки, яка рівною мірою динамічна, швидко розвивається та характеризується дуже складними та витонченими загрозами [117].

Сталий корпоративний розвиток може бути досягнутий лише за допомогою прагматичної стратегії, яка включає стійкість у своїй основі разом із стійкими бізнес-моделями, а для збереження конкурентоспроможності динамічні можливості є ключовими факторами, що сприяють підтримці конкурентних переваг у бізнес-ландшафті, що постійно змінюється [118].

Теорія динамічних можливостей, висунута Д. Тіс [119], є інструментальною, але вона не розширює взаємозв’язок динамічних можливостей із 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 інформаційної 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 і функції розподілу ресурсів.

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

Головним джерелом потенційного ефекту гнучкості корпоративних структур є сфера споживання її продукції. Саме в цій сфері 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 усі складові соціально-економічного ефекту у сфері виробництва та споживання продукції гнучких корпоративних структур. Тим не менш, саме ці складові найбільш інтенсивно впливають на підвищення соціально-економічної ефективності діяльності корпорацій. Своєчасне та якісне задоволення потреб суспільства часом настільки важливе з погляду на необхідність вирішення суспільно-політичних завдань, що саме ці причини спонукають до прискореного впровадження в промисловість гнучких корпоративних структур. Задоволення таких потреб, безумовно, у переважній більшості випадків принесе й економічний ефект, але не прямий, а непрямий, розрахувати який за допомогою діючих методик виявляється часом неможливим.

Ефект гнучких корпоративних систем, що включає всі елементи, слід визначити як «стратегічний» ефект гнучкого реагування корпоративної політики інформаційної безпеки на зміну потреб суспільства» [148].

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 спричинити. Це становище випливає з відомого закону необхідної різноманітності. Тут слід ураховувати принаймні дві найважливіші обставини [148].

По-перше, щодо величини витрат, пов’язаних із 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 [148].

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 слід ураховувати й ефект цілісності (принцип емерджентності), що виражає таку важливу властивість системи: чим більша система і чим більша різниця в розмірах між частиною та цілим, тим частіше ймовірність того, що властивості цілого можуть значно відрізнятися від властивостей частин [120].

Це означає, що чим менший об’єкт, прийнятий як модуль гнучкої корпоративної політики інформаційної безпеки, тим менш імовірне 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 їх інформаційної безпеки, лінії та інші підрозділи, які не можуть забезпечити виникнення передумов для отримання ефекту, достатнього для окупності капітальних вкладень. У зв’язку з цим робиться висновок (іноді необґрунтований) про потенційну неможливість створення високоефективних гнучких інструментів реалізації корпоративної політики інформаційної безпеки або необхідність розроблення спеціальних методик визначення їх 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, що забезпечують її збереження, тобто системоутворюючих, системозберігаючих факторів. Що стосується гнучкої корпоративної політики інформаційної безпеки, то подібним системо - утворюючим чинником є значимість елементів системи з точки їх зору впливу на ступінь гнучкості всієї системи.

У кожній корпоративній системі можуть бути знайдені провідні елементи, від яких залежить визначальною мірою 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, він має стати, насамперед, основою 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 омертвленими.

Таким чином, для кожного модуля гнучкої корпоративної політики інформаційної безпеки або їх сукупності має бути визначена оптимальна, з точки зору співвідношення витрат та потенційного стратегічного ефекту, прогресивність корпоративної системи, що забезпечує високий рівень ефективності задоволення потреб суспільства [148].

Зміна потреб суспільства відбивається на прогресивності корпоративної політики інформаційної безпеки. У разі збільшення темпів зміни потреб, що виражаються у збільшенні темпів оновлення продукції, прогресивність корпоративної політики інформаційної безпеки має посилюватись. Інакше корпорація змушена перебувати в стані постійного переозброєння чи реконструкції. Посилення прогресивності неминуче пов’язано зі зростанням ступеню виробничої різноманітності продукції, що випускається корпорацією [121].

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, $I_{np}(t_h, t_k)$, де t_h, t_k – відповідно початок і кінець проаналізованого періоду. Економічною характеристикою задоволення потреб, що змінюються, за той же період може бути прийнятий індекс зміни витрат, пов'язаних із функціонуванням корпоративної політики інформаційної безпеки $I_n(t_h, t_k)$. Тоді кількісною характеристикою гнучкості корпоративної політики інформаційної безпеки може бути показник:

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

У разі збільшення ступеня гнучкості системи за проаналізований період усе більше відрізнятиметься від одиниці (у більшу сторону). Це означає, що чим вище 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 $G(t_h, t_k) > 1$, 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.

Для вимірювання ступеня різноманіття напрямів корпоративної політики інформаційної безпеки в найпростішому випадку, як було показано вище, може бути використаний коефіцієнт асоціації. Тоді значення $I_{np}(t_h, t_k)$ визначаються 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 слід особливо обумовити їх склад. Це зумовлено важливими положеннями визначення потенційного стратегічного ефекту гнучкого реагування на потреби суспільства, викладеними вище.

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

У табл. 2.8 було розглянуто характеристику елементів корпоративних структур як сукупності певним чином технічних, технологічних, кадрових, інформаційних та організаційно-економічних ресурсів.

Виходячи із цього, а також зважаючи на склад потенційного стратегічного ефекту гнучкого реагування, визначимо узагальнений склад витрат, здатних спричинити виникнення потенційного стратегічного ефекту гнучкого реагування на зміну потреб суспільства (табл. 2.9).

Дані, наведені в табл. 2.9, можуть бути деталізовані з необхідною для тих чи інших цілей аналізу ступенем конкретизації. Для розрахунку кожної із складових одноразових чи поточних витрат розробляються відповідні моделі.

Результати цих розрахунків ми можемо окреслити за допомогою такого виразу:

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

де C_{it} – поточні витрати на підтримку в актуальному стані i-ої умови функціонування корпоративної політики інформаційної безпеки в 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 в період (t_h, t_k).

Таблиця 2.9

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

Напрями витрат	
Одночасні	Поточні
Формування технічних ресурсів корпоративної політики інформаційної безпеки – K_1	Підтримка технічних ресурсів корпоративної політики інформаційної безпеки в актуальному стані – C^1
Формування технологічних ресурсів корпоративної політики інформаційної безпеки – K_2	Підтримка технологічних ресурсів корпоративної політики інформаційної безпеки в актуальному стані – C^2
Формування кадрового потенціалу корпоративної політики інформаційної безпеки – K_3	Підтримка в актуальному стані кадрового потенціалу корпоративної політики інформаційної безпеки – C^3
Формування інформаційних ресурсів корпоративної політики інформаційної безпеки – K_4	Підтримка 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

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 в першому році аналізованого періоду.

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

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

Таким чином, здатність корпоративної політики інформаційної безпеки до гнучкого реагування змін 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 висловлюючись, 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, під ефективністю корпоративної політики інформаційної безпеки слід розуміти досягнення заданих системі цілей із 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 та якісно задовольняти потреби корпорації, що змінюються. Однак ступінь різноманітності потреб, що задовольняються має бути визначена в певних межах. Тоді як основний чинник прогресивності корпоративна політика інформаційної безпеки слід розглядати сталість і повторюваність ступеня розмаїття її напрямів та інструментів.

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

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

Специфіка потреб суспільства, що розглядаються в динаміці, диктує необхідність використання тих чи інших видів відтворюваних та не відтворюваних ресурсів, залучення в діяльність корпорацій нових ресурсів. З іншого боку обмеженість ресурсів, можливості їх поповнення та регенерації коригують потреби суспільства, що впливають на обсяг цих потреб. Урахування зазначених факторів дозволяє формувати потенційні обсяги виробництва продукції корпорації, які в сукупності з вимогами природоохоронних обмежень та особливостями діяльності корпорації викликають до життя ті чи інші варіанти 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 розширення напрямів діяльності

корпоративних структур створюють передумови для галузевої їх 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 із суспільними потребами та завданнями соціально-економічного розвитку країни. Ці зв’язки стимулюють чи, навпаки, стримують розвиток тих чи інших потреб. Надмірно мала прогресивність корпоративної політики інформаційної безпеки має консервативність по відношенню до процесу оновлення діяльності корпорацій. У той же час прогресивність корпоративної політики інформаційної безпеки стимулює прискорений розвиток потреб суспільства, створює сприятливі передумови 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 слід віднести: технічні, технологічні, кадрові, інформаційні і, навіть, організаційно-економічні ресурси. 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.

Принципово основними етапами вибору кращої прогресивності корпоративної політики інформаційної безпеки слід 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 дозволяє системі досягти заданих цілей із максимальним ефектом в умовах обмежень засобів розширення сукупності ресурсів, що становлять виробничу систему.

Завдання першого етапу може бути вирішено 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 із них, реалізація яких не викликає виникнення потенційно неприпустимих із точки зору встановлених суспільством нормативів негативних соціально-екологічних наслідків та забезпечує якісне та 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.

У дод. А представлено схему оптимізації прогресивності 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 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.

Розглянута схема пошуку кращої прогресивності корпоративної політики інформаційної безпеки виходить із можливості формування множини. Звідси слід зазначити, що саме це завдання є найскладнішим. Складність полягає не так у тому, щоб знайти вид параметрів і значень, адекватно відобразити стан того чи іншого елемента корпоративної політики інформаційної безпеки, як у можливості ув’язати ці параметри та поєднати їх із 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 змінливих потреб ринку;

– прогнозування можливостей оснащення процесу реалізації корпоративної політики інформаційної безпеки технічно та програмносумісними засобами виробництва та 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.

2.3. Систематизація показників оцінки економічної ефективності управління корпоративною інформаційною безпекою

Управління корпоративною інформаційною безпекою є надзвичайно складним процесом з декількох причин: по-перше, підприємства функціонують в умовах постійно зростаючих загроз (як кількості, так і ступеня агресивності), що потребує постійного вдосконалення системи управління, креативності, інноваційності та випереджального характеру заходів; по-друге, реалізація заходів із 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 із цим постає актуальне питання, яким чином виміряти економічну ефективність управління корпоративною інформаційною безпекою.

Процес вимірювання економічної ефективності управління корпоративною інформаційною безпекою натикається на ряд 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 носять різноманітний характер та з т. з. 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 досягатися за рахунок еволюційних змін процесів, які не носять дуже витратного характеру, але сам ефект від таких удосконалень складно виокремити. До того ж він не знаходить відображення в окремих документах бухгалтерського обліку та звітності підприємства. Часто це потребує специфічних налаштувань у системі збору інформації та введення додаткових звітів у системі управлінського обліку.

Не дивлячись на ці перешкоди, науковці не припиняють спроб сформулювати підходи до оцінювання такої ефективності. Зазначеній проблемі присвячені праці [122–146]. Вивчення джерел з відповідної тематики дозволило нам виокремити три принципові підходи до обґрунтування показників оцінювання економічної ефективності управління корпоративною інформаційною безпекою підприємства:

– перший підхід спрямовано на оцінку одного показника ефективності корпоративної інформаційної безпеки;

– другий підхід 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 роботах А. Бєгуна [122–125].

Так, автор [125] під економічною ефективністю безпеки вважає відношення відвернутого збитку до витрат на її забезпечення. Але, на думку автора, відвернутий збиток – це не єдиний результат діяльності системи безпеки, з огляду на те, що 100 % захисту неможливо досягти, а тому існує залишковий ризик реалізації загрози, який прогнозує можливість збитку – від'ємного результату. Таким чином, ефектом дій із забезпечення ІБ є, на думку А. Бєгуна відвернутий та понесений збиток у вартісному вигляді. Виходячи з цього 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.

Ураховуючи формулу $U_2 = U_{2.1} + U_{2.2}$ ($U_{2.1}$ – прямі збитки, $U_{2.2}$ – непрямі збитки), розрахунок E має здійснюватися за такою формулою:

$$E = (U_1 - U_2) / (Z_1 + Z_2 + Z_3), \qquad (2.7)$$

де Z_1 – витрати на формування політики інформаційної безпеки;

Z_2 – витрати на відповідність політики інформаційної безпеки;

Z_3 – витрати, які пов'язані з наслідками порушення політики інформаційної безпеки.

Автор пропонує враховувати страхування залишкового інформаційного ризику: величина страхового внеску (s) збільшить величину витрат (Z), а страхові виплати у випадку настання страхової події (S) зменшать розмір збитку(U):

$$E =(U_1 - U_2 + S) / (Z_0 + s) \qquad (2.8)$$

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 автор 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 забезпеченні інформаційної безпеки. Для цього пропонується така формула:

$$E^* = C / Z_0 \quad (2.10)$$

Зазначимо, що автор 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» [125].

У цілому, погоджуючись з окремими ідеями представленого підходу, зокрема: необхідністю оцінювання відверненого збитку, наявності залишкового інформаційного ризику, співвіднесення цих показників з понесеними витратами на інформаційну безпеку, необхідності підтримання рентабельної діяльності підприємства, на наш погляд, 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 оцінка здійснюється за результатами року і до складу витрат на інформаційну безпеку автор відносить і інвестиційні і 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 і отриманий ефект у наступні роки буде порівняно із заниженими витратами, що суттєво знижує об'єктивність оцінки.

По-третє, методика носить 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 рядом авторів пропонується застосовувати в якості критеріїв ефективності системи організації інформаційної безпеки показник сукупної вартості володіння (англ. *Total Cost of Ownership, TCO*) [126–132].

Сукупна вартість володіння або вартість життєвого циклу – 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 в 1987 р. компанією «Gartner Group» з розробки рішень у сфері інформаційних технологій із метою точного розрахунку фінансових витрат, пов'язаних із володінням і експлуатацією комп'ютерних мереж [150].

У 1994 р. компанія «Interpose» здійснила вдосконалення моделі, що перетворило її в 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 в 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 попередження інцидентів 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; вивід з експлуатації [150].

При цьому різні науковці обґрунтовують власні підходи щодо уточнення складу витрат, які включаються до сукупної вартості володіння. Такі методики представлені в роботах А. Рибидайла зі співавторами, В. Луговця та Л. Гальчинського Ознайомлення з методиками цих авторів дозволило 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 і 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 [133–144].

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*).

Зазначений підхід характеризується методологічною коректністю, оскільки дотримується базових принципів інвестиційного аналізу. Проте, на наш погляд, його не можна вважати комплексним. Він ураховує 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 Велігури А .В. [143], Журавля М. Ю. [144] та багатьох інших. Так, Дячков Д. В. на основі розвитку роботи Велігури А. В. пропонує для оцінювання інформаційної безпеки застосовувати показники, що наведені в табл. 2.10.

Зазначений підхід, на наш погляд, можна охарактеризувати таким чином

По-перше, носить 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.

Таблиця 2.10

Показники оцінки корпоративної інформаційної безпеки

Показник	Стисла 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
Коефіцієнт фінансування технічної захищеності інформації	Співвідношення вартості технічного забезпечення 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 фінансового напряму 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

Продовження табл. 2.10

Показник	Стисла характеристика
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
Оцінка інформаційної надійності персоналу	
Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства	Співвідношення чисельності працівників до загальної чисельності працівників, що мають доступ до комерційної таємниці (баз даних, банків даних тощо), які мають доступ до комерційної таємниці (баз даних, банків даних тощо), що працюють на підприємстві більше одного року
Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства	Співвідношення чисельності працівників, звільнених за причиною 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, що 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, який 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. 2.10

Показник	Стисла 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 компетентостей 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: [145].

По-друге, методика певною мірою переобтяжена за кількістю показників, доцільність оцінювання окремих із них, на наш погляд, є досить дискусійною з точки зору їх значимості та відповідності принципу «розумної доцільності». Так, наприклад, групу показників, що характеризує 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 носити досить суб'єктивний характер, а тому в 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 в 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 не зрозуміло як оцінити «здатність системи управління інформаційною безпекою швидко адаптувати організаційну побудову до зовнішніх та внутрішніх потреб».

По-третє, методика не містить класичних показників ефективності. Важливим принципом забезпечення інформаційної безпеки є її економічна ефективність, тому, на наш погляд, система показників оцінювання КІБ має включати такі індикатори.

По-четверте, невизначеність критеріїв оцінювання ускладнює інтерпретацію результатів аналізу, а відсутність інтегрального або узагальнюючого показника унеможливлює ідентифікацію рівня інформаційної безпеки підприємства загалом.

Таким чином, вивчення сучасних підходів до оцінювання ефективності КІБ дозволило, насамперед, зробити висновок про складність застосування єдиної методики з описаних вище для формування вичерпного висновку щодо ефективності КІБ, а також 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 узагальнюючого показника ефективності КІБ.

Виходячи з 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 запровадження 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), оскільки ефект від заходів захисту інформації є результатом комплексного використання ресурсів, який досить складно розмежувати 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 різними механізмами фінансування витрат на такі заходи.

3. Принцип ієрархічності, який передбачає виокремлення основних та допоміжних показників ефективності, що дозволяє 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, на що вказує 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, що 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. 2.11).

Важливим аспектом в оцінюванні стратегічної економічної ефективності КІБ є оцінка основних абсолютних показників, що виступають 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.

Таблиця 2.11

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 (↑)
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 вдосконалення інформаційних процесів (*Td*)* (↑)

Джерело: розвинено та доповнено автором за [135–137, 143, 145]

** запропоновано автором*

Фактичним кінцевим результатом упровадження 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, відповідно до і після впровадження засобів і заходів по ІБ [146].

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 [141].

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 варіювати від мінімального (*min*) до максимального (*max*) значення. Подібний крок виконується як до, так і після реалізації заходів щодо посилення ІБ ОБІ [146].

Крок 3. Застосовуючи попередньо обраний закон розподілу, створити модель величини втрат (до і після впровадження заходів і засобів ІБ) [146].

Крок 4. Розрахувати сумарне значення попереджуваної шкоди від кібератак на підставі попередніх кроків 1–3 [146].

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 [146].

Для візуалізації результату розрахунку доцільно побудувати гістограму розподілу результуючого значення попереджуваної шкоди від кібератак або гістограму інтегрального відсотка 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 [146].

Таким чином, імовірнісна характеристика попереджуваної шкоди від кібератак може бути прийнята в якості обґрунтованого критерію ефективності заходів, спрямованих на підвищення ІБ ОБІ [146].

Інвестиційні витрати на формування КІБ оцінюються виходячи з методології інвестиційного аналізу і включають витрати на придбання техніки, технологій, транспортування, монтаж, уведення в експлуатацію, розробку.

ТСО крім інвестиційних витрат включає всі поточні витрати на утримання та обслуговування інформаційних систем підприємства.

Отримані на підставі реалізації кроків 1–5 результати можна використовувати 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 такі розробки обходяться дешевше підприємству, а з іншого боку це відображає рівень високих компетентностей задіяного в 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 носять стратегічний характер, оскільки віддача від них не є миттєвою. Тому показник ефективності навчання персоналу, що залучені до процесів формування КІБ ми пропонуємо включити до системи допоміжних вимірників економічної ефективності КІБ стратегічного контуру управління. Крім того, пропонується вимірювати капіталомісткість однієї кібератаки, яка дозволить розуміти порівнянність інвестиційних витрат із потенційними загрозами інформаційній безпеці підприємства.

У межах оперативно-тактичного контуру управління в якості основних показників 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 вважаємо за потрібне оцінювати з огляду на те, що інформаційні процеси пронизують усі напрями діяльності підприємства, забезпечуючи здійснення операційної, фінансової, інвестиційної складової, а вдосконалення інформаційної системи, КІБ має сприяти зростанню ефективності функціонування підприємства в цілому.

В якості допоміжних показників на оперативно-тактичному рівні пропонується оцінювати темпи росту кількості інцидентів витоку конфіденційної інформації, заходів із поліпшення інформаційних процесів та порушення регламентів зберігання та передавання інформації. Не будучи за своєю природою класичними показниками економічної ефективності, вони надають уявлення щодо зміни якості політики КІБ.

Інтерпретація авторських показників, що пропонуються для оцінювання ефективності КІБ в межах стратегічного та оперативно-тактичного контурів управління, представлена в таблиці 2.12.

На основі запропонованих окремих показників 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 включаємо *IP*, коефіцієнт продуктивності навчання персоналу, капіталомісткість кібератаки, продуктивність *IC*, рентабельність *IC*, темп росту кількості порушень регламентів передачі та зберігання інформації, темп зростання кількості інцидентів витоку конфіденційної інформації, темп зростання реалізованих поточних заходів із вдосконалення інформаційних процесів.

Таблиця 2.12

Характеристика показників економічної ефективності корпоративної інформаційної безпеки

Показник	Стисла 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 на річну вартість 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 передачі і зберігання інформації	
Темп зростання кількості інцидентів витоку конфіденційної інформації	
Темп зростання реалізованих поточних заходів із вдосконалення інформаційних процесів	

Джерело: розроблено автором

На другому етапі формується матриця стандартизованих значень показників *X*, тобто матриця **X** трансформується в матрицю **Z**. Це обумовлено тим, що показники можуть мати різну природу і незрівнянні один з одним значення. Елементи матриці **Z** обчислюються за такою формулою:

$$Z_{ij} = \frac{X_{ij} - \overline{X_J}}{\sigma_j} \qquad (2.12)$$

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 являє собою відстань між окремими стандартизованими показниками та точками-еталонами:

$$\mathrm{C}_{i0} = \sqrt{\sum_{j=1}^{n}(Z_{ij} - Z_{0j})^2} \tag{2.15}$$

Отримані значення відстаней безпосередньо використовуються при розрахунку інтегрального показника.

На п’ятому етапі здійснюється розрахунок значення інтегрального показника (d_i):

$$d_i = 1 - \frac{C_{i0}}{C_0} \quad (2.16)$$

$$C_0 = \bar{C}_0 + 2 \times S_0 \quad (2.17)$$

$$\bar{C}_0 = \frac{\sum_{i=1}^{m} C_{i0}}{m} \quad (2.18)$$

$$S_0 = \sqrt{\frac{\sum_{i=1}^{m} (C_{i0} - \bar{C}_0)^2}{m}} \quad (2.19)$$

Крім того, на цьому етапі також відбувається оцінка ступеня прогресивності системи захисту корпоративної інформації, як найважливішої характеристики системи захисту корпоративної інформації, що вказує на залежність збільшення прибутку від впровадження в діяльність корпорацій ефективної системи захисту корпоративної інформації. Методичний підхід до оцінки ступеня прогресивності системи захисту корпоративної інформації та його апробація будуть представлені в п. 4.3.

На шостому етапі формується висновок щодо рівня економічної ефективності КІБ та виявляються основні «слабкі місця» в її забезпеченні. Для цього може бути використаний метод Ісікави, який дозволяє 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.2.3).

Запропонований підхід до оцінювання економічної ефективності КІБ ґрунтується 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.

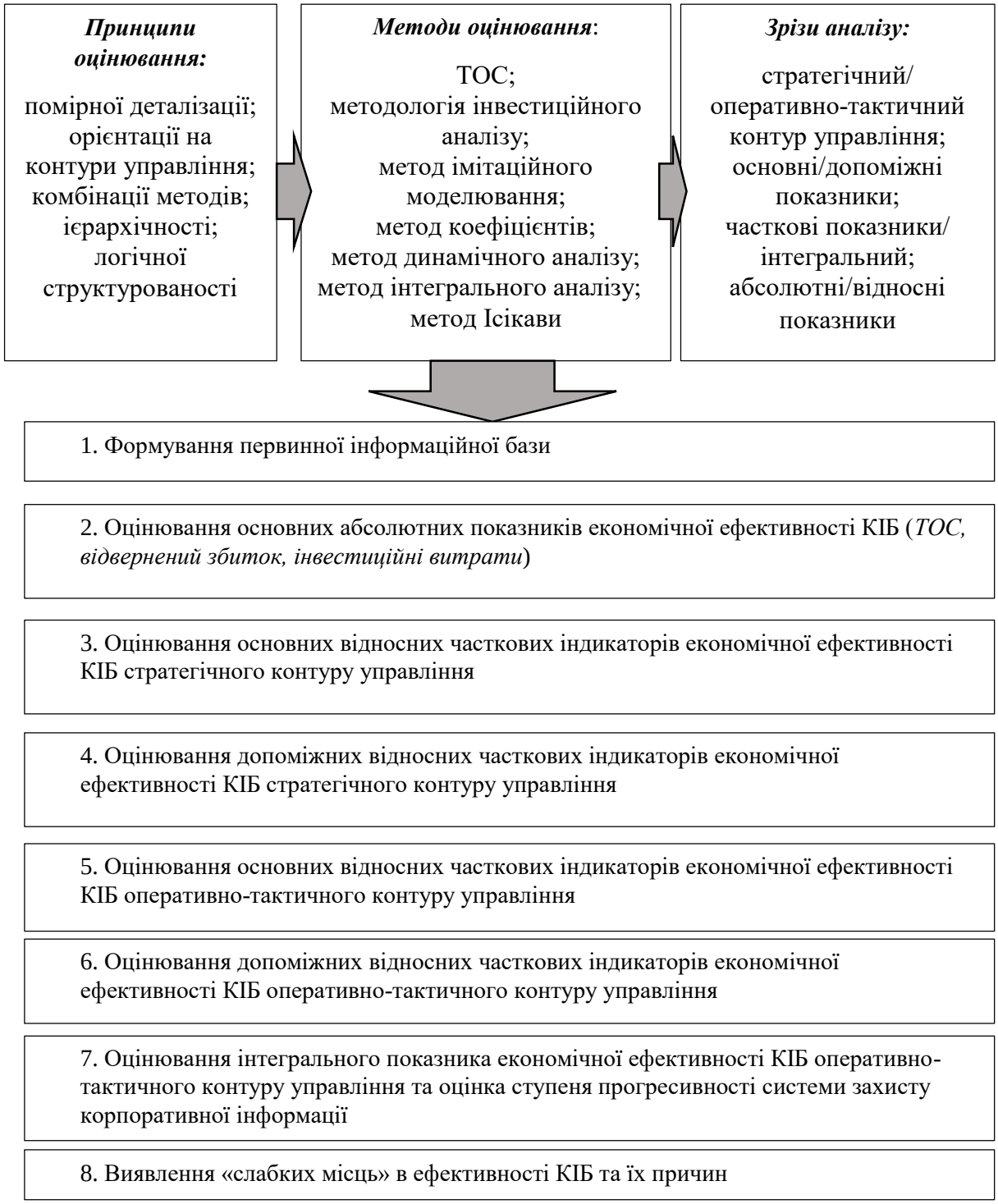


Рис.2.3. Архітектура процесу оцінювання економічної ефективності КІБ

Джерело: розроблено автором

Результати застосування запропонованого підходу є базою для подальшого вдосконалення як самого процесу формування КІБ, так і підвищення його економічної ефективності.

Висновки до розділу 2

1. Комплексний характер заходів формування ефективних систем інформаційної безпеки потребує цілісного бачення цього процесу. Проте на сьогоднішній день відсутні сформульовані концепції формування інформаційної безпеки, що унеможливлює забезпечити системний характер запроваджуваних заходів захисту інформації. На основі аналізу, синтезу та розвитку сучасних підходів до розуміння концепції визначено зміст концепції формування корпоративної інформаційної безпеки як систему поглядів на організацію та забезпечення такої безпеки, що відображається через обрану методологію формування, окреслені принципи та розроблений механізм забезпечення. Таким чином, концепція формування корпоративної інформаційної безпеки містить три принципові структурні компоненти: методологічна основа, принципи, механізм, які знаходяться в логічному зв'язку та підпорядкуванні.

2. Базовим елементом концепції є її методологічна основа. Саме вона індивідуалізує концепції корпоративної інформаційної безпеки на різних підприємствах та в наукових дослідженнях. Адже саме обрана методологічна база обумовлює принципи та механізм формування корпоративної інформаційної безпеки. Виходячи з того, що, на наше переконання, забезпечення інформаційної корпоративної безпеки з одного боку має ґрунтуватися на строго окреслених наукових засадах, а з іншого боку носити суто прагматичний характер, уважаємо за потрібне в межах компоненту «методологічна база» виокремити два підрівні «метаметодологія» та «підходи до управління».

3. Метаметодологія визначає загальні філософські основи пізнання світу та окремих явищ та процесів. Так, серед наявних загальнонаукових та філософських концепцій пізнання світу в основу формування підходів до забезпечення інформаційної безпеки доцільно покласти методологію позитивізму та нормативну теорію. Позитивізм – філософія позитивного знання, що відкидає теоретичні спекуляції й умогляди, як засоби одержання знання. Зазначена методологія найкращим чином, на наш погляд, може виступати основою

формування концепції корпоративної інформаційної безпеки, адже захист корпоративної інформації потребує постійного 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. Нормативна теорія описує «як має бути» та яким чином досягати цього стану. Важливою складовою цієї методології є нормативний аналіз, який власне й описує бажаний (ідеальний) стан об'єкта. У межах обґрунтування концепції формування корпоративної інформаційної безпеки нормативна методологія є основою для подальшого цілевизначення та розробки заходів у сфері захисту корпоративної інформації.

4. Інший підрівень методології – підходи до управління – спрямований на конкретизацію метаметодології і 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 корпоративної інформаційної безпеки, інтеграцію системного, процесного, проєктного підходів та концепції динамічних здатностей.

5. Важливе місце в концепції формування корпоративної інформаційної безпеки посідають принципи, серед яких ми виокремили: законності, дотримання балансу інтересів, системності, плановості, комплексності, безперервності, взаємної відповідальності, розумної достатності, персональної мінімізації повноважень, обов'язковості контролю, превентивного характеру заходів інформаційної безпеки, креативності та інноваційності, економічної ефективності, ситуативності та адаптивності, ризик-орієнтованості.

6. Прагматичною складовою концепції формування корпоративної інформаційної безпеки є її механізм, який є сукупністю об'єктів, суб'єктів, мети, завдань, функцій та методів впливу. Останні систематизовані за окремими видами: економічні, організаційно-правові, технічні. Представлений перелік методів

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

7. У процесі обґрунтування методологічних засад корпоративної політики інформаційної безпеки узагальнені та систематизовані напрями корпоративної політики інформаційної безпеки, які характеризуються багатовимірністю, системністю, можливістю врахування та аналізу домінантних чинників формування її базису, що дає змогу врахувати стратегічну і тактичну складові корпоративної політики інформаційної безпеки, визначити елементи її конфігурації, які забезпечать можливість залучення суб'єктів різних рівнів із метою вчасного виявлення, запобігання та ліквідації наслідків впливу дестабілізуючих чинників для досягнення інтересів корпоративних структур.

8. Управління корпоративною інформаційною безпекою є надзвичайно складним процесом з декількох причин: по-перше, підприємства функціонують в умовах постійно зростаючих загроз (як кількості, так і ступеня агресивності), що потребує постійного вдосконалення системи управління, креативності, інноваційності та випереджального характеру заходів; по-друге, реалізація заходів із протидії інформаційним загрозам завжди обмежується ресурсним потенціалом підприємства, перед усім – наявним бюджетом. Тому, 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 із цим постає актуальне питання, яким чином виміряти економічну ефективність управління корпоративною інформаційною безпекою.

9. Процес вимірювання економічної ефективності управління корпоративною інформаційною безпекою натрапляє на ряд методологічних перешкод: отриманий дохід або прибуток, що оцінюється як непонесений (відвернений) збиток, завжди є складно і неточно детермінованим показником;

витрати на забезпечення інформаційної безпеки носять різнорідний характер та з точки зору бухгалтерського обліку відносяться до різних періодів; окремий ефект у захисті корпоративної інформації може досягатися за рахунок еволюційних змін процесів, які не носять дуже витратного характеру, але сам ефект від таких удосконалень складно виокремити. До того ж він не знаходить відображення в окремих документах бухгалтерського обліку та звітності підприємства. Часто це потребує специфічних налаштувань у системі збору інформації та введення додаткових звітів у системі управлінського обліку.

10. Вивчення сучасних підходів до оцінювання ефективності КІБ дозволило зробити висновок про складність застосування єдиної методики для формування вичерпного висновку щодо ефективності КІБ та виявити ряд проблем, які потребують вирішення, зокрема: необхідності обґрунтування принципів оцінювання та систематизації показників економічної ефективності; визначення чітких критеріїв оцінювання окремих показників; обґрунтування рекомендацій щодо логічної послідовності аналізу окремих показників; необхідності формування інтегрального або узагальнюючого показника ефективності КІБ.

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

Основні результати розділу опубліковано в наукових працях автора: [1, 2, 4, 6, 7, 17, 18] – відповідно до списку опублікованих праць за темою дисертації на початку роботи.

Список використаних джерел до розділу 2

1. Сурмін Ю. П. Майстерня вченого : підручник для науковця / Ю. П. Сурмін. Київ : Консорціум із удосконалення менеджмент-освіти в Україні, 2006. 302 с.
2. Концепція / В. Лук'янець. Концепції науки // Філософський енциклопедичний словник / В.І. Шинкарук (гол. редкол.) та ін. Київ : Інститут філософії імені Григорія Сковороди НАН України: Абрис, 2002. 742 с.
3. Проєкт Концепції інформаційної безпеки України. 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 : навчальний посібник. Київ, 2014. 680 с.
6. Судакова О. І., Щеглова О. Ю., Гасенко О. О. Головна характеристика механізму управління економічною безпекою розвитку підприємства // Науковий вісник Міжнародного гуманітарного університету. 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. / М.І. Камлик. 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 [Електронне фахове наукове видання]. 2019. № 1(5), С. 61–72.

11. Позитивізм як найбільш впливовий рух західної філософії другої половини XIX. [Електронний ресурс]. URL: https://osvita.ua/vnz/reports/philosophy/13067 (дата звернення 14.06.2022).
12. Економічна енциклопедія : у трьох томах. Т. 1. / За ред. С.В. Мочерного. Київ : Видавничий центр «Академія», 2000. 864 с.
13. Словник економічних термінів [Електронний ресурс]. URL: http://epi.cc.ua/slovar-ekonomicheskih-terminov247.html (дата звернення 14.06.2022).
14. Холод Б. І. Системний підхід – основа сучасного управління діяльністю промислових підприємств / Б.І. Холод, О.М. Зборовська // Академічний огляд. 2010. № 1(32). С.48–54.
15. Єфімова О. Системний підхід – основа управління діяльністю підприємств / О.Єфімова // Персонал. 2007. № 2. С. 67–72.
16. Мескон М., Альберт М., Хедоурі М. Основи менеджменту / Переклад з англійської мови. URL: https://infotour.in.ua/meskon.htm (дата звернення 14.06.2022).
17. Сутність проектного підходу до управління організацією [Електронний ресурс]. URL: https://pidru4niki.com/1580042053533/menedzhment/upravlinnya_proektami (дата звернення 14.06.2022).
18. Управління ресурсами підприємства: монографія / за заг. ред. к.е.н., 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. 2014. №5. 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. Інформаційна безпека підприємства та організаційні заходи її забезпечення / Ірина Анатоліївна Маркіна, Юрій Миколайович Гарічев // Українськии 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: навчальний посібник / Ортинський В. Л., Керницький І. С., Живко З. Б. 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 інституту Київського національного університету 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 [Електронний ресурс]. 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: навчальний посібник. 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», Міністерсово освіти і науки України, 2000. С. 17–21.
36. Амитан В. М. Економічна безпека: концепція й моделі / В. М. Амитан // 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. [за ред. Т.Г. Васильціва]. Львів: Видавництво, 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 трьох томах. Т. 2. / За ред. С.В. Мочерного. Київ : Видавничий центр «Академія», 2000. 848 с.
40. Герцик В. А. Ієрархічна структура організаційно-економічного механізму управління розподілом підприємства / В.А. Герцик // Культура народов Причерноморья. 2009. № 172. С. 22–24.
41. Пономаренко В. С., Ястремская Е. Н., Луцковский В. М. Механизм управления предприятием: стратегический аспект: Монографія / В.С. Пономаренко, Е.Н. Ястремская, В.М. Луцковский. Харьков: изд. ХГЭУ, 2002. 252 с.
42. Саблук П. Т. Формування міжгалузевих відносин: проблеми теорії і методології / П.Т. Саблук, М.Й. Малік, В.А. Валентинов. Київ: ІАЕ, 2002. 294 с.
43. Полтавський Ю. А. Ринковий механізм як система забезпечення ефективної діяльності аграрних підприємств / Ю.А. Полтавський, О.М. Супрун // Вісник харківського національного технічного університету сільського господарства: економічні науки. ринкова трансформація економіки АПК. 2004. вип. 31. С. 376.
44. Методи моделювання бізнес-процесів [Електронний ресурс]. 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. Основи програмної інженерії / Л.П. Бабенко, К.М. Лаврищева. 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 / О.В. Вербіцький. – Львів: В-во наук.-техн. літ-ри, 1998. 247 с.
49. Goodliff P. Programmer's craft. Practice writing good code / 1st edition. San Francisco, California: No Starch Press, 2006. 624 p.
50. Гундарь К. Защита информации в компьютерных системах / К.Ю. Гундарь, А.Ю. Гундарь, Д. А. Янишевский. Київ: Корнейчук, 2000. 152 с.
51. Жуков І. Експлуатація комп’ютерних систем та мереж: Навчальний посібник / І. А. Жуков, В.І. Дрововозов, Б.Г. Махновський. Київ: НАУ, 2007. 361 с.
52. Катренко А. Дослідження операцій: підручник з грифом МОН / А.В. Катренко. Львів: Магнолія 2006, 2009. 350 с.
53. Малайчук В. Основи теорії кодування й декодування / В.П. Малайчук, В.Ф. Рожковський. Дніпр.: Дніпропетр. держ. ун-т, 2000. 204 с.
54. Taha H. Operations Research. An Introduction. London: Pearson Higher Education, 2017. 813 p.
55. Томашевський В. Моделювання систем / В.М. Томашевський. Київ: БИУ, 2005. 400 с.
56. Цегелик Г. Чисельні методи / Г.Г. Цегелик. 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 р. № 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 György. Anti-corruption compliance in the enterprise's program [Electronic resource] / G. Kocziszky, M. Veres Somosi, P.G. Pererva // 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 György. Compliance risk in the enterprise / G. Kocziszky, M. Veres Somosi, T.O. Kobielieva // Стратегії інноваційного розвитку економіки України: проблеми, перспективи, ефективність «Форвард-2017» : пр. 8-ї Міжнар. наук.-практ. Internet-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 György. Reputational compliance / G. Kocziszky, M. Veres Somosi, T.O. Kobielieva // 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 Szabolcs. Current evaluation of the patent with regarding the index of its questionnaire / S. Nagy, M. Sikorska, P. Pererva // 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. Compliance service at guest services enterprises / M. Sikorska, G. Kocziszky, P.G. Pererva // 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 / Ю. Бондаренко // Корпоративный юрист. № 6. 2008. С. 31–34.

66. Бортников Г. Комплайенс-риск (риск несоблюдения): международные стандарты и их применимость для банков в странах СНГ [Электронный ресурс]/ Г. Бортников. URL: http://www.iiru.ru/inner_auditor/publication/ foreignmass_media_articles/bortnikov (дата звернення 14.06.2022).
67. Климко Т. Ю. Корпоративний комплаєнс як превентивний захід боротьби з шахрайством / Т.Ю. Климко, Е.А. Мельник // Економіка і Фінанси. 2015. № 6-7. С. 25.
68. Козлов Д. Н. Контроль регуляторных рисков / Д.Н. Козлов, Ю.Н. Юденков. [Электронный ресурс]. URL: http://futurebanking.ru/reglamentbank/ article/2092 (дата звернення 14.06.2022).
69. Козырева Н. А. Внутренний контроль и комплаенс / Н.А. Козырева // Внутренний контроль в кредитной организации. 2015. № 1. С. 65.
70. Кобєлєва Т. О. Сутність та визначення комплаєнс-ризику / Т. О. Кобєлєва // Вісник Національного технічного університету «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 [Електронний ресурс]. 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. [Електронний ресурс]. 2016. URL: https://infourok.ru/lekciya- po-zaschite-informacii-modeli-bezopasnosti-927637.html (дата звернення 14.06.2022).
73. Мельник М. О. Аналіз побудови моделі політики інформаційної безпеки підприємства / М.О. Мельник, Г.Д. Нікітин, К.О. Мезенцева // Системи обробки інформації. 2017. Вип. 2(148). С. 126–128.
74. Носарев А. Модели в информационной безопасности [Електронний ресурс]. 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. Галатенко В. А. Стандарты в области безопасности распределенных систем // Jet Info. 1999. № 5. С. 16–19.
77. Степанов В. Ю. Інформаційна безпека як складова державної інформаційної політики / В.Ю. Степанов // 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 / С.М. Чуруброва // Проблеми програмування. 2016. № 4. С. 97–103.
79. Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. Киев: ООО «ТИД», 2004. 912 с.
80. Caballero A. Information security essentials for it managers: protecting mission-critical systems. URL: https://booksite.elsevier.com/samplechapters/9781597495332/02~Chapter_1.pdf (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 Національного університету «Львівська політехніка». Сер.: 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 національного університету імені Тараса Шевченка. Сер.: 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 університету. Серія: Технічні науки. 2018. №1. С.81–88.
89. 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).
90. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 р. № 537-V. Дата оновлення 06.02.2007. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 13.06.2022).
91. Домарєв В. В. Обґрунтування основних функцій системи управління інформаційною безпекою // Вісник Державного університету інформаційно-комунікаційних технологій. 2012. Т. 10, № 2. С. 102–104.
92. 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.
93. Інформаційні системи і технології в банках : Навч. посіб. / А.Я. Страхарчук, В.П. Страхарчук. Київ: УБС НБУ: Знання, 2010. 515 с.
94. Інформаційна безпека банку / Є. М. Бодюл // Протидія злочинам, які вчиняються з використанням комп'ютерних мереж [Текст] : тези доповідей

Міжнародної науково-практичної конференції (м. Севастополь, 1–2 жов. 2010 р.) / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». Суми: ДВНЗ «УАБС НБУ», 2010.

95. Хохлачова Ю. Політика інформаційної безпеки об’єкта // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2012. вип. 2(24). С. 23–29.
96. Визначення та обґрунтування суті політики інформаційної безпеки / М. Ф. Бондаренко, О. В. Потій, Ю. І. Горбенко та ін. // Радіотехніка. 2003. № 134. С. 9–25.
97. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання. Київ: ВД «Гельветика», 2017. 168 с.
98. Валіулліна З. В. Інформаційна безпека корпоративної економіки в умовах глобалізаційних процесів // Вісник Дніпропетровського університету. Серія: Менеджмент інновацій. 2016. Випуск 6. С. 34–41.
99. 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).
100. Жабинець О. Й. Політика інформаційної безпеки страхових компаній: українські реалії та досвід США // Проблеми економіки. 2014. № 4. С. 22–27.
101. Шилов М. С. Жевелєва І. С. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). Київ: НА СБУ, 2021. С. 325.
102. Бакай В. Й., Зима В. М. Нові виклики та особливості створення системи інформаційної безпеки підприємства // Вісник Хмельницького національного університету. 2020. № 5. С. 19–22.
103. Kim S. H., Wang Q.-H., Ullrich J. B.. A Comparative Study of Cyberattacks // Communications of the ACM. 2012. № 55:3. P. 66.
104. 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.

105. Park S., Ruighaver T. Strategic Approach to Information Security in Organizations // ICISS. International Conference on Information Science and Security. IEEE, 2008. P. 26–31.

106. 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.

107. 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.

108. 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.

109. 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.

110. 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.

111. Georg L. Information security governance: pending legal responsibilities of non-executive boards // Journal of Management and Governance. 2017. Vol. 21. № 4. P. 793–814.

112. 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.

113. 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.

114. Büyüközkan G., Göçer F. Digital supply chain: literature review and a proposed framework for future research // Computers in Industry. 2018. Vol. 97. P. 157–177.

115. 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.

116. 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.

117. 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.

118. 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.

119. Teece D.J. Business models and dynamic capabilities // Long Range Plan. 2018. № 51. P. 40–49.

120. 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.

121. Clauß T., Bouncken R.B., Laudien S., Kraus S. Business model reconfiguration and innovation in SMEs: a mixed-method analysis from the electronics industry // International Journal of Innovation Management. 2020. Vol. 24. № 2. 2050015. URL: https://www.worldscientific.com/doi/abs/10.1142/S1363919620500152

122. Бєгун А. В. Інформаційна парадигма безпеки економічної системи // Моделювання та інформаційні технології в економіці. 2011. № 83. С. 144–151.

123. Бєгун А. В. Аспектноорієнтована технологія оптимізації захисту додатків Web-порталу // Моделювання та інформаційні технології в економіці. 2010. № 81. С. 189–196.

124. 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.

125. Бєгун А. В. Оцінка економічної ефективності інформаційної безпеки підприємства // Інвестиції: практика та досвід. 2012. № 21. С. 35–36.

126. Рибидайло А. А Модель процесно-орієнтованої оцінки ефективності впровадження інформаційних технологій для поліпшення управління адміністративно-господарчими процесами / І.Г. Зотова, О.С. Левшенко, О.В. Поривай, С.В. Бобров // Збірник наукових праць ЦВСД НУОУ. Київ, 2014. № 1(50).

127. Тюріна Н. М. Оцінка вартості та ефективності використання інформаційних систем управління на промислових підприємствах / Н.М. Тюріна, В.Т. Параконний // Вісник Хмельницького національного університету. Економічні науки. 2006. № 2. Т. 2. С. 22–27.

128. Andresen J. L. A Framework for Selecting an IT Evaluation Method: in the Context of Construction / J. L. Andresen // Danmarks Tekniske Universitet. 2001. 257 p.

129. Cronk M. A. Conceptual Framework for Furthering Understanding of ‹IT business value› and its Dimensions / M. Cronk, E. Fitzgerald // PACIS 1997 Proceedings. 1997. P. 405–415.

130. Patel N. V. Evaluating information technology in dynamic environments: a focus on tailorable information systems / N. V. Patel, Z. Irani // Logistics Information Management. 1999. Vol. 12. P. 32–39.

131. Remenyi D. The Effective Measurement and Management of IT Costs and Benefits / D. Remenyi, A. Money, M. Sherwood-Smith // Oxford: Butterworth-Heinemann. 2000. 362 p.

132. 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.

133. 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.

134. 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.

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

136. 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.

137. 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.

138. 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.

139. 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.

140. Maqbool Z., Pammi V. C., Dutt V. Behavioral Cybersecurity: Investigating the influence of Patching Vulnerabilities in Markov Security Games via Cognitive Modeling // IJCSA. 2019. № 4(1). P. 185–209.

141. 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.

142. Majd S, Pindyck R. Time to build, option value, and investment decisions // Journal of Financial Economics. 1987. № 1(1). P. 7–27.

143. Велігура А. В. Оцінювання стану інформаційної безпеки підприємства / А.В. Велігура // Управління проектами та розвиток виробництва: Зб. наук. пр. Луганськ: вид-во СНУ ім. В. Даля, 2014. № 4(52). С. 28–39.

144. Журавель М. Ю. Формування системи показників оцінки рівня інформаційної безпеки підприємства / М.Ю. Журавель, Т.В. Полозова, О.В. Стороженко. // Вісник економіки транспорту і промисловості. 2011. № 33. С. 171–177.

145. Дячков Д. В. Методичні підходи до оцінки інформаційної безпеки підприємства [Електронний ресурс]. URL: http://dspace.pdaa.edu.ua:8080/ bitstream/123456789/2572/1/СТАТТЯ_СУМИ_ДЯЧКОВ.pdf (дата звернення: 17.06.2022).

146. Чубаєвський В. І, Лахно В. А., Криворучко О. В.. Касаткін Д. Ю., Десятко А. М.. Блозва А. І. Ефективність методики розрахунку показників інвестицій в систему інформаційної безпеки об’єктів інформатизації // Кібербезпека: освіта, наука, техніка. 2021. № 4(12). С. 96–105.

147. Чубаєвський В. Стратегічні орієнтири формування корпоративної політики інформаційної безпеки // Причорноморські економічні студії. 2021. Вип. 72. (Ч. 2). С. 24–30.

148. Чубаєвський В. І. Прогресивність розвитку системи захисту корпоративної інформації// Економіка та суспільство. 2022. № 44. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1793 (дата звернення: 01.11.2022).

149. Чубаєвський В. І. Методичний підхід до оцінки економічної ефективності системи захисту корпоративної інформації // Електронний журнал «Ефективна економіка». 2022. № 11. URL: https://nayka.com.ua/index.php/ee/article/view/730/738 (дата звернення: 21.11.2022).

150. Сукупна вартість володіння // Електронний ресурс. Режим доступу: https://uk.wikipedia.org/wiki/Сукупна_вартість_володіння. (Дата звернення: 15.05.2022)

151. Чубаєвський В. І. Методи управління корпоративною інформаційною безпекою. Економіка та суспільство. 2022. № 43. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1732

РОЗДІЛ 3
МОДЕЛІ ТА ТЕХНОЛОГІЇ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ

3.1. Систематизація ознак несанкціонованого доступу до корпоративної інформації

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 рівні, але і вдосконалювати 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, яка займається вивченням особливостей комп'ютерної злочинності [5].

Необхідно відзначити, що стрімкі темпи розвитку ІТ значно випереджають темпи реалізації нормативно-правової бази, що 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, розширюється і простір ознак, що характеризують способи отримання НСД до інформаційних ресурсів підприємств. Оскільки простір ознак НСД постійно розширюється, навіть кваліфікованим експертам у сфері ІБ без підтримки спеціалізованих програмних продуктів при прийнятті рішення у подібних питаннях обійтися складно. Власне все сказане вище зумовлює необхідність продовження досліджень у напрямі інтелектуалізації на основі ІТ процедури первинної формалізації неправомірних дій комп’ютерних зловмисників, які роблять спроби отримати НСД до ІС суб’єктів господарської діяльності.

У роботах [6, 7, 8] проаналізовано класифікаційні методи обґрунтування вимог до СЗІ. Проте, як зазначають автори, ці методи не позбавлені низки недоліків. Зокрема, ці методи не надають повноцінно реалізовувати синтез контурів ІБ при проєктуванні автоматизованих систем (АС).

Саме ця причина робить, на думку авторів [9, 10, 11], 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 практичні приклади застосування викладеного підходу.

Розвитком формального підходу до опису динаміки НСД до ресурсів ІС можна вважати роботи [12, 13]. У цих роботах авторами розвинений підхід, відповідно до якого для формалізації конфліктно-динамічних процесів під час НСД до ІС застосовано математичний апарат Марківських процесів. Але недоліком такого підходу стала та обставина, що необхідно в кожному конкретному випадку виробляти побудову графа, що описує алгоритм реалізації НСД до ІС. І хоч це дає дослідникам наочне уявлення про етапи реалізації атаки, але водночас вимагає досить високої кваліфікації експерта з ІБ та витрат часу для побудови подібного графа.

Крім того, 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 робіт. Наприклад, у [14] виконано огляд та аналіз існуючих методів забезпечення ІБ безпеки автоматизованих систем аутентифікації та розподілених мереж. Робота має оглядовий характер і конкретних рекомендацій автори не наводять.

У роботах [15, 16, 17] автори акцентують увагу на необхідності прийняття цілеспрямованого методу моніторингу безпеки та аналітики загроз. Це робить актуальним завдання формування простору ознак НСД до ІС. Як і багато інших робіт із цієї проблематики зазначене дослідження не дає конкретних рекомендацій щодо формування простору ознак НСД до ресурсів ІС підприємств.

Існує досить багато досліджень, присвячених ефективності застосування того чи іншого математичного апарату для опису функцій НСД до інформаційних ресурсів підприємств. До них відносяться: теорія ймовірностей [18], нечіткі множини [19], теорія ігор [20], графи та автомати [21], мережі Петрі та випадкові процеси [22].

Перспективним та недостатньо вивченим у сфері ІБ залишиться напрямок 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 вище сказаного, 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.

При формуванні 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, як правило, в електронних системах виявлення спроб НСД використовуються класифікатори, що зустрічаються в описах об'єктів одного класу та не зустрічаються в описах об'єктів інших класів. З іншого боку, набори значень ознак функцій НСД, які в описі жодного з класів НСД характеризують всі об'єкти даного 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 підприємств ефективно застосовувати принцип «незустрічності» наборів із допустимих значень ознак, що у свою чергу, дасть змогу будувати такі вирішальні правила для СЗІ, за яких розпізнавання спроб НСД (або загроз ІБ) проводилося б з мінімальною кількістю помилок.

На підставі результатів робіт [12, 13, 23] вираз, що описує ймовірність реалізації функції НСД до ресурсів ІС підприємства (P_{UNA}) можна описатитак:

$$P_{UNA} = \prod_{i=1}^{N}\left(1 - \frac{1}{\left(1+\sum_{k=1}^{N}\frac{\lambda_i^k}{\vartheta_i^k}\cdot\left(1+\beta_i^k\cdot\frac{\vartheta_i^k}{\chi_i^k}\right)\right)}\right), \quad (3.1)$$

де *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 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;

χ_i^k – параметр, що характеризує експоненційний час реалізації дій зловмисника, який реалізує функції НСД у ході *k*-го способу *i*-го етапу реалізації НСД;

ϑ_i^k – параметр, що характеризує експоненційний час, що вимагається штатним СЗІ для нейтралізації виявлених дій зловмисника під час *k*-го способу *i*-го етапу реалізації НСД;

N – число методів реалізації функцій НСД на різних етапах.

Значення змінної λ_i^k може бути в 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 такої ієрархічної структурної схеми, див. рис. 3.1. Ця структурна схема послужить основою для опису ієрархічної структури ознак НСД до ресурсів ІС.

Вважаємо, що при необхідності і при виникненні нових способів отримання НСД з боку зловмисників кількість ієрархічних рівнів можна змінювати. Крім того, думатимемо, що комп'ютерні зловмисники, залежно від мотивів та кваліфікації можуть переслідувати різні цілі НСД. І, відповідно, для реалізації НСД ними може бути використаний різний арсенал засобів, спрямований на досягнення тактичних цілей атаки або стратегічних цілей. У такому випадку НСД тільки випереджає

таргетовану атаку, а основним завданням зазвичай є спроба отримання контролю над бізнес-процесами підприємства або компонентами ІС.

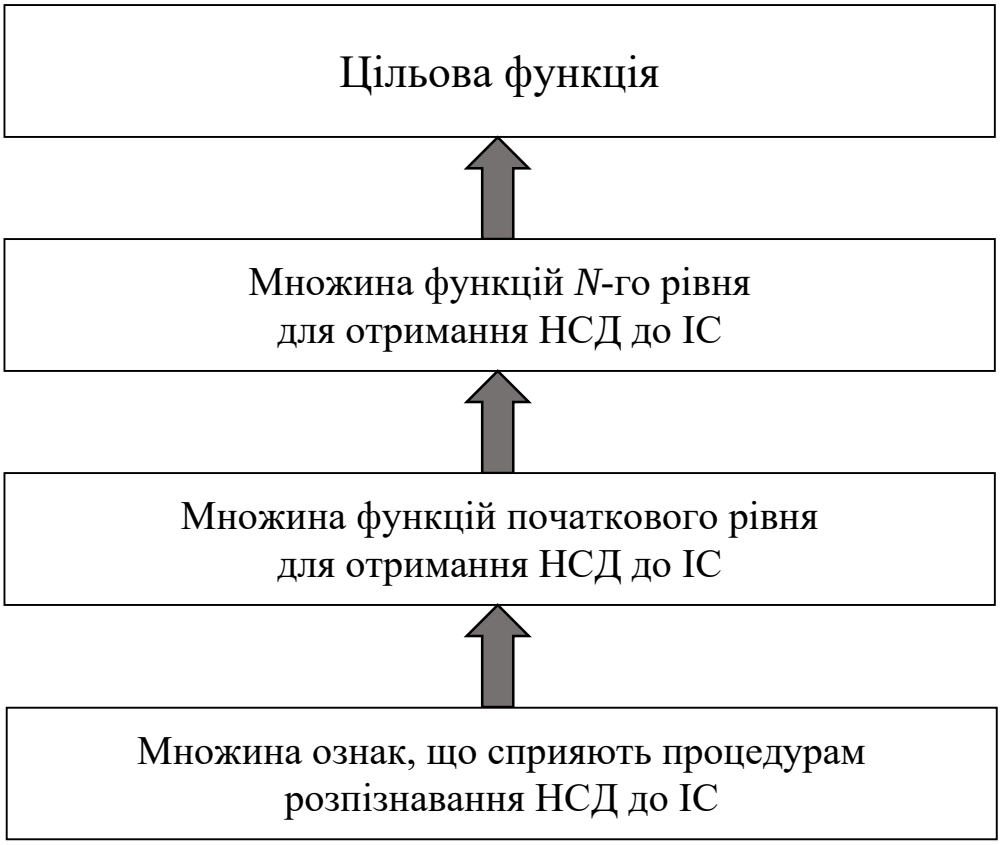


Рис. 3.1. Сутнісні характеристики інформаційного простору

Джерело: узагальнено та доповнено за [12, 13, 23]

Запропонована на рис. 3.1 ієрархічна структурна схема формування простору ознак НСД до ресурсів ІС підприємства носить 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;

– існують причинно-наслідкові зв’язки між реалізованими порушником функціями з НСД до ресурсів ІС та їх ознаками;

– слід дотримуватися 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

$\left(C^{(1)}\right)$ цієї множини ознак є підставою опису таких дій зловмисника. Тоді можна записати такий вираз:

$$\{RS\} \widehat{=} C^{(1)}, \tag{3.2}$$

де $rs_i \widehat{=} c_i^{(1)},\ i = 1,2,\ldots,I.$

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	$c_2^{(1)}$
Вивчення можливостей отримання доступу до		
3	каналів зв'язку ІС поза приміщенням ПК та серверів	$c_3^{(1)}$
4	каналам 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 з		
7	клавіатур ПК	$c_7^{(1)}$
8	моніторів ПК	$c_8^{(1)}$
9	мережевих пристроїв ІС та ін.	$c_9^{(1)}$

Закінчення табл. 3.1

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	$c_{15}^{(1)}$
	та ін.	

Джерело: розроблено автором

Зрозуміло, що враховуючи специфіку бізнес-процесів підприємства та особливості ІТ, які в них застосовані, ознаки не є постійними. Однак, якщо говорити про більшу частину інформації, що циркулює в ІС підприємств, перелік ознак буде досить стабільним. Частково це показано в таблиці 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 $I = \left|C^{(1)}\right|$ – 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:

$$\left|C^{(1)}\right| < \left|C^{(2)}\right|. \quad (3.5)$$

У табл. 3.2 функції НСД, які раніше в табл. 3.1 віднесені до першого ієрархічного рівня, наприклад, до категорій знімання 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

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

Джерело: розроблено автором

Для функцій, що входять до множини, і які утворені в результаті композиції ознак НСД до ресурсів ІС, слід застосувати причинно-наслідковий підхід. Тобто розглянути зв’язки між даними функціями та відповідними функціями, що належать $\left|C^{(1)}\right|$.

Сформована множина $C^{(2)}$:

$$C^{(2)} = \left\{c_j^{(2)}\right\},\ j = 1,2,\ldots,j, \qquad (3.6)$$

На наступному рівні аналізу ієрархічної структурної схеми формування простору ознак НСД до ресурсів ІС підприємства може бути розширено на третьому рівні – $C^{(3)}$.

Доцільність формування третього та наступних рівнів диктується специфікою бізнес-процесів підприємства і визначається тими ІТ, які конкретне підприємство використовує в цих бізнес процесах. Наприклад, якщо це транспортна компанія, то НСД може бути реалізований не лише через ІС, а й через електронні підсистеми, відповідальні за відстеження:

– маршруту;

– вантажу;

– витрати пального;

– зв’язку з диспетчером;

– та ін.

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 роботах [25, 26] було запроваджено поняття елементарного класифікатора. Під елементарним класифікатором розуміється 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 інформційно-комунікаційним системам торговельної галузі (ІКСТГ), у якому розпізнавання проводилося з мінімальною кількістю помилок.

Як інформативну значущість ознаки функції НСД до інформаційних ресурсів підприємства використовується параметр [25]:

$$IZ_{pa} = \frac{\sum_{(sp_a, NP_{pa}) \in \mathrm{MC}^{\mathrm{AL}}(KL)} v_{(sp_a, NP_{pa})}}{\sum_{(sp_a, NP_{pa}) \in \mathrm{MC}^{\mathrm{AL}}(KL)} v_{(sp_a)}}, \quad p_{aj} \in NP_{pa} \tag{3.7}$$

де $v_{(sp_a, NP_{pa})}$ – функція значимості елементарного класифікатора класу функції НСД;

$NP_{pa} = \{p_1, \ldots, p_N\} -$ 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 усіх 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 дає можливість фахівцям з ІБ підприємства на наступних етапах експлуатації ІС не тільки виконувати аудит ІБ, але й 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 даній тематиці, наприклад, робіт [27, 28, 29] для коректності та обґрунтованості вимог контурів ІБ підприємства формалізація ознакового 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 подібного роду діаграм часто пов'язана із суб'єктивним трактуванням і не враховує реальну інформативність ознакового простору спроб НСД.

Таким чином, у даному 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 невеликого числа. Це дозволяє ефективно реалізувати первинну формалізацію неправомірних дій комп'ютерних зловмисників для подальшого математичного опису параметра ймовірності НСД, наприклад, на основі Марківських ланцюгів.

3.2. Програмний комплекс для оцінки актуальності загроз витоку інформації

У сучасному світі високотехнологічні електронні пристрої, які стали звичними для ефективних бізнес-процесів, породили й нові загрози для інформаційної безпеки (ІБ) не тільки їх власників, а й для підприємств загалом. Своєчасне виявлення загроз ІБ – це перший крок до їх 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 широких завдань зі знімання,

реєстрації, перехоплення, прийому тощо будь-якої електронної та іншої інформації, яка необхідна для реалізації бізнес-процесів підприємств.

Бізнес-середовище багатьох сучасних суб'єктів господарювання, які активно впроваджують у свої бізнес-процеси інформаційні технології (ІТ), останнім часом зазнало якісних змін. Свою частину в ці процеси вносить і посилення тенденцій щодо глобалізації економіки, посилення конкуренції, появи на ринку нових економічних суб'єктів, збільшення мобільності бізнесу та ін. Зауважимо, що в таких умовах, навіть якщо не ставити задачі з цілеспрямованого ведення конкурентної розвідки, менеджменту підприємств необхідно прикладати значні зусилля для збирання та аналізу відповідної бізнес-інформації. Наприклад, якщо підприємство працює із зовнішніми постачальниками, її спеціалістам необхідна інформація про постачальників, компанії-субпідрядників, дистриб'юторів, транспортних компаній, що займаються логістичним забезпеченням, оптових і роздрібних продавців, страхових компаній тощо.

Наразі за допомогою технічних засобів розвідки (ТЗР) зловмисники можуть не тільки вести спостереження за об'єктом, що їх цікавить, але й здійснювати за допомогою спеціальної техніки, наприклад, підслуховування переговорів або перехоплювати радіосигнали. Таке перехоплення дозволяє зловмиснику 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 протягом усієї історії промислового шпигунства різні дійові особи, які представляють як сторони захисту, так і бік нападу, мінялися своїми ролями. Так чи інше незмінними залишалися лише об'єкти захисту: приміщення, в яких знаходиться інформація; матеріальні носії; засоби обробки інформації та ін.

З розвитком електронних пристроїв та ІТ акцент сторони захисту та атакуючої сторони змістився в бік захисту (чи атаки) на технічні канали передачі інформації (ТКПІ).

У роботах [30–32] авторами проведено досить глибокий аналіз можливостей засобів технічної розвідки. Проте дані дослідження мають швидше ретроспективний характер, не містять методологічних рекомендацій, спрямованих на зниження рівня загроз витоку інформації.

У роботах [33–35] розглянуто перспективи розвитку та можливості технічних засобів розвідки (ТЗР) для конкурентної розвідки. Насамперед увага авторами приділена можливостям ТЗР перехоплення побічного електромагнітного випромінювання та наведення (ПЕМВН) від засобів обчислювальної техніки (ЗОТ). Це пов'язано із широким упровадженням 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 наш погляд, не розкрито суб'єктивну складову проявів ефекту захищеності інформації від витоків у ТКПІ.

У роботах [36–38] розглянуто питання витоків інформації через шпигунське програмне забезпечення. Цей напрямок є відносно новим, оскільки ринок ПЗ стрімко змінюється, зокрема виникли системи електронного документообігу.

У роботах [39, 40] автори зосередили увагу на потенційних загрозах витоку інформації через різні ТКПІ, а також дали вичерпну класифікацію каналів витоку інформації (КВІ).

У роботах [41, 42] автори приділили особливу увагу захисту від витоків віброакустичними каналами, 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 достатньо оперативно може реагувати на зміну ландшафту кібернетичних загроз. А саме цей вид загроз сьогодні, на думку низки дослідників [43, 44] та практиків у сфері захисту інформації [45], є найбільшою небезпекою для інформаційних ресурсів підприємств.

У роботах [30, 34, 40, 42, 43] розглянуто основні умови, за яких виникають параметричні канали витоку інформації (КВІ). Автори віднесли до таких умов: наявність у системах нелінійних елементів, встановлення зловмисниками

напівактивних закладних пристроїв, застосування атакуючої стороною високочастотних генераторів з антенами та ін. Зауважимо, що останній КВІ виявити досить складно. Для виявлення таких генераторів необхідно скласти повну карту електромагнітної обстановки, а ця робота є частиною методики аналізу та оцінки актуальності загроз витоків інформації. Авторами такої роботи не проведено.

У роботах [46, 47] наведено результати досліджень із проблематики систематизації проявів ефекту захищеності інформації від витоків по ТКПІ. Однак ці дослідження носять фрагментарний характер і не завжди пов'язані із системними проявами суб'єктно-об'єктних відносин у бізнес-процесах підприємств.

Таким чином, зростаючі вимоги до протидії ТЗР у цілому, а також збільшені вимоги до ступеня захищеності інформаційних ресурсів підприємств, зокрема, та обґрунтованості заходів запобігання витоку інформації по ТКПІ є актуальними та потребують розвитку методологічного апарату та відповідного прикладного програмного забезпечення (ПЗ), що сприяє автоматизації рутинних трудомістких розрахунків.

Усе вище сказане зумовило релевантність нашого дослідження. Головна мета якого – автоматизувати оцінку актуальності 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, і акустичним (віброакустичним) каналам.

Завдання комплексного захисту на підприємствах, принаймні зміни ландшафту, охоплюють дедалі більше коло питань. Однією з граней є обстеження різних фізичних полів, що виникають під час роботи технологічного та офісного обладнання підприємств.

Вирішення завдань, пов'язаних із захистом інформації в 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 демаскуючі ознаки.

В основу методики, що застосовується в інтелектуальній ІС щодо оцінювання актуальних загроз ІБ (у контексті оцінки конфіденційності інформації) покладемо автоматизацію експертизи. Експертизі піддаються обставини, які дозволяють оцінити фактори, що в тій чи іншій мірі впливають на ступінь захищеності інформації.

Розглянемо таку важливу складову методики як оцінка рівнів загроз витоку конфіденційної інформації через побічне електромагнітне випромінювання та наведення (ПЕМВН) та віброакустичні сигнали.

Для початку виділимо джерела та ознаки, які дозволяють або експерту, або автоматично за допомогою інтелектуальної ІС віднести їх до потенційних джерел загроз для ІБ підприємства.

При цьому вважаємо, що в множинах виду, що формуються КВІ при експертному оцінюванні, необхідно врахувати всі ознаки відповідного для 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 – $\{v_j\}$, див. таблицю 3.3. Де індекси j – номери факторів вразливості.

Для множини $\{v_j\}$ вважаємо, що будь-які види загроз із часом або в міру залучення певних заходів захисту інформації або 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 при експлуатації відповідної вразливості або

повністю відсутня, або незначна. Одиниця в цьому випадку відповідає максимально високому рівню виконання загрози відповідної вразливості КВІ.

Рис. 3.2. Класифікація порушників ІБ підприємств

Джерело: розроблено автором

Неактуальні загрози при автоматизованих розрахунках не брати до уваги, а зосередити його лише на актуальних загрозах.

Таким чином, у табл. 3.3 перелічено фактори, що характеризують потенційний перелік вразливостей. Основна розрахункова залежність із метою оцінки актуальності загроз витоку інформації з ТКПІ за умов динамічного

вдосконалення ТЗР визначить ймовірністю наявності відповідних умов виконання відповідної загрози порушником з відповідним рівнем підготовки.

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: розроблено автором

Вважаємо, що попередня оцінка виконується експертами під час анкетування. Анкета складена таким чином, що оскільки межі актуальності / неактуальності загроз та коефіцієнта реалізованості не завжди чітко визначені, 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*-ї вразливості.

Тоді ймовірність визначиться так:

$$P_j = 1 - \left(k_{j,1}\left(1 - p_{j,1}\right) \cdot k_{j,2}\left(1 - p_{j,2}\right)\right), \quad (3.8)$$

де $k_{j,1}$ – коефіцієнт, що набуває значення якщо для 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 та 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. У загальному випадку це опишемо так: $\{th_c\},\ c = 1,2,\ldots,C$.

Для множини $\{th_c\}$, наприклад, загрози можуть виглядати так, див. табл. 3.4 (наведено лише фрагмент найзагальніших загроз).

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]
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: розроблено автором

Для множини $\{th_c\}$, джерел загроз витоку технологічного вважаємо, що будь-які види джерел загроз із 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:

$$P_c^v = 1 - \prod_{j=1}^{N}\left(1 - \lambda_{j,c} \cdot P_j\right), \qquad (3.9)$$

де $P_c^v -$ ймовірність виконання c-ої 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);

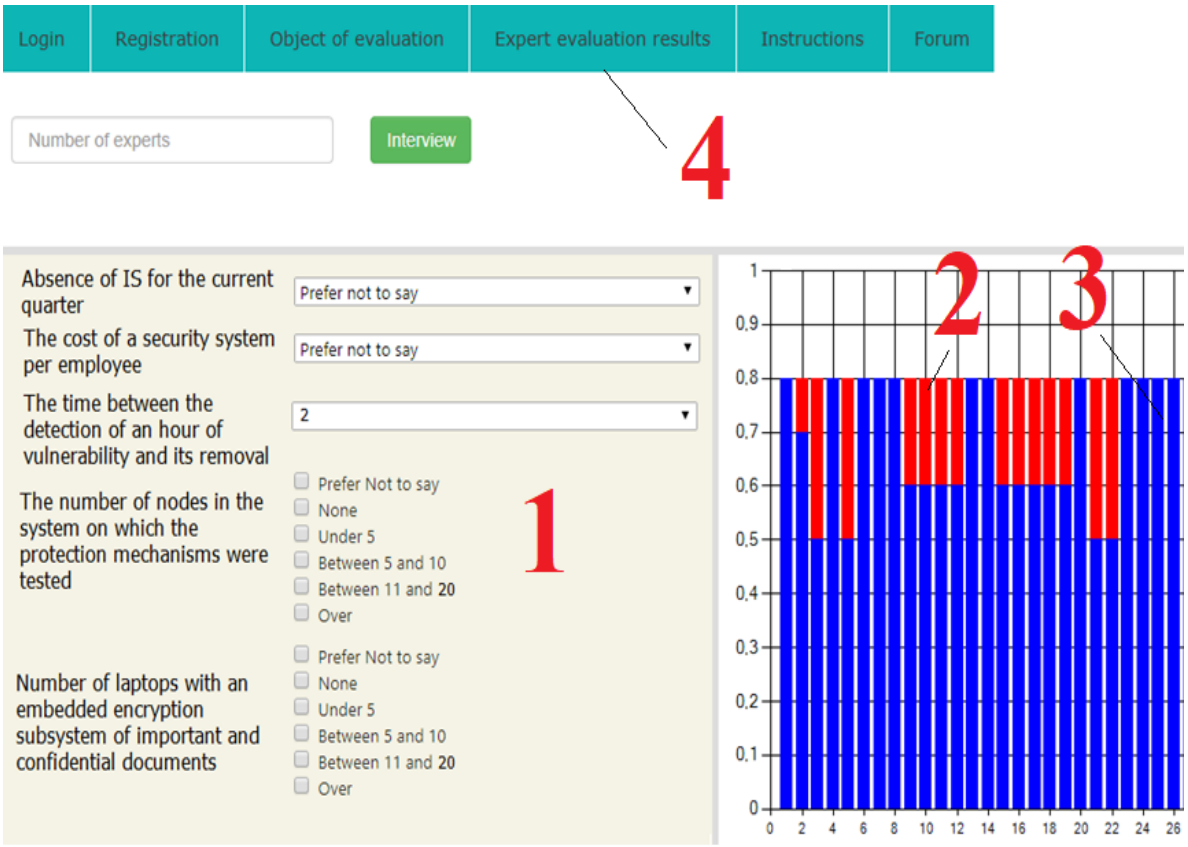
$\lambda_{j,c} -$ коефіцієнт актуальності, який приймається на підставі застосування апарату нечіткої логіки (в діапазоні від 0 до 1).

При оцінюванні припускаємо, що зовнішній або внутрішній порушник ІБ не має можливостей впливати на інформацію, що 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 із 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 збору, обробки, 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 і отримання інформації про вразливі елементи обладнання та технологічні процеси підприємств, наміри протидіючої сторони та ін.

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.



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 вигляд програмного комплексу «Assessment of threats» для оцінки актуальності загроз витоку інформації

Джерело: розроблено автором

На рис. 3.3 представлений скріншот основного діалогового вікна ПЗ «Assessment of threats». Щоб підвищити рівень об'єктивності вважаємо, що експерт з інформаційної безпеки спеціалізується на питаннях аналізу каналів витоків

інформації певного виду. Наприклад, він є фахівцем у галузі акустичних (віброакустичних) КВІ або в галузі витоку інформації через канали ПЕМВН.

На рис. 3.4 та 3.5 показано 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 оцінки актуальності загроз витоку інформації було запрошено експертів з досвідом роботи в галузі захисту інформації не менше 5 років.

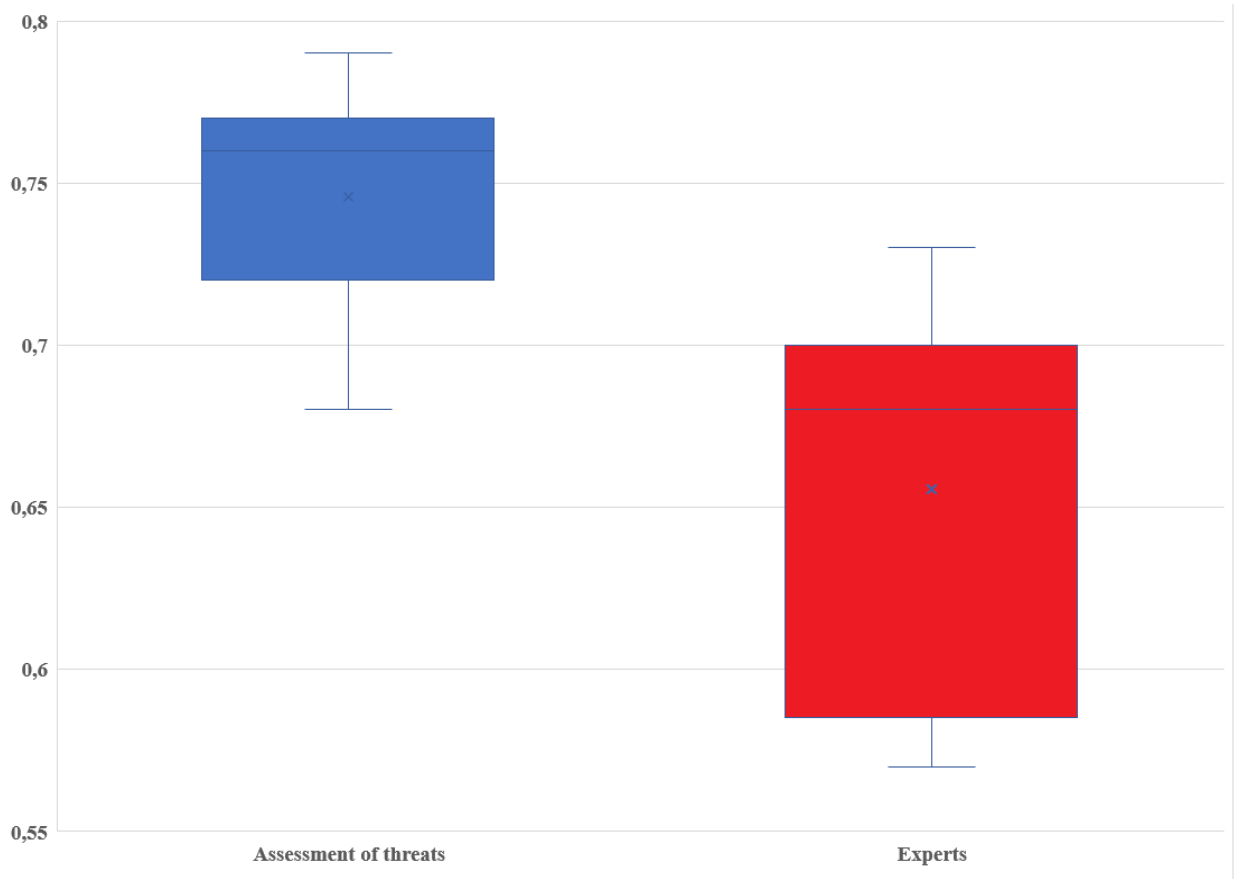


Рис. 3.4. Результати оцінювання експертами самостійно та за допомогою ПЗ «Assessment of threats» ступеня захищеності ТКПІ підприємства

Джерело: укладено автором

На 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.

Під час тестування на ПЗ «Assessment of threats» 45 – 55 %. скоротилися витрати часу оцінювання ознак несанкціонованого доступу до ТКПІ підприємства.

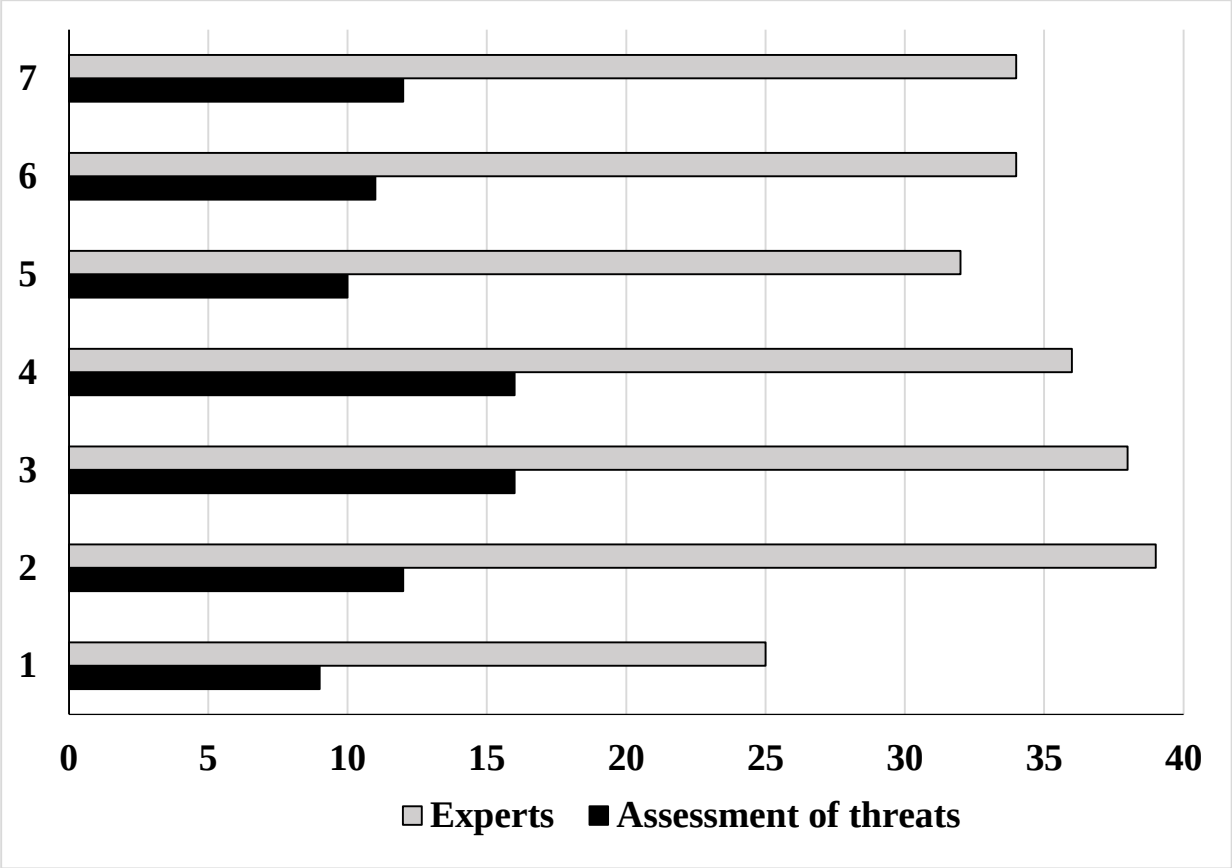


Рис. 3.5. Час, що витрачається експертами самостійно та за допомогою інтерфейсу ПЗ «Assessment of threats» для оцінювання ознак несанкціонованого доступу до ТКПІ підприємства

Джерело: розроблено автором

Порівняно з аналогічними рішеннями, розглянутими в [47–50], ПЗ «Assessment of threats» має такі переваги:

– можлива інтеграція розробленого ПЗ з існуючою 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.

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.

Крім того, виявленим недоліком запропонованого підходу є той факт, що ПЗ «Assessment of threats» не дає можливості на даному 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. Наразі 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 дозволяє 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 оцінки ризиків втрати інформації, дозволяє комплексно оцінити рівень захищеності ТКПІ підприємства. Розроблене ПЗ сприяє зниженню витрат на проведення вузькоспеціальних досліджень у питаннях щодо оцінки актуальності загроз витоку інформації з ТКПІ в умовах динамічного вдосконалення ТЗР. Таким чином, використання запропонованого ПЗ дозволяє автоматизувати процедуру оцінки актуальності загроз витоку інформації з ТКПІ в умовах динамічного вдосконалення ТЗР та вдосконалити процес оцінювання захищеності підприємств шляхом використання релевантних оцінок експертів.

3.3. Моделювання ефективності інвестицій на формування системи захисту корпоративної інформації

Відповідно до загальноприйнятої точки зору, характерної для більшості фахівців у галузі інформаційної безпеки (ІБ), сформувалася думка, що інвестування в ІБ та її концепція щодо оптимального складу апаратно-програмних засобів для конкретного об'єкта інформатизації (ОБІ), зокрема, підприємства, будуть ефективними якщо забезпечити виконання вимог державних нормативних документів та стандартів. Така думка сформувалася з урахуванням відсутності єдиної загальновизнаної методики оцінки економічного ефекту від інвестування в ІБ ОБІ [51, 52]. Зауважимо, що в цьому контексті проблематики оцінювання ефективності інвестування в ІБ ОБІ ми розуміємо перевищення вартісної оцінки кінцевого результату відповідних заходів над сумарними розмірами інвестицій, тобто сукупними витратами фінансових ресурсів на ІБ ОБІ протягом фіксованого періоду часу [53].

Складність оцінювання реального ефекту від інвестування в ІБ ОБІ обумовлюється досить великим переліком специфічних для сектору захисту інформації (ЗІ) та кібернетичної безпеки (КБ) факторів. Не вдаючись в їх детальний аналіз, відзначимо лише істотний вплив на ефективність інвестування в ІБ ОБІ таких факторів як:

1) ландшафт кіберзагроз, що постійно змінюється;

2) різноваріантні стратегії та тактики атакуючої сторони (комп'ютерних зловмисників);

3) швидкий розвиток технічних засобів захисту інформації (ЗІ) та кібербезпеки (КБ) тощо.

У свою чергу, відповідно до базових постулатів теорії оцінки ефективності систем, відомо, що якість засобів захисту інформації (далі ЗЗІ) може проявлятися лише під час їх реального цільового застосування на ОБІ. Саме ця обставина дає можливість об'єктивно оцінювати ефективність їх застосування, а отже і результативність інвестицій у системи захисту інформації (СЗІ) на ОБІ [54, 55].

Додаткова складність при оцінюванні ефективності інвестування в ІБ ОБІ пов’язана з невизначеністю результатів функціонування СЗІ. Уже на етапі проектування СЗІ є фактори невизначеності. Наприклад, пов’язані з тим, що може скластися така ситуація, коли сторона захисту ОБІ витратить значні суми коштів на захист від складних таргетованих кібератак, а атакуючій стороні часто досить вдатися до невеликих витрат (інвестицій в кібератаку) застосувавши методи соціальної інженерії. Така тактика застосування методів соціальної інженерії в певних випадках допомагала обходити найсучасніші СЗІ [56]. Таким чином, у ході реалізації проєктів у сфері ІБ рівень функціональності СЗІ може знизитись. Отже, з погляду методології моделювання ефективності інвестування в ІБ, ряд функціональних метрик СЗІ не може бути тотожно виражений і описаний детермінованими показниками.

Процедури, які передбачають тестування та сертифікацію компонентів СЗІ, не сприяють повною мірою усуненню невизначеності властивостей системи захисту. Ці процедури не можуть передбачити майбутні сценарії атак та тактику зловмисників. Таким чином, об’єктивною якісною характеристикою СЗІ, а також її здатністю пристосування до необхідного рівня ІБ в умовах зростання кількості та складності деструктивних впливів комп’ютерних зловмисників на інформаційно-комунікаційні системи (ІКС) або інфраструктуру ОБІ, можна обґрунтовано вважати ймовірнісні параметри СЗІ. До останніх можна віднести параметри, що характеризують, наприклад, рівень можливості конкретного засобу захисту інформації (далі за текстом ЗЗІ) за заданих умов, досягати обумовлених цілей ІБ. Даний імовірнісний параметр і має бути покладено в основу комплексного показника (критерію) оцінки ефективності аналізованого ЗЗІ. Як підкритерії в такому випадку можна прийняти придатність певного ЗЗІ та його оптимальність для конкретної задачі.

У контексті завдання, що вирішується, під придатністю ЗЗІ розумітимемо його здатність спільно з іншими засобами (як апаратними, так і програмними) виконувати всі встановлені в системі захисту інформації вимоги. А в такому разі

оптимальність можна трактувати як ознаку здатності ЗЗІ, досягати в своїй роботі екстремальних значень при дотриманні низки обмежень.

Звичайною практикою в процесі синтезу ЗЗІ для контурів є розв'язання багатокритеріальної задачі, яка обумовлюється необхідністю виконувати порівняння різноваріантних архітектур контурів ЗЗІ. Як приклад, можна навести порівняння централізованої та децентралізованої схеми побудови контурів ЗІ. При вирішенні багатокритеріальних оптимізаційних завдань щодо вибору ЗЗІ для розподілених обчислювальних систем неминуче виникає потреба проаналізувати показник ефективності як окремих ЗЗІ, так і їх наборів. Власне такі набори апаратно-програмних засобів ЗІ, організаційних та ін. заходів формують комплексні системи захисту інформації (далі КСЗІ). Такі набори засобів ЗІ можна описати і використовуючи імовірнісно-часові характеристики функцій розподілу. До останніх, зокрема, можна віднести й імовірнісні показники можливості зловмисників протягом деякого часу подолати контури ЗЗІ ОБІ.

Усі вище викладені аргументи дозволяють стверджувати, що в процесі оцінки ефективності функціонування СЗІ об'єкта господарювання найбільш доцільно застосовувати імовірнісні методи. Відповідно до цих методів прийнятний для сторони захисту гарантований рівень ІБ трансформуватиметься в довірчі ймовірності відповідних метрик захисту інформації та КБ ОБІ підприємства.

Зауважимо, що під час багатокритеріальної оптимізації ЗЗІ також виконується оцінювання рівня гарантій ІБ залежно від особливостей ОБІ (наприклад, банк, промислове підприємство, сфера торгівлі чи освіти тощо). А цей рівень досить великою мірою залежить від розміру потенційних збитків для інформаційних масивів ОБІ. У такому випадку виникає нове завдання, пов'язане з отриманням чисельної оцінки ризику для ОБІ. Тобто стороні захисту необхідно мати уявлення про розподіл випадкових величин збитків у разі атаки. У такій ситуації традиційно вдаються до методів імітаційного моделювання. Як альтернативний підхід використовують результати активного аудиту ІБ (або СЗІ) для ОБІ, що аналізується [80].

У роботах [57, 58] було показано, що когнітивні моделі дають можливість загалом аналізувати СЗІ для ОБІ. Автори у своїх моделях здійснюють вибір комплексів заходів щодо вдосконалення СЗІ. Крім того, можна визначати спрямованість необхідних впливів на ситуацію із ЗІ. Крім того, авторами розглянуто процедуру вибору метрик ІБ, які здатні охарактеризувати розвиток ситуації в перспективі. На думку авторів [58, 59] перевагою когнітивного моделювання є можливість обліку як якісних, так і кількісних показників ЗЗІ. Як недолік такого підходу, можна назвати лише сценарні прогнози розвитку ситуації.

У [60] авторами під час моделювання розглядався тимчасовий чинник у процесі інвестування в ІБ ОБІ. Проаналізовано тактику захисту, яку автори назвали «чекай і дивись». Тобто стороні захисту слід обмежити надмірне інвестування коштів у СЗІ та ІБ (або авторської термінології КБ), виходячи з вже досягнутого результату. Безперечною перевагою такого підходу слід визнати можливість брати до уваги невизначеність настання того моменту часу, коли виходячи з наявних даних про атаку, можна гнучко збільшувати (або зменшувати) розміри інвестиційних коштів на ЗЗІ для пом’якшення наслідку атаки. На наш погляд, цей підхід позбавлений суб’єктивності. І справді, на думку авторів [60], єдиний спосіб отримати інформацію про атаку це фіксація факту атаки. Тільки після цього сторона захисту має прореагувати та виділити фінансовий ресурс (далі ФР) на ІБ ОБІ. Недоліком цього підходу є те, що він ґрунтується на структурі з дискретним часом атаки. І це призводить до необхідності повторно проводити розрахунки у разі зміни ситуації та метрик ІБ ОБІ. У [61] показано, що традиційні методи оцінювання інвестиційних проєктів, як правило, занижують їх вартість. Автори роботи [62] пропонують модель, у якій розглянуто необхідний поріг інвестицій з урахуванням невизначеності ситуації під час інвестування. Однак подальшого розвитку цей підхід не отримав. У [63] автори запропонували модель послідовного інвестування в нові технології. Відмінністю моделі стало те, що автори враховують можливість послідовного інвестування в нові технології. Наприклад, підприємство може використовувати вже наявну технологію в очікуванні, що нова технологія стане більш доступною на ринку. Чинник технологічної невизначеності для варіанта

застосування нової технології авторами детально не розглядається, що загалом може вплинути на кінцевий прибуток від інновацій, у тому числі у сфері ІБ. У [64] автори досліджують параметри оптимальності термінів запровадження нових технологій. За основу прийнято підхід, що базується на пуассонівському процесі. Проте, зауважимо, що автори не враховують цінової невизначеності, а це на ринку інформаційних технологій та технологій ЗЗІ може відігравати не останню роль.

Оригінальний підхід у моделюванні технологічної невизначеності при впровадженні інновацій описаний у [65]. Автори аналізують ситуацію, коли підприємство може зіткнутися із ціновою та технологічною невизначеністю при інвестуванні. Перевагою описаного підходу стала можливість урахування компенсації монопольного прибутку, який отримає лідер на ринку. До недоліків такого підходу можна віднести відсутність обліку часових параметрів інвестування. А така ситуація у сфері ІБ не є типовою.

У [60, 66] розглянуто проблематику інвестування в кібербезпеку для випадку, коли контрагенти можуть обмінюватися інформацією, наприклад, щодо виявлених вразливостей у своїх інформаційних системах (ІС). Авторами показано, що подібний обмін даними сприяє зниженню рівня невизначеності щодо потенційних ризиків. Це, у свою чергу, сприяє оптимізації термінів інвестування. Автори самі вказали на певні обмеження, що накладаються на модель. Одним з основних обмежень є припущення зниження ризиків лише завдяки ситуації широкого обміну інформацією між контрагентами. Модель не дозволяє інвестору знаходити оптимальну стратегію інвестування, оскільки модель є лише формалізованим описом інвестиційного процесу у КБ ОБІ.

У [67] автором узагальнено підходи реалізації процесу інвестування в КБ. У роботі розглянуто п’ятиетапну методологію підтримки рішень щодо КБ ОБІ. Оскільки методологія досить об’ємна, її реалізація практично без відповідної комп’ютерної підтримки прийняття рішень стане досить трудомісткою, що знижує практичну цінність описаного підходу. У [68] автори виклали оригінальну емпіричну модель для вибору оптимальної стратегії інвестування в ІБ. Модель заснована на байєсівській статистиці та враховує конкретні механізми КБ. У самій

роботі розглянуто приклад обліку у процесі інвестування технологій систем виявлення вторгнень (СВВ), що стрімко розвиваються. Запропонований у [68] підхід отримав розвиток у роботах [69, 70]. Так, автори в нових дослідженнях урахували оптимальні терміни інвестування. Крім того, покращена модель дозволила врахувати можливості вдосконалення характеристик СВВ на основі їх байєсовського навчання. На думку авторів, найбільш прийнятною стратегією інвестування в ІБ повинна стати поетапна стратегія вкладення фінансових коштів в ІБ ОБІ, якщо виявляються нові загрози та вразливості. У роботі [68] також розглянутий варіант, коли інвестування виконується у взаємопов'язані інвестиційні проєкти.

У [71] запропонована модель ураховує негнучкість низки інвестиційних проєктів. Це в деяких ситуаціях може бути властиво і вибору стратегій інвестування в ІБ ОБІ. Модель спрямовано на вивчення рентабельності використання поточних технологій і здатна спрогнозувати ситуацію, коли підприємству доцільно перейти більш досконалу технологію. Автори застосували традиційні методи динамічного програмування під час розрахунку вартості інвестування. Зауважимо, що застосування динамічного програмування накладає обмеження через неможливість вирішення багатовимірної задачі інвестування в ІБ ОБІ. У [72] автор пропонує модель, що враховує підвищення ефективності інвестицій у КБ. Модель ураховує зниження невизначеності від очікуваної втрати через атаку і загального зниження рівня захищеності ОБІ. Проте, за визнанням автора, модель має обмеження. Це пов'язано з тим, що наявність заходів для зменшення потенційної шкоди внаслідок атаки безпосередньо залежить від технологічних інновацій в області КБ. А ці інновації можуть відбуватися в будь-який час. Відповідно, цей стохастичний вплив на КБ ОБІ може зрештою знизити ефект від інвестування та збільшити ризики для інвестора. У [73, 74] розглянуто моделі процесу інвестування в ІБ на основі розв'язання системи білінійних диференціальних рівнянь. Моделі спрямовані лише на економічні аспекти інвестування в ІБ та не враховують технологічні підходи до забезпечення захисту інформації та КБ ОБІ.

Таким чином, аналіз публікацій на тему дослідження показує, що зараз відсутні єдині підходи до питання оцінки ефективності заходів, спрямованих на забезпечення ІБ ОБІ в умовах невизначеності. На даний момент відсутня єдина загальновизнана модель, що дозволяє оцінити динамічні характеристики інвестиційних проєктів у сфері ІБ ОБІ. Така модель має брати до уваги як традиційні фінансові, так і технологічні, тимчасові, організаційні та інші параметри інвестиційного проєкту.

Резюмуючи вищевикладене, можна констатувати, що:

1) ефективність заходів, спрямованих на підвищення ступеня захищеності та ІБ ОБІ, не може бути дано лише на основі детермінованих оцінок;

2) ефективність заходів, спрямованих на підвищення захисту ОБІ та поліпшення його ІБ, вимагає залучення ймовірнісних характеристик. До таких можна, зокрема, віднести функцію розподілу показників запобігання внаслідок деструктивних дій зловмисників збитків для ОБІ [80].

У процесі розрахунку економічної ефективності від інвестицій в ІБ ОБІ, як правило, використовують дві змінні. Відповідно, отриманий у ході застосування коштів і заходів з ІБ результат приведений до фінансового показника. І відповідні витрати на кошти та заходи, які впроваджуються, щодо забезпечення ІБ [80].

Фактичним кінцевим результатом застосування коштів із забезпечення ІБ вважатиметься розмір (у грошовому еквіваленті) попереджених втрат (попередженого збитку від кібератак). Цей параметр можна формалізувати так:

$$D_i = D_i^{'} - D_i^{''}, \qquad (3.10)$$

де $D_i^{'}, D_i^{''} -$ збитки атак, відповідно до і після впровадження коштів та заходів щодо ІБ.

Фактично, розмір попередженої шкоди від кібератак відображає частку прибутку, недоотриманого, якщо не запровадити відповідні заходи щодо ІБ.

Тоді сумарний розмір попередженої шкоди від кібератак визначимо так:

$$P = \sum_{i=1}^{n} P_i + R_i, \qquad (3.11)$$

де R_i – величина фінансових ресурсів, що безпосередньо повертаються. До таких ресурсів можуть бути віднесені, наприклад, кошти від штрафних санкцій щодо співробітників, які порушили політику ІБ підприємства тощо.

Як показує практика [74–76], визначити реальний розмір попередженої шкоди від кібератак досить складно. Для цього необхідно мати реальну статистику щодо кіберінцидентів, а також у ряді ситуацій необхідно залучати експертів з ІБ. Зауважимо, що залучення експертів неминуче привносить в оцінку розміру попередженого збитку суб'єктивізм. І хоча експертні методи все частіше замінюються широким застосуванням інтелектуальних СППР у завданнях оцінки збитків та ризиків від атак, найбільш доцільним можна вважати об'єднання двох вище зазначених підходів у процесі прийняття рішення.

Використовуючи подібний комбінований підхід передбачається така послідовність дій для моделювання (наприклад, імітаційного) розміру попередженої шкоди від кібератак:

Крок 1. Розбиваємо потенційні втрати (збитки) на групи. Як критерій такого розбиття, можна застосовувати категорійний поділ інцидентів ІБ за ступенем небезпеки для ОБІ, застосовуючи типові метрики ІБ;

Крок 2. На підставі наявної статистики кіберинцидентів з ОБІ та використовуючи СППР або експертів виконуємо оцінку значення величини втрат (попередженої 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 та засобів ІБ);

Крок 4. Розрахувати сумарне значення попереджених збитків від кібератак на підставі попередніх кроків 1–3;

Крок 5. Розрахувати статистичні характеристики для змодельованих величин, а також результуючі показники економічної ефективності впроваджених засобів та проведених заходів щодо посилення ІБ ОБІ [80].

Для візуалізації результату розрахунку доцільно побудувати гістограму розподілу результуючого значення запобігання шкоди від кібератак або гістограму інтегрального відсотка розподілу попереджених збитків від кібератак.

Точний підбір закону розподілу сумарного результуючого значення попереджених збитків від кібератак дозволить досить точно оцінювати імовірнісні характеристики в будь-якому місці гістограми або щодо аналізованого інтервалу.

Таким чином, імовірнісна характеристика попередженої шкоди від кібератак може бути прийнята як обґрунтований критерій ефективності заходів, спрямованих на підвищення ІБ ОБІ.

Найбільш трудомістким завданням є визначення конкретних розмірів витрат на забезпечення ІБ ОБІ [80]. Зазначені витрати включають такі статті:

– утримання відділу ІБ ОБІ;

– витрати на закупівлю, експлуатацію, ремонт тощо апаратно-програмних ЗЗІ та ін.

Крім того, при розрахунку ефективності інвестування в ІБ ОБІ обов’язково слід урахувати важливість інформаційних активів у бізнес-процесах підприємства. Розрахувати цей параметр можна застосувавши таку залежність [75]:

$$S_j = C \diagup Y, \tag{3.12}$$

де S_j – важливість j-го інформаційного активу в бізнес процесах підприємства;

C – вартість j -го інформаційного активу;

Y – величина капіталу, вкладеного в експлуатацію j-го інформаційного актив [80].

Коли йдеться про оцінку ефективності того чи іншого ЗЗІ, слід брати до уваги і таку категорію параметрів, як ризики порушення ІБ ОБІ. Ризик може бути одиничним, суб'єктивним, сукупним [75].

Отже, кожен із цих видів ризику може бути обчислений так:

Поодинокий ризик (R_i):

$$R_i = p_i \cdot d_i, \tag{3.13}$$

де $p_i -$ ймовірність того, що зловмисник реалізує загрозу ІБ ОБІ;

$d_i -$шкода від i-ї загрози для ІБ ОБІ.

Суб'єктивний ризик (R_{sub}):

$$R_{sub} = {N_R}/{Y}, \tag{3.14}$$

де $N_R -$ сумарна кількість усіх ризиків;

$Y -$ кількість актуальних ризиків.

Сукупний ризик (Q):

$$Q = \sum_{i=1}^{n} R_i + R_{sub}, \tag{3.15}$$

де $n -$ загальна кількість кіберзагроз для ІБ ОБІ.

Як показує аналіз низки публікацій [76-78], більшість дослідників спрямовують оцінювання ризиків порушення ІБ за локальними ознаками. Якщо узагальнити дані публікації (див. таблицю 3.5), можна помітити, що переважно застосовуються такі моделі:

– Cost Benefit Analysis – CBA;

– Net Present Value – NPV;

– Profitability Index – PI;

– Internal Rate of Return – IRR та інші [78].

Таблиця 3.5

Моделі для оцінки витрат на ІБ ОБІ

№	Модель	Переваги	Недоліки
1	DCF	1. Комплексний підхід при оцінюванні витрат на ІБ. 2. Врахування всіх етапів життєвого циклу компонентів ЗЗІ, а також бізнес процесів підприємства.	Модель статична. Не враховує можливі зміни ситуації з ІБ, наприклад, у ході довготривалої атаки.
2	PI	1. Достатня корельованість моделі з типовими методами бухгалтерського обліку. 2. Простота та швидкість отримання результатів оцінки інвестування в ІБ.	1. Не береться до уваги інфляція. 2. Неадитивність.
3	NPV	1. Можливість урахування різної вартості ресурсів для підвищення ступеня ІБ ОБІ. 2. Взято до уваги позицію та інтереси інвестора.	1. Частину ресурсів неможливо оцінити у грошовому еквіваленті. 2. Прив’язка моделі до показників вартості підприємства.

Джерело: розроблено автором на основі [76-78]

На сьогодні найбільш популярні такі моделі для оцінки витрат на ІБ: NPV (Net Present Value) та DCF (Discounted Cash Flow). Не вдаючись детально в аналіз переваг і недоліків кожного із цих та інших методів та моделей (цьому питанню присвячено чимало публікацій, наприклад [78, 79]), зауважимо, що самі собою багато моделей орієнтовані лише на економічний аспект оцінки ефективності. Однак у контексті розв’язуваних у розділі дисертації завдань зауважимо, що залишаються дискусійними такі питання:

1) які саме витрати слід конкретно віднести до ІБ? Нині загальноприйнятих критеріїв немає:

2) сьогодні ІБ стала невід’ємним супутником практично всіх бізнес-процесів підприємств. Отже, багато компонентів забезпечення ІБ та кібербезпеки (наприклад, витрати на мережеві технології та розподілені обчислювальні системи

ОБІ) стали невід'ємною частиною бізнес-процесів підприємств. Звідси виникає нове питання. Яка частина інвестицій у розвиток ІТ підприємств спрямована саме на ІБ? А, наприклад, не на мережеві чи інші ІТ підприємства? Помилкова думка з цих питань у результаті може дати неправильну картину про частку інвестицій саме на ІБ. Вони лише частина загальних інвестицій підприємства в ІТ;

3) акцентування уваги лише на розмірі інвестицій в ІБ ОБІ перестав бути коректним. Більш пильна увага до цієї проблематики відразу покаже, що неможливо відкинути багато складових комплексу заходів, спрямованих на підвищення рівня ІБ ОБІ. Наприклад, до цієї статті видатків можуть бути віднесені тренінги спеціалістів відділу ІБ, а також підвищення кваліфікації з питань ІБ усіх працівників підприємства.

На нашу думку, саме викладена вище методика оцінки попереджених збитків від кібератак на основі базисного показника розрахунку економічного ефекту від інвестування у ЗЗІ дозволить усунути суперечливість у питанні оцінювання ефективності заходів, спрямованих на забезпечення ІБ ОБІ.

Отримані на підставі реалізації кроків 1-5 результати можна використовувати разом із будь-яким із методів (CBA, NPV, PI, IRR та ін.). Такий комбінований підхід дозволить власникам інформаційних ресурсів підприємства (ОБІ) із гарантійною ймовірністю отримати різні сценарії (від песимістичних до оптимістичних) результатів інвестування в ІБ ОБІ. При цьому основна обчислювальна робота може бути перекладена на інтелектуальні інформаційні системи, наприклад, СППР [80].

Розглянемо приклад варіанта оцінювання ефективності заходів, направлених на забезпечення ІБ ОБІ.

Нехай є проєкт підвищення ступеня ІБ ОБІ. У тестовому прикладі проєкт може включати наступні заходи (див. табл. 3.6).

Для розрахунку показників чистої приведеної вартості (NPV), індексу рентабельності (PI), внутрішньої норми прибутковості (IRR), модифікованої внутрішньої норми прибутковості (MIRR), дисконтованого терміну окупності проєкту (DPB) скористаємося наведеними у [54], а також формулами (3.10)–(3.15) у цьому підрозділі дисертації. Необхідно отримати результати для трьох сценарних

результатів розрахунку з метою прийняття обґрунтованого рішення щодо доцільності інвестування у проєкти ІБ [80].

Таблиця 3.6

Витрати та можливі надходження коштів
у результаті проведення заходів щодо підвищення ІБ ОБІ

Заходи щодо підвищення рівня ІБ ОБІ	Витрати, тис. у. о.	Надходження, тис. у.о.			
		Ум. познач.	Min (мінімальне)	Mid (найбільш вірогідне)	Max (максимальне)
M1 (технічні, наприклад, придбання нового фаєрволу)	65	P1	160	270	420
M2 (організаційні, наприклад тренінги для співробітників відділу ІБ)	35	P2	90	170	300
M3 (інші)	20	P3	50	100	190
Сума	**120**		**300**	**540**	**910**

Джерело: розроблено автором

Спочатку слід змоделювати обсяги потенційних надходжень у результаті впровадження СЗІ та відповідних заходів. Фактично ці показники відповідатимуть розміру попереджених збитків від кібератак.

Результати потенційних надходжень візуалізовані до СППР у вигляді гістограми, що характеризує підсумковий розподіл коштів від заходів М1–М3 (див. рис. 3.6).

Описову статистику підсумкового розподілу суми попереджених збитків від кібератак подамо в табличній формі. Наприклад, як показано в таблиці 3.7.

Результати моделювання для різних сценаріїв інвестиційного процесу в ІБ ОБІ для тестового прикладу наведено в таблиці 3.8 [80].

На фінальному етапі тестування за кожним із сценаріїв визначаємо показники ефективності проєкту підвищення ІБ. Результати зведено в таблиці 3.9 [80].

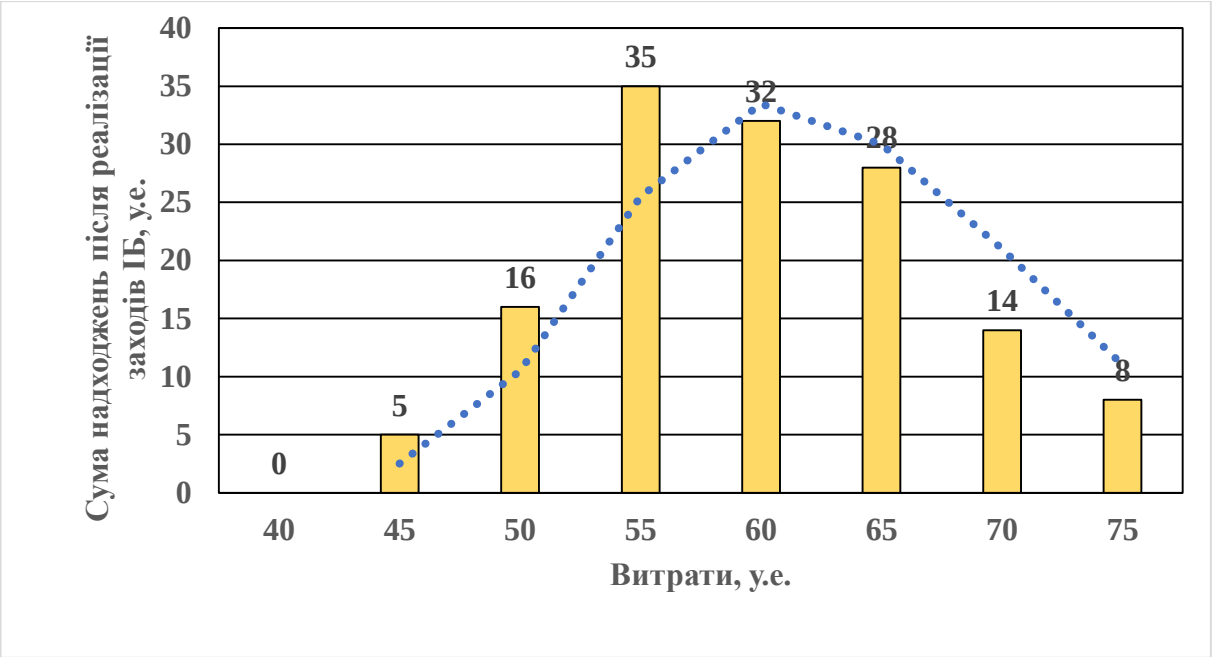


Рис. 3.6. Сумарний та середній розподіл можливих надходжень коштів від реалізації заходів (М1–М3), спрямованих на підвищення ІБ ОБІ

Джерело: розроблено автором

Таблиця 3.7

Результати розрахунку описової статистики для надходжень коштів у результаті проведених заходів щодо підвищення ІБ ОБІ

Показник	Позначення	Значення
Середнє значення	μ	33,9
Стандартна помилка	δ	0,74
Стандартне відхилення	σ	7,4
Дисперсія вибірки	Ω	470,2
Min значення	*Min*	5
Max значення	*Max*	35,1

Джерело: розроблено автором

Таблиця 3.8

Оцінка ефективності проєктів підвищення ІБ ОБІ для різних сценаріїв

Сценарії	Позначення	Надходження за період, тис. у. о.
Песимістичний	S_{pes}	31
Найбільш імовірний	S_{mp}	45
Оптимістичний	S_{op}	62

Джерело: розроблено автором

Таблиця 3.9

Показники ефективності ІТ-проєкту за сценаріями

Показник ефективності інвестиційного проєкту в ІБ ОБІ	Позначення параметра	Варіант сценарію		
		S_{pes}	S_{mp}	S_{op}
Індекс рентабельності	*PI*	0,85	1,2	1,11
Чиста приведена вартість	*NPV*	9,2	27,0	13,3
Модифікована внутрішня норма прибутковості	*MIIR*	0,12	0,18	0,17
Надходження, наведені на момент закінчення проєкту посилення ІБ ОБІ	*FPI*	189,0	196,0	161,3
Дисконтований термін окупності проєкту ІБ ОБІ	*DPB*	3,7	2,4	1,79
Витрати, наведені на момент часу $t = 0$	*PVO*	120	120	120
Внутрішня норма прибутковості проєкту ІБ ОБІ	*IIR*	0,14	0,22	0,18

Джерело: розроблено автором

Аналіз результатів розрахунків дозволив зробити такий висновок (для заданих вихідних даних). Усі сценарії, крім песимістичного, задовольняють умовам схвалення з боку керівництва підприємства проєкту з інвестування в ЗЗІ та заходи, спрямовані на підвищення рівня її ІБ.

Для того, щоб керівництву підприємства (компанії) ухвалити остаточне рішення щодо доцільності інвестування в ІБ, слід визначити близькість кожного з розглянутих сценаріїв до ідеального гіпотетичного проєкту. Це можна реалізувати, застосувавши, наприклад, такі метрики як Евклідова відстань або кореляція Пірсона. У такому разі необхідно виконати нормування показника чистої приведеної вартості (NPV) для відповідного сценарію. Нормування необхідно виконувати по відношенню до максимального значення. Ідеальним можна вважати проєкт інвестування в ІБ, якщо сценарій відповідає таким нормованим показникам: [80]

$$NPV = 2;\ \ PI = 2;\ \ MIRR = 1.$$

Зауважимо, що сьогодні в умовах ускладнення сценаріїв проведення кібератак на підприємства, їх менеджмент (особи, що приймають рішення – ОПР), усвідомлюють необхідність пошуку адекватних відповідей на зростання кіберзагроз. Однак у практичній діяльності не рідкісна ситуація, коли підприємство та його керівництво має обмеження щодо коштів, які вони готові вкласти в підвищення рівня ІБ. Це частково пов’язано з тим, що збільшення прибутку підприємства внаслідок підвищення рівня ІБ менш очевидне, як, наприклад, інвестування в нові виробничі засоби чи маркетинг. Тому всі переваги інвестицій в ІБ ОБІ можна показати лише, підкріплюючи вербальні та логічні аргументи результатами розрахунків та імітаційного моделювання. Акцент на віддачі від інвестування в ІБ підприємства необхідно робити, насамперед, отримавши дані модельних досліджень і маючи переконливу статистику інцидентів по КБ, які могли призвести (або вже призвели) до фінансових, репутаційних та інших втрат для підприємства.

Висновки до розділу 3

У третьому розділі роботи отримано такі основні результати:

1. Запропоновано підхід до процедури формалізації ознакового функціонального подання неправомірних дій комп'ютерного зловмисника у ході реалізації функцій НСД до ресурсів ІС підприємств.

2. Виконано формалізацію ієрархічної схеми формування простору ознак НСД до ресурсів ІС підприємства. Отримана ієрархічна структура є основою для подальшого синтезу інтелектуальної системи виявлення спроб НСД в умовах важкозрозумілих ознак або їх невеликого числа. Це дозволяє ефективно реалізувати первинну формалізацію неправомірних дій комп'ютерних зловмисників для подальшого математичного опису параметра ймовірності НСД, наприклад, на основі Марківських ланцюгів.

3. Конкретизація багатофакторного характеру реалізацій функцій НСД до інформаційних ресурсів ІС заснована на Марківському ланцюзі. Розглянуто варіант, у якому представлення ознак НСД виходить із побудови комбінаційної функціональної моделі неправомірних дій порушника інформаційної безпеки.

4. Запропоновано методологічний підхід, що дозволяє автоматизувати та систематизувати прояви ефекту захищеності інформації від витоків по технічних каналах. Доповнено імовірнісну модель виконання загроз, яка дозволяє на основі запропонованого програмного забезпечення (ПЗ) 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 оцінки ризиків втрати інформації, дозволяє комплексно оцінити рівень захищеності ТКПІ підприємства. Розроблене ПЗ сприяє зниженню витрат на проведення вузькоспеціальних досліджень у питаннях щодо оцінки актуальності загроз витоку інформації з ТКПІ в умовах динамічного вдосконалення ТЗР. Таким чином, було досягнуто основної мети даного розділу дисертації – автоматизувати процедуру оцінки актуальності загроз витоку інформації з ТКПІ в умовах

динамічного вдосконалення ТЗР та вдосконалити процес оцінювання захищеності приміщень підприємств шляхом використання релевантних оцінок експертів.

5. Запропоновано методику розрахунку показників ефективності інвестиційних заходів у межах підвищення метрик ІБ ОБІ. Описано конкретний приклад імітаційного моделювання. У запропонованій методиці передбачено оцінку попереджених збитків від кібератаки. Як основу для розрахунку економічного ефекту від інвестування в СЗІ прийнято розмір попередженого збитку від кібератаки.

6. Розрахунок ефективності інвестування в конкретний процес ІБ ОБІ показано засобами імітаційного моделювання. За рахунок цього було показано яким чином враховується відносна невизначеність реальної ситуації з ІБ ОБІ. Показано, що проведені дослідження допоможуть практикам у сфері ІБ отримувати з допомогою викладеного в роботі підходу обґрунтовані рішення підвищення ефективності інвестиційних проєктів у сфері ІБ для ОБІ. Дана методика в умовах сьогодення є єдиною, яка враховує прямі та непрямі фактори інвестиційних проєктів.

Основні результати розділу опубліковані в наукових працях автора: [1, 9, 19, 20, 21, 25, 26, 28, 32, 35, 36] – відповідно до списку опублікованих праць за темою дисертації на початку роботи.

Список використаних джерел до розділу 3

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 // The Oxford Handbook of Cyberpsychology. Oxford University Press,

2018. URL: https://www.researchgate.net/publication/328763267_The_Group_Element_of_Cybercrime_Types_Dynamics_and_Criminal_Operations (date of access: 15.07.2022).

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 [Electronic resource]. 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. Vol. 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. 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.
30. 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.

31. Razumov P. V., Zelensky A. A., Cherckesova L. V., Safary-an 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.
32. Конахович Г. Ф., Назаренко Є. Л., Свириденко В. М. Захист інформації від витоку по технічних каналах // Наукоємні технології. 2009. № 2(2). С. 90–93.
33. 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.
34. 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.
35. 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.
36. 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.
37. Kirda E., Kruegel C., Banks G., Vigna G., Kemmerer R. Behavior-based Spyware Detection // In Usenix Security Symposium (2006, August). 694 p.
38. 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.
39. 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.

40. 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.
41. 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.
42. 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.
43. 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.
44. Schiavone S., Garg L., Summers K. Ontology of information security in enterprises // Electronic Journal of Information Systems Evaluation. 2014. № 17(1). P. 71–87.
45. 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.
46. 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.
47. 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.
48. Хлапонін Ю. І. Неоднозначність трактування та протиріччя деяких визначень в нормативних документах системи технічного захисту інформації // Сучасний захист інформації. 2015. № 4. С. 104–109.

49. Олашин М. М., Гапяк С. С. Кримінальні процесуальні аспекти зняття інформації з електронних інформаційних систем // Вісник ЛТЕУ. Юридичні науки. 2018. № 7. С. 233–242.
50. Дудикевич В. Б., Микитін 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.
51. 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.
52. 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. P. 9–16.
53. 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.
54. Chronopoulos M., Panaousis E., Grossklags J. An options approach to cybersecurity investment // IEEE Access. 2017. № 6. P. 12175-12186.
55. 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. Vol. 11. № 2. P. 91–112.
56. Nagurney A., Shukla S. Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability // European Journal of Operational Research. 2017. Vol. 260. № 2. P. 588–600.
57. 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.
58. 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.

59. Maqbool Z., Pammi V. C., Dutt V. Behavioral Cybersecurity: Investigating the influence of Patching Vulnerabilities in Markov Security Games via Cognitive Modeling // IJCSA. 2019. № 4(1). P. 185–209.
60. Gordon L., Loeb M., Lucyshyn W. Information security expenditures and real options: A wait-and-see approach // Computer Security Journal. 2003. Vol. 19. № 2. P. 1–7.
61. Majd S, Pindyck R. Time to build, option value, and investment decisions // Journal of Financial Economics. 1987. Vol. 18. № 1. P. 7–27.
62. Malchow-Muller N., Thorsen B. Repeated real options: Optimal investment behaviour and a good rule of thumb // Journal of Economic Dynamics and Control. 2005. Vol. 29. № 6. P. 1025-1041.
63. Grenadier S., Weiss A. Investment in technological innovations: An option pricing approach // Journal of Financial Economics. 1997. Vol. 44. № 3. P. 397–416.
64. Farzin H., Huisman K., Kort P. Optimal timing of technology adoption // Journal of Economic Dynamics and Control. 1998. Vol. 22. № 5. P. 779–799.
65. Huisman K., Kort P. Strategic technology adoption taking into account future technological improvements: A real options approach // European Journal of Operational Research. 2004. Vol. 159. № 3. P. 705–728.
66. Gordon L., Loeb M., Lucyshyn W., Zhou L. The impact of information sharing on cybersecurity underinvestment: A real options perspective" // Journal of Accounting and Public Policy. 2015. Vol. 34. № 5. P. 509–519.
67. Daneva M. Applying real options thinking to information security in networked organizations. Centre for Telematics and Information Technology, University of Twente, Tech. Rep., 2006. P. 1–12.
68. Herath H., Herath T. Investments in information security: A real options perspective with Bayesian postaudit // Journal of Management Information Systems. 2008. Vol. 25. № 3. P. 337–375.
69. Benaroch M., Shah S., Jeffery M. On the valuation of multistage information technology investments embedding nested real options // Journal of Management Information Systems. 2006. Vol. 23. № 1. P. 239–261.

70. Herath H., Park C. Multi-stage capital investment opportunities as compound real options // The Engineering Economist. 2002. Vol. 47. № 1. P. 1–27.
71. Khansa L., Liginlal D. Valuing the flexibility of investing in security process innovations // European Journal of Operational Research. 2009. Vol. 192. № 1. P. 216–235.
72. Benaroch M. Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making // Information Systems Research. 2018. Vol. 29. № 2. P. 315–340.
73. Lakhno V., Malyukov V., Gerasymchuk N., Shtuler I. Development of the decision making support system to control a procedure of financial investment // Eastern-European Journal of Enterprise Technologies. 2017. Vol. 6. № 3. P. 35–41.
74. Akhmetov B. B., Lakhno V. A., Akhmetov B. S., Malyukov V. P. (2018). The Choice of Protection Strategies During the Bilinear Quality Game On Cyber Security Financing // Bulletin of The National Academy of Sciences of the Republic of Kazakhstan. 2018. № 3. P. 6–14.
75. Рабчун Д. І. Оцінка ефективності інформаційної безпеки з урахуванням економічних показників // Сучасний захист інформації. 2015. № 4. P. 91–96.
76. Shameli-Sendi A., Aghababaei-Barzegar R., Cheriet M. Taxonomy of information security risk assessment (ISRA) // Computers & security. 2016. № 57. P. 14–30.
77. Behnia A., Abd Rashid R., Chaudhry J. A. A survey of information security risk analysis methods // SmartCR. 2012. № 2(1). P. 79–94.
78. Cherdantseva Y., Burnap P., Blyth A., Eden P., Jones K., Soulsby H., Stoddart K. A review of cyber security risk assessment methods for SCADA systems // Computers & security. 2016. № 56. P. 1–27.
79. Wangen G. Information security risk assessment: a method comparison // Computer. 2017. Vol. 50. № 4. P. 52–61.
80. Чубаєвський В.І. Стратегічні орієнтири формування корпоративної політики інформаційної безпеки. Причорноморські економічні студії (72) 2021. https://doi.org/10.32843/bses.72-28

РОЗДІЛ 4
ЕКОНОМІЧНА ДІАГНОСТИКА СИСТЕМ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ

4.1. Оцінка інформаційної безпеки в Україні та світі

В умовах Четвертої промислової революції стрімкими темпами стався розвиток та збільшення масштабів застосування інформаційно-комунікаційних технологій (ІКТ) та систем. Сучасні суб'єкти господарської діяльності, починаючи з великих транснаціональних компаній і закінчуючи невеликими підприємствами, не можуть обійтися у своїх бізнес-процесах без застосування наскрізних ІКТ. Інтеграція ІКТ та інформаційних систем (ІС) у бізнес-процеси компаній дала різноплановий ефект. З одного боку, їх широке застосування сприяло оптимізації виробничих відносин, раціоналізації системи управління, істотного скорочення витрат на логістику та ін. З іншого боку, ІКТ та ІС підприємств стали об'єктом для деструктивних впливів на бізнеспроцеси підприємств. Причому тут тактика та стратегія комп'ютерних зловмисників постійно вдосконалюється. І сьогодні «банальним» розкраданням інформації на змінних носіях здивувати будь-кого складно.

Ландшафт кібернетичних загроз мінливий. На нього впливають багато зовнішніх факторів. Наприклад, такий: хто б із фахівців наприкінці 2018 р. або на початку 2019 р. міг спрогнозувати як буде змінено ландшафт кібернетичних загроз із початком пандемії Covid-19?

Ландшафт загроз кібербезпеці, що існував наприкінці 2018 р., був повністю порушений через пандемію Covid-19 на початку 2020 року. Пандемія Covid-19, починаючи з 2020 р., стала не тільки центральною темою засобів масової інформації, але й призвела до серйозних змін на ринку ІКТ. Останнє ґрунтовно, зокрема, сприяло сплеску інтересу бізнесу до хмарних сервісів та технологій, коли велика кількість підприємців адаптувала свої бізнес-процеси під нові реалії.

Слідом за переходом людей та бізнесу на онлайн сервіси та хмарні технології, активізувалися і кіберзлочинці, оперативно перебудовуючи свою тактику.

Недоліки ІБ можуть дорого обійтися комерційним та некомерційним організаціям, а також пересічним користувачам. Йдеться як про втрату часткових чи повних важливих інформаційних ресурсів (ІР), так і про фінансові та репутаційні втрати. Відповідні статистичні дані наведено на рисунках 4.1 та 4.2.

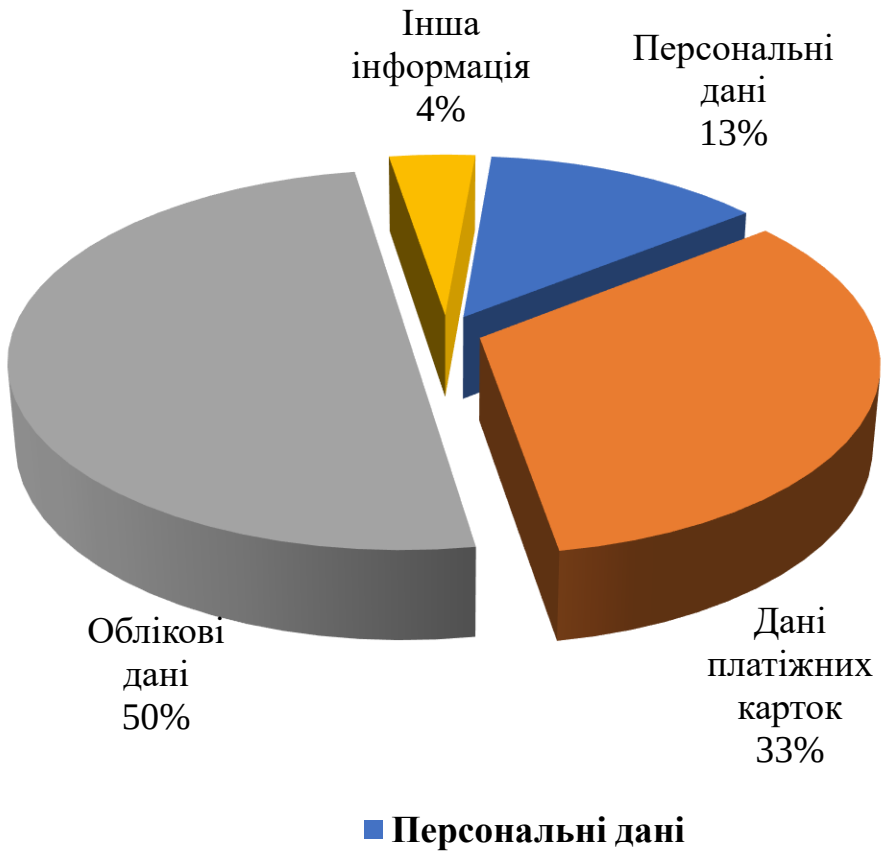


Рис. 4.1. Типи вкрадених даних у результаті кібератак на приватних осіб (2019 - 2021 роки)

Джерело: [1–3]

За статистикою [1, 2] близько половини кібератак націлені па приватних осіб та підприємства, що працюють у сфері малого бізнесу. При цьому невеликі підприємства, не кажучи вже про приватних підприємців, не мають достатніх ресурсів, щоб убезпечити себе від серйозних атак та загроз. Згідно з опитуваннями аналітиків, у сфері ІБ у період із 2018 по 2021 роки найбільше занепокоєння в

невеликих підприємствах викликали фішинг та вторгнення в мережі компаній із боку хакерів.

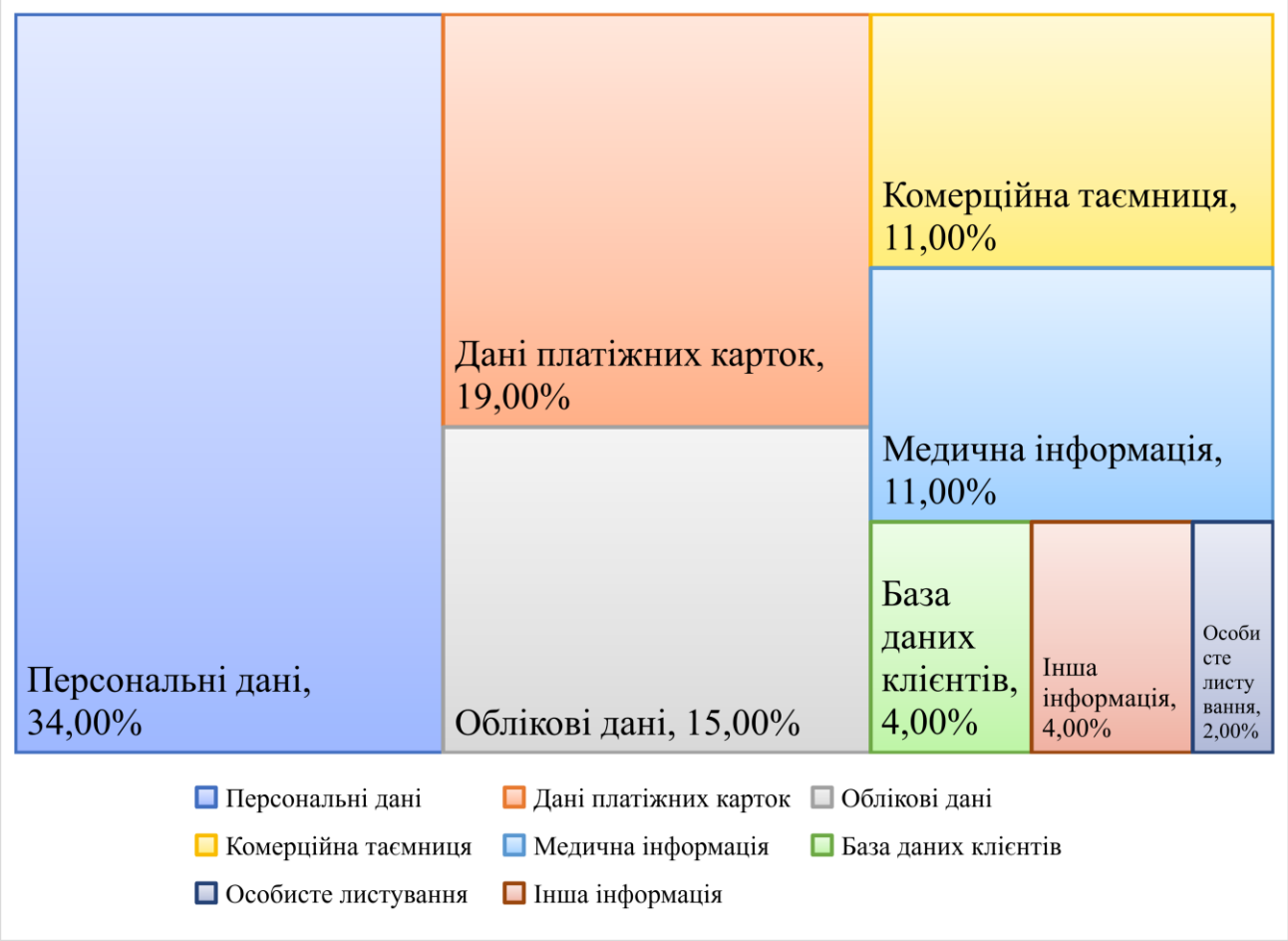


Рис. 4.2. Типи вкрадених даних в результаті кібератак на юридичних осіб (2019-2021 р.)

Джерело: [1–3]

Низка підприємств також зіткнулася з наслідками DoS атак або стали жертвами цілеспрямованих (таргетованих атак). На ці типи складних атак звертають увагу, насамперед, системні адміністратори або фахівці з ІБ компанії, див. 4.4.

У міру підвищення рівня обізнаності менеджменту компаній, у тому числі малого бізнесу, про кібернетичні загрози керівництво компаній та організацій стало приділяти питанням ІБ дедалі більше уваги. Цьому сприяло збільшення агресивності і частоти проведення кібератак, вкладених у господарську діяльність.

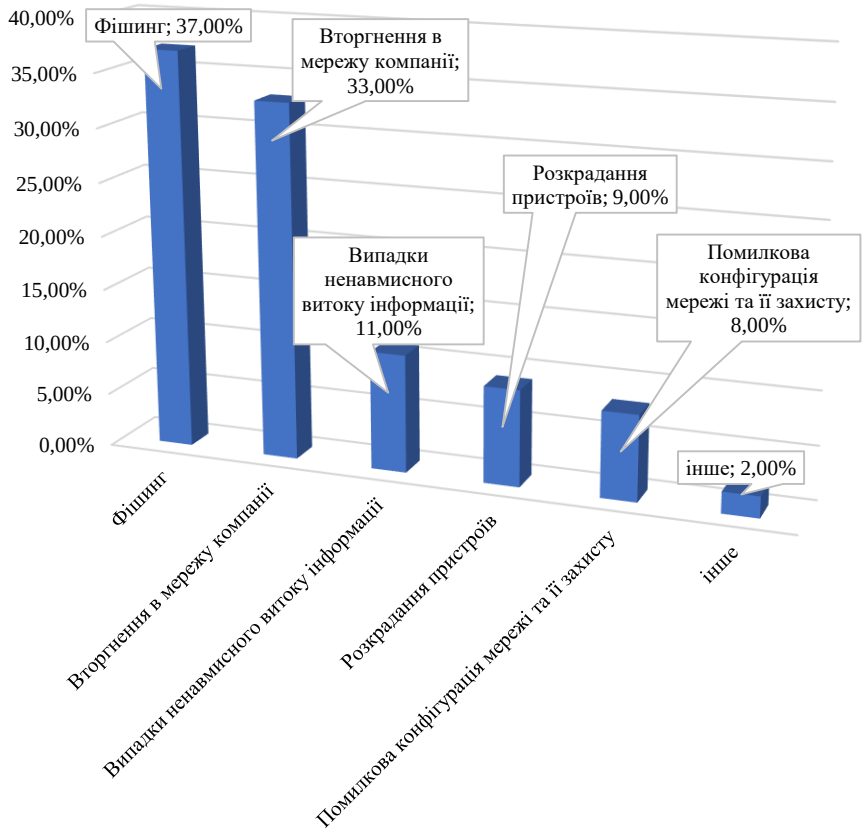


Рис. 4.3. Найбільш поширені типи кібератак, із якими стикаються невеликі підприємства

Джерело: [1–3]

У ситуації, що склалася для більшості компаній і приватних підприємців, поінформованість про кібернетичні загрози та заходи щодо забезпечення ІБ стали мати важливе значення. Ці загрози активізували зусилля фахівців та менеджменту компаній та організацій щодо запобігання витоку інформаційних ресурсів та недопущення зламів мережі або пристроїв співробітників.

Однак, незважаючи на цю поінформованість персоналу та менеджменту компаній про кібернетичні загрози, ситуація далека від ідеальної. Так, за даними досліджень ISACA [4], переважна кількість людей не знають деталей проведення сучасних кібератак. У звітах Infosec [6] зазначено, що 97 % людей не можуть ідентифікувати фішингові електронні листи. Приблизно 4 % стають жертвами переходу за посиланнями, зазначеними в таких листах. При цьому хакери

знаходять нові способи і високотехнологічні способи зацікавити людину відкрити таке посилання в листі.

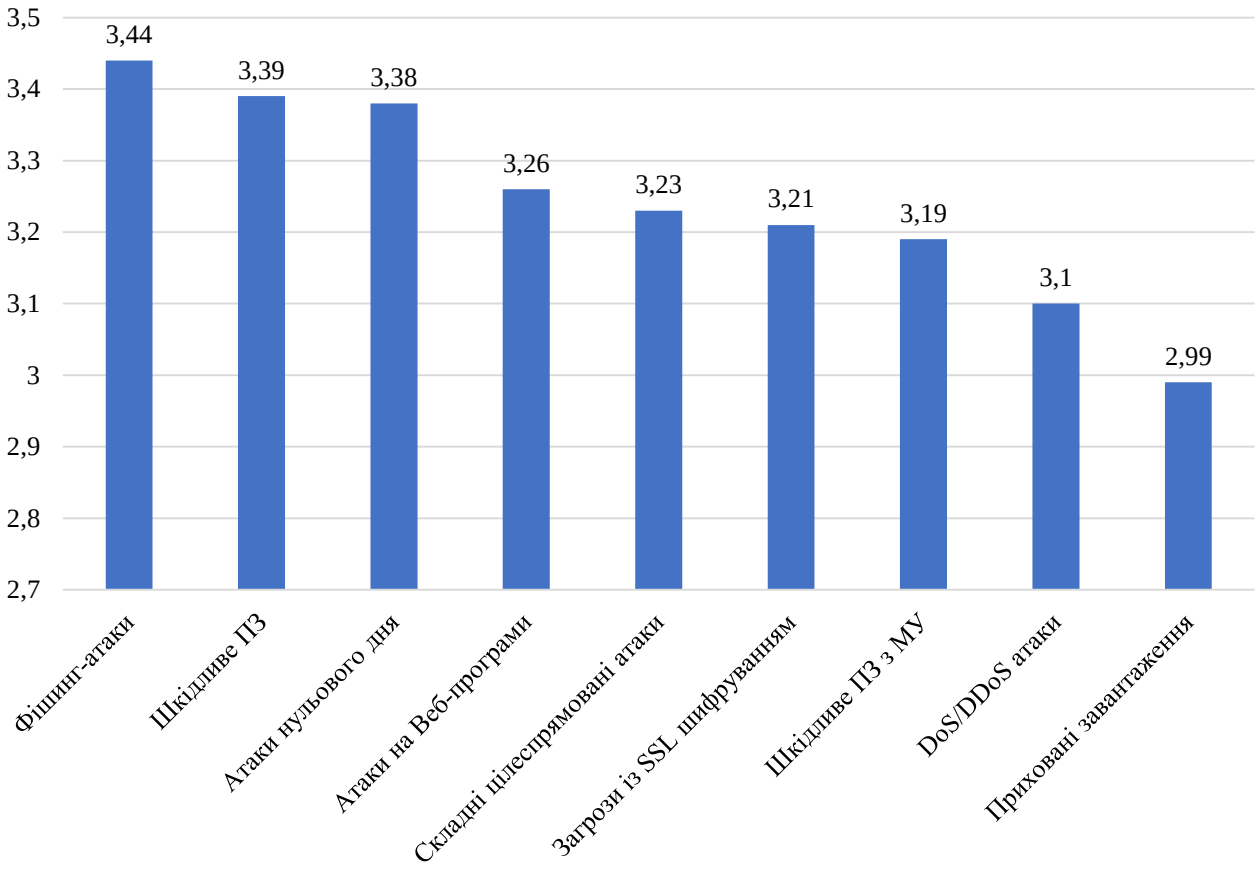


Рис. 4.4. Рівень стурбованості менеджменту компаній та підприємств кібернетичними загрозами (на кшталт атак) у 2019–2021 р.

Джерело: [1–4]

Як відповідь на загрози ІБ, багато підприємств активно впроваджують практики навчання персоналу діям при кібератаках [4–6]. Комбінування веб- та аудиторних методів, а також застосування наочних посібників під час занять дозволило дещо покращити поінформованість персоналу з правилами обробки конфіденційних корпоративних даних, а також обміну такими даними.

Якщо аналізувати галузеву прив’язку атак за типами суб’єктів господарської діяльності, ситуація динамічно змінюється. Відсоткове співвідношення розподілу кількості атак за типами установ та видами підприємств не є стабільним. На цей відсотковий розподіл великий вплив за останні кілька років справила пандемія

коронавірусу Covid-19. Проте загалом «лідером» серед жертв атак, зокрема й в Україні, залишаються державні установи (від 19 % до 23 % за різними джерелами, а також залежно від країни [5]). Далі йдуть промислові підприємства (приблизно 10 %). Останніми роками зловмисники активно атакують медичні установи (від 9 до 10 %). Гістограму розподілу показників атак по секторам економіки наведено на рис. 4.5.

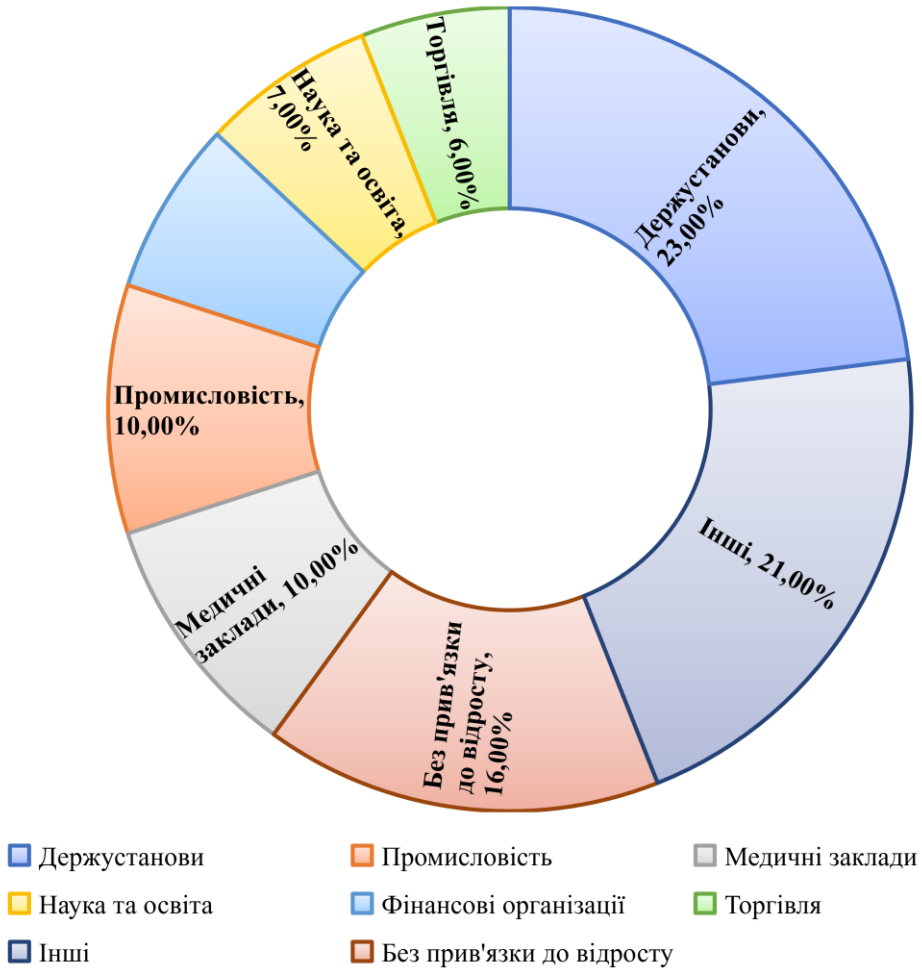


Рис. 4.5. Статистичні дані щодо секторального розподілу атак у 2019–2021 р.

Джерело: [4, 6]

Зміна цільової спрямованості атак є наслідком якісної диверсифікації та функціональної диференціації атак хакерів у всьому світі. Наслідком якісної диверсифікації стало виникнення нового типу як шкідливого, так і шпигунського програмного забезпечення (ПО). Це шкідливе і шпигунське ПО все більшою мірою

орієнтовано не скільки на крадіжку даних користувачів (наприклад, логіни, паролі, особисту інформацію та ін), скільки на потенційне знищення заражених систем. Нове покоління шкідливого ПЗ у ряді випадків здатне вирішувати такі відносно нові завдання, як, наприклад, майнінг криптовалют, чого не спостерігалося ще 4-5 років тому.

Ряд дослідників [7–13] відзначає і таку тенденцію як збільшення кількості та складності архітектурних рішень програм здирників. У [13] проаналізовано програми, які орієнтовані на використання нових способів монетизації ресурсу, що зазнав злому. Наприклад, наслідком такої монетизації може стати несанкціоноване дистанційне приєднання до зламаних комп'ютерів або інших цифрових гаджетів для подальшого залучення в майнінгу.

Аналітики у сфері ІБ відзначають [8, 9] і таку тенденцію як стрімке зниження порогу для початку діяльності хакера. Це пов'язано, не в останню чергу, з тим, що зросла пропозиція і збільшився попит на специфічному ринку шкідливого ПЗ. Сьогодні початківцю хакеру не обов'язково мати високу кваліфікацію для початку протиправної діяльності, а достатньо купити на відносно невеликі гроші шкідливе ПЗ, відповідні інструкції в сегменті DarkNet (тіньовий Інтернет).

Якщо говорити про функціональну диференціацію атак, то тут складається така ситуація. Насамперед, йдеться про кримінальну спеціалізацію хакерських угруповань. Багато подібних угруповань [12] спеціалізуються на проведенні цільових атак, причому ці атаки спочатку плануються як багатоетапні, що, у свою чергу, викликає розподіл ролей у групі хакерів і породжує нові спеціалізації, наприклад, фішери, розробники вірусного ПЗ, заливники, дидосери та ін.

Постійно змінюється тактика хакерів. Сьогодні не рідкість, коли зловмисники використовують складні, багатоетапні техніки зламу. Такі техніки, наприклад, на перших етапах передбачають зараження ресурсів відомих виробників ПЗ. Як це, наприклад, сталося під час поширення вірусу «NotPetya» [14].

Зміна ситуації у світі, пов'язана з пандемією коронавірусу Covid-19, і, відповідно, перехід університетів на дистанційні формати навчання викликали

досить активний інтерес хакерів до цього сегменту. Наприклад, за даними [15] тільки в період 2020-2021 років жертвами кібератак стали три приватні американські університети. Інциденти були пов’язані зі зломом бази даних, що містять інформацію про вступників до університету (абітурієнтів) і зарахованих студентів [15]. Як реакція у відповідь на подібні випадки злому стало активне впровадження американськими університетами суворіших заходів щодо захисту даних студентів та викладачів.

На жаль, подібної статистики по Україні немає, але можна припустити, що подібні інциденти можливі і для вітчизняних університетів.

У міру зростання ринку пристроїв інтернету речей (IoT) хакери звернули свої погляди на цей «перспективний» і поки що недостатньо захищений сегмент ринку. Це створює досить серйозні загрози безпеці для користувачів. Уже неодноразово фіксувалися випадки кібератак на пристрої IoT [16, 17]. Наприклад, у 2018-2021 роках сталося одразу кілька випадків DoS за допомогою пристроїв IoT. Наприклад, аналітичні звіти компанії Symantec показують, що на заражені маршрутизатори припадало 75 % усіх атак IoT, що відбулися у 2018 році.

На думку [17], пристрої IoT відкривають великі можливості як для бізнесу, так і для кіберзлочинців.

Ще одна галузь, яка привертає пильну увагу зловмисників – це сектор фінансових послуг. Ця галузь стикається з кіберзагрозами щодня. Причому, як зазначає ряд дослідників, у цьому випадку не допомагає навіть той факт, що багато фінансових організацій активно працюють над проблемами кібербезпеки, і намагаються слідувати тренду на переведення бізнес-процесів у хмарні структури та збільшують кількість правил ІБ. Згадані вище фішингові атаки, як і раніше, досить поширені в секторі фінансових послуг. Але зловмисники оперативно переорієнтувалися з розсилки фішингових листів через електронну пошту на технології фішингових атак через соціальні мережі та інші платформи обміну повідомленнями.

Фінансові організації по всьому світу [15] зіткнулися не лише із загрозою атак фішингу. Фахівцям з ІБ, які працюють у даному секторі економіки (це банки,

страхові компанії, компанії з управління активами тощо) доводиться відображати і безліч атак, що відбуваються за допомогою зараження ПК та гаджетів співробітників шкідливим та/або шпигунським ПЗ.

Аналітика провідних компаній у сфері ІБ, а також багато фахівців [18–21] уже порівнюють фінансові збитки від кібератак із ВВП великих держав. Наприклад, за даними компанії Cybersecurity Ventures [19], глобальні витрати від кіберзлочинності зростають із жахливими темпами – до 15 % на рік. Кіберзлочинність і, насамперед, цільові кібератаки призвели до того, що сумнівається інноваційна стратегія розвитку компаній. Адже умовним конкурентам чи іншим зловмисникам фінансово вигідніше витратити зусилля на реалізацію кібератак руками хакерів, ніж розвивати свої технології та інновації.

Свою лепту в ці процеси привнесла і пандемія Covid-19. Вона надихнула велику кількість онлайн-шахраїв, що наживаються на страхах споживачів та бізнесу. А масова міграція офісних співробітників на віддалену роботу – ідеальні умови для проведення фішингових атак. Підприємства та організації в усьому світі, як правило, будують стратегії своєї кібербезпеки, ґрунтуючись на оцінці ризиків, з якими ці підприємства чи організації можуть стикатися в кіберпросторі. Тому, ці підприємства та організації повинні мати чіткий план, як вони діятимуть реально, зіткнувшись із ризиковою ситуацією. На основі цих оцінок ризиків, а також операційних атрибутів підприємства або організації фахівці в галузі ІБ створюють відповідні програми захисту від кіберзагроз. Такі програми захисту включають концепції, інформаційні технології, відповідний персонал, методології, плани реагування на інциденти та багато іншого.

Слід зазначити, що за умов так званих кібервійн [22, 23] не всі кібератаки призводять до крадіжки фінансових ресурсів безпосередньо. Усе частіше фахівці з ІБ стикаються з атаками так званих програм-здирників. Фактично жертві пропонується нескладний вибір – або натрапити на ризик втрати своєї інформації (часто конфіденційної), або заплатити злочинцям, щоб знову отримати доступ до своїх даних. За даними [15, 18], середня атака програм-здирників виводить ІС компанії з ладу приблизно на 18 годин. З вірусом «NotPetya» цей часовий інтервал

часом сягав кількох днів. Такого часу більш ніж достатньо, щоб вплинути на бізнес процеси і призвести до серйозних наслідків для продуктивності підприємства.

За даними [21], витрати на переривання роботи компанії та усунення негативних наслідків можуть бути в 5–100 разів більшими ніж вартість самого викупу за зняття блокування з комп'ютерів, заражених програмою-здирником. У таблиці 4.1 показано прогнозну оцінку розподілів збитків від кібератак, складену за даними американських аналітиків.

Таблиця 4.1

Прогнозна оцінка розподілу збитків від кібератак, доларів США

Період	Сума збитків
Рік	41 368 320 000 000
Місяць	3 447 360 000 000
Тиждень	114 912 000 000
День	16 416 000 000
Час	684 000 000
Хвилина	11 400 000
Секунда	190 000

Джерело: [18]

Актуальною залишається проблема дефіциту фахівців з ІБ (зауважимо, що ця проблема актуальна не тільки для України, але й для розвинених держав – США, країни ЄС та ін.). Багато підприємств, зіткнувшись із нестачею фахівців у сфері кіберзахисту, починають вирішувати цю проблему за рахунок упровадження відповідного інтелектуального ПЗ. Сучасні інтелектуальні системи ІБ будуються за принципами машинного навчання (штучного інтелекту). Найчастіше такі інтелектуальні системи успішно справляються із завданнями виявлення кібер-зловмисників. Подібного роду системи навчаються на великих наборах даних, зібраних протягом кількох десятиліть. Системи можуть аналізувати терабайти

даних протягом дня, що очевидно неможливо для навіть високо кваліфікованої команди фахівців у сфері ІБ.

У середньому для розвинених країн світу, за даними [15-21], збитки, завдані підприємствам унаслідок зовнішніх інцидентів ІБ, наприклад, таких як розподілені атаки типу «відмова в обслуговуванні» (DDoS) та програм-вимагачів, становлять близько 81 % за останні шість років.

Зростання залежності від цифрових технологій, сплеск віддаленої роботи в період пандемії Covid-19 та обмежені розміри бюджету на ІБ – це лише деякі з причин, з яких уразливість у сфері ІТ посилилася.

Крім того, ширше поширення криптовалют, таких як біткойн, які дозволяють здійснювати анонімні платежі, стало ще одним ключовим фактором зростання кількості випадків застосування зловмисниками програм-вимагачів.

Біткойн, на який, за оцінками [24], припадає близько 98 % платежів програм-вимагачів, відносно легко придбати та використовувати для таких операцій. Це з тим, що злочинці і жертва можуть проводити транзакції анонімно, що у свою чергу, дозволяє злочинцям приховувати особистість.

Однак, незважаючи на всі ці виклики, за даними [25, 26], багато підприємств і організацій, як і раніше, заявляють, що у них немає довгострокових планів як щодо запобігання кіберинцидентам, так і реагування на них. Водночас лише третина підприємств, які мали плани щодо розвитку інфраструктури ІБ, заявили, що їх плани ефективні.

Прискорена цифрова трансформація української економіки, масштабне впровадження КІС та IoT зробили більшість бізнес-процесів уразливими перед деструктивними впливами з боку комп’ютерних зловмисників. У міру того, як цей трансформаційний шлях української економіки продовжується, стало життєво важливим, щоб фінансові ризики, пов’язані з кіберінцидентами, ураховувалися менеджментом компаній як пріоритетний фактор при плануванні заходів щодо забезпечення безперервності бізнесу.

Коли всі «прості» напрямки кібератак уже охоплені кіберзлочинцями, наступні атаки стають все більш витонченими та складними. Однак, чим

складніший сценарій реалізації атаки, тим складніше кіберзлочинцям, що стоять за нею, знайти і реально побудувати «ефективний» механізм реалізації подібної атаки. Після того, як новий вид атаки виявлено та системи захисту інформації можуть його заблокувати, цикл починається спочатку. Власне, чим ефективніші системи захисту, тим дорожче обходиться кіберзлочинцям пошук нових методів чи способів обходу СЗІ. Однак це не означає, що сторона захисту може почуватися спокійно, розгорнувши в компанії багатоконтурний захист. Багато аналітиків у сфері ІБ пропонують діяти на випередження. Наприклад, [27] запропоновано стороні захисту проводити активну компанію з дезінформації зловмисників, щоб останні були впевнені, що їх атаки були успішними або невиявленими. У той же час сторона захисту може фактично збирати інформацію для виявлення винних.

Як показують численні дослідження в області ІБ та КБ ОБІ, зростання обсягів та вартості інформації призводять до відповідного ускладнення СЗІ. Сучасні СЗІ стають багаторівневими та багатоконтурними [28].

Зростання вартості СЗІ актуалізує проблему оптимального використання ресурсів захисту. У процесі пошуку рішень слід ураховувати зміну умов протистояння з стороною атакуючої в часі. Це пов’язано зі «старінням» інформаційних ресурсів, їх оновленням, появою нових засобів нападу, модернізацією СЗІ тощо.

Вирішення практично будь-яких завдань у сфері забезпечення ІБ великих об’єктів інформатизації (ОБІ) стикається з організаційними та технологічними складнощами. Якщо ОБІ має складну архітектуру та топологію мережі, з безліччю вузлів, то розробникам мимоволі доводиться вирішувати складні оптимізаційні завдання. Більше того ці завдання не просто однопараметричні. Побудова ефективних контурів ІБ великого ОБІ потребує вирішення багатокритеріальної оптимізаційної задачі. А розв’язання таких завдань, у свою чергу, передбачає або варіант залучення математиків, або як альтернативний варіант задіяння потенціалу інтелектуальних інформаційних систем (ІІС) [29, 30]. У таких системах аналіз варіантів вирішення та інші рутинні операції перекладаються на плечі обчислювального ядра ІІС. Особливо пошук оптимальних чи раціональних

варіантів рішень утруднений для слабоструктурованих завдань. До подібних завдань можна віднести і завдання щодо підбору варіантів та оцінки потенціалу рішень у галузі побудови багатоконтурних систем ІБ.

Визначення конкретного ефективного рішення вимагає від особи, що приймає рішення (ОПР) оцінювати як технічні характеристики аналізованого варіанта, а й вирішувати паралельно інші завдання. До таких завдань відносяться завдання, пов’язані з оцінюванням комерційного потенціалу відібраного варіанта рішення, його ресурсної складової та ін. Таким чином, на підставі вищезазначеного, можна припустити таке – частково пошук раціональних варіантів рішення доцільніше перекласти на плечі ІІС. Проте це необхідно на першому етапі побудови, використовуючи наявну в експертів сукупність формалізованих і описаних знань у конкретній предметній області, чіткий алгоритм підтримки прийняття рішення. Наприклад, як в проаналізованому випадку стосовно вибудовування ефективної багатоконтурної системи ІБ ОБІ.

Успішне функціонування ІІС припускає, що при її експлуатації враховуватимуться не тільки вже наявні дані. Але, апріорі, існує можливість перетворювати інформацію на форми, які дозволяють ефективно виконувати оцінку наявних ситуацій, що стосуються ступеня захищеності ОБІ. А також за необхідності ІІС має видавати рекомендаційні рішення.

На початкових стадіях проєктування ІІС, наприклад у галузі ІБ, надзвичайно важливо отримати структуровані знання експертів. Сукупність таких експертних знань сформує поле знань (ПлЗ). Фактично ПлЗ визначатиме в різних форматах неформальні описи основних понять. Така робота виконується для кожної предметної області. Наприклад, для такої предметної галузі як інформаційна безпека ОБІ, ПлЗ мають місце неформальні описи таких понять, як: атака, аномалія, вразливість, загроза та ін.

Крім того, у ПлЗ необхідний опис стану середовища. Під середовищем розумітимемо конкретну ситуацію, що впливає на ІБ ОБІ. Вирішення подібних завдань передбачає багатокроковість, оскільки вирішити таке складне завдання за

один крок неможливо. Тоді сукупність усіх можливих кроків, що реалізуються для розв'язання задачі, утворює простір станів (або ПС) [29].

Пошук рішення за допомогою обчислювального ядра ІІС заснований на формалізованому поданні задачі. Крім того, необхідно виконати описи послідовності зміни станів. Це, зрештою, веде до досягнення поставленої мети, пошуку рішень. Крім того, необхідно при побудові ПлЗ сформувати концепти, що є основними структурними компонентами ІІС. Вирішенню даних завдань і присвячена заключна 5 глава дисертації.

4.2. Аналіз діючої практики управління інформаційною безпекою на підприємствах

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 [31, 32]. Накопичені у сфері захисту інформації (ЗІ) досвід, а також нові вимоги щодо побудови політики інформаційної безпеки (ПІБ) підприємств дозволили виробити досить ефективні рекомендації щодо побудови системи управління інформаційною безпекою (СУІБ). Причому сьогодні СУІБ інтегрує окремі, часто розрізнені заходи, спрямовані на забезпечення ЗІ та ІБ підприємства.

Центральним процесом у СУІБ компаній 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) [33, 34]. Цей ланцюжок заходів щодо забезпечення ІБ компанії підтвердив свою ефективність для превентивних, реактивних та/або ретроспективних заходів у межах захисту корпоративної інформації як невеликих суб'єктів господарської діяльності, так і великих підприємств.

Зауважимо, що розв’язання задачі, пов’язаної з організацією в межах СУІБ компанії, процесу ЕМ носить комплексний характер.

Залежно від масштабу компанії та специфіки її бізнес-процесів різні суб’єкти господарської діяльності використовують свої набори процесів та підпроцесів СУІБ. Як показує практика [35], відрізняються і підходи до ієрархії та інтеграції процесів та підпроцесів СУІБ.

У міру інтеграції України та її суб’єктів господарської діяльності до глобалізованого міжнародного ринку українські компанії як методологічну основу побудови СУІБ застосовують стандарти серії ISO/IEC 2700x [35, 36].

Проте зауважимо, що в ряді випадків таке формування СУІБ підприємства на основі ISO/IEC 2700x не враховує особливостей ЕМ у вітчизняних умовах. Така ситуація стала наслідком того, що міжнародна практика побудови СУІБ підприємств, насамперед, спирається на процес управління інцидентами. При цьому багато фахівців в області ІБ компаній вважають, що ЕМ є менш значущим фактором. Уважаючи, що пріоритет при побудові ефективної СУІБ відданий виключно управлінню інцидентами, можна пропустити поза увагою таку обставину. Тільки процес управління інцидентами не може втілити ефективний проактивний підхід у межах надання ІТ-послуг та СУІБ підприємства. Отже, не забезпечує максимально високий рівень ІБ підприємства [68].

Обмежена увага до впровадження процесу ЕМ у компаніях найчастіше є наслідком відсутності стандартизованої та загальновизнаної методології. Причому ця методологія має бути адаптована до ПІБ підприємств. Складності вирішення цього завдання обумовлені, насамперед, тими обсягами та трудомісткістю підготовчих робіт, яку необхідно провести аналітикам ІБ підприємства. Причому чим більший масштаб підприємства, тим більше параметрів необхідно врахувати. Параметри, що враховуються, можуть стосуватися як організаційного, так технічного рівнів ІС або КІС підприємств [68].

Питанням побудови ефективної СУІБ підприємства присвячено чимало досліджень. Зауважимо, що ряд авторів [37-41] по-різному трактують такий термін

як «подія» (event) у тих СУІБ. Таке «різночитання» саме собою створює складнощі в роботі аналітиків ІБ підприємства. Насамперед лише на рівні термінології.

У проаналізованих роботах [37-41] автори не враховують той факт, у ході реалізації процесів, пов'язаних з ЕМ. Спочатку аналітика або аудитора ІБ, цікавить факт запису про подію, що відбулася. Такий запис може бути зафіксований в системі збору даних служби ІБ підприємства. Додатково фіксується пов'язані події та стани КІС, наприклад, може йтися про підвищені рівні завантаження процесорів (або ядер) серверів, нетипові встановлені мережеві з'єднання [42] і т.п. Наведені приклади також є подіями. Однак більшість нормативних документів з управління інформаційною безпекою [42-46] подібним подіям не приділяють належної уваги. На думку авторів [43, 44], не варто звужувати визначення події, якщо йдеться про забезпечення ІБ підприємства. На думку ряду авторів [47, 48, 49], різночитання поняття управління подіями може призвести до фактичного дублювання подій та активностей. А це породжує 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 ІБ підприємства [50, 51].

У межах цього дослідження проаналізовано два найбільш ефективні варіанти (США та Європа) організації процесу ЕМ. А саме детально проведено порівняння між стандартом NIST SP 800-92 [52] та методологією ITIL [53].

У [52] регулюються питання управління логами (Log Management). У цьому документі лог (Log) сприймається як запис, відповідний певній події в системі. Під системою розуміється, наприклад, КІС чи мережа підприємства. За своїми цілями, беручи до уваги контекст трактування, можна говорити про опис лога як про опис управління подією.

У свою чергу в [53] розглядається комплекс процесів СУІБ, у тому числі торкнулися і питання управління подіями.

У таблиці 4.2 наведено детальне порівняння даних документів та визнаних світових практик із виділенням їх сильних та слабких сторін.

Таблиця 4.2

Світові практики організації процесу ЕМ у СУІБ

Нормативний документ	Область 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 ключових 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: розроблено автором

Таким чином, проведений аналіз літературних джерел, у тому числі провідних світових стандартів [52], методик [53], теоретичних та практичних досліджень [37, 41, 46, 49] дозволяє зробити такий висновок.

Дані документи не містять структурованого опису процесу ЕМ, яке, апріорі, включає принципи безперервного вдосконалення. Нагадаємо, що ці принципи

містяться в послідовності: 1) планування (Plan); 2) реалізація (Do); 3) перевірка (Check); дія (Act) [33, 34]. Крім того, у більшості з розглянутих теоретичних робіт не було враховано найважливіші аспекти реалізації сучасних ІТ-інфраструктур компаній, особливості сучасних бізнес-процесів, особливості обробки подій, що реалізуються в межах їх ЖЦ.

У такий спосіб можна констатувати. Потрібно сформувати комплексний підхід до організації процесів ЕМ. Цей комплексний підхід повинен ураховувати взаємопов'язаність з іншими процесами управління. Крім того, він повинен бути гармонізований зі стандартами ISO/IEC 2700x.

Удосконалення процесів управління ІБ пропонує необхідність урахування всієї сукупності принципів управління. Очевидно, що ці принципи беруть до уваги й особливості таких об'єктів [51, 52]:

– «інформаційна безпека»;

– «необхідність запобігання інцидентам»;

– «необхідність ослаблення інцидентів».

Традиційний підхід передбачає вирішення проблеми підвищення рівня ІБ компанії шляхом збільшення витрат на СУІБ. Це здебільшого сприяє зниженню рівня ризиків, пов'язаних із втратою інформації. Даний 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 ландшафту кібернетичних загроз, збільшення складності сценаріїв кібернетичних атак), акцент слід робити на адаптивність та інваріантність способів реалізації інфраструктурних рішень ІБ підприємства.

Упровадження ІТ у процеси управління ІБ і, зокрема, в організацію процесів Управління подіями ІБ підприємств сприяє недопущенню потенційно можливих втрат. З урахуванням робіт [33, 34, 37, 38, 50, 54] у межах побудови СУІБ компанії

запропоновано доповнення до способу організації процесу Управління подіями (ЕМ), див. рис. 4.6.

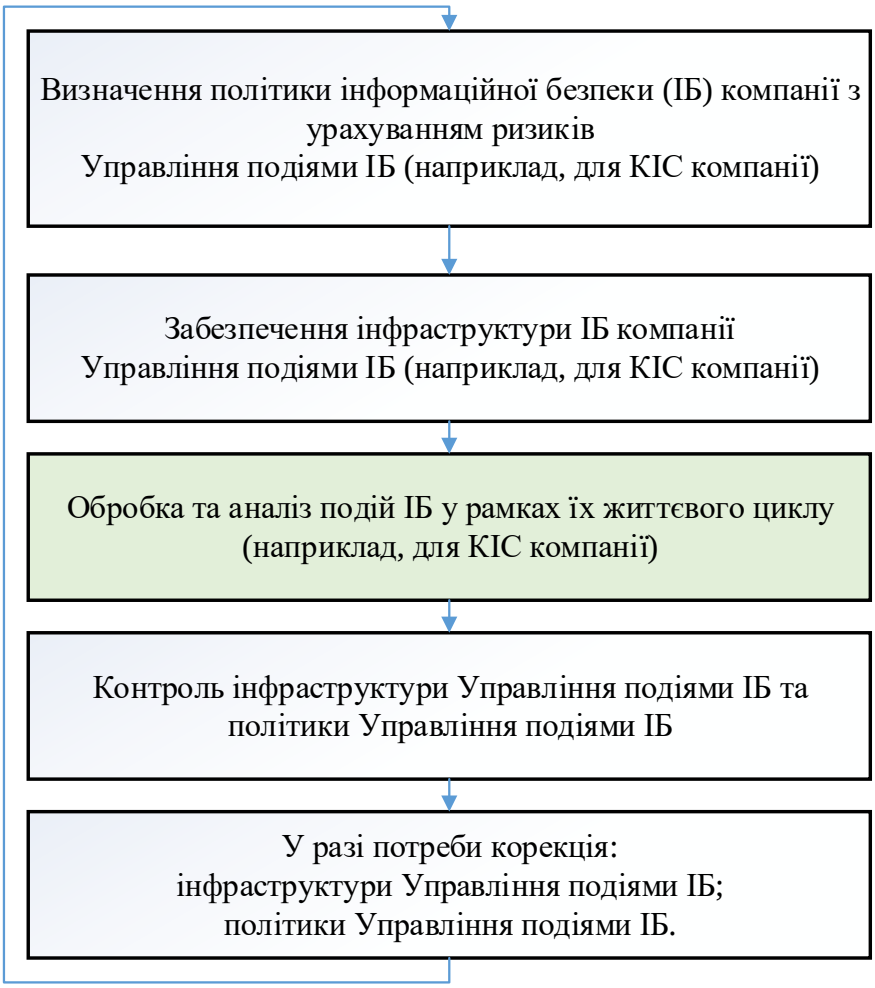


Рис. 4.6. Схема адаптивного процесу Управління подіями ІБ компанії (підприємства)

Джерело: розроблено автором

На відміну від існуючої практики запропоновані доповнення дозволяють враховувати той факт, що:

– практично не всі події реєструються;

– не всі ті події, які були зареєстровані, відправляються на обробку до системи класу SIEM (Security information and event management) [40] або SIP (Security event management) [55],

– обробка подій може породжувати нові події.

Запропонована на рис. 4.6 схема адаптивного процесу ЕМ дозволяє, на наш погляд, урахувати особливості, пов’язані із:

– визначенням політики ЕМ для КІС підприємства;

– забезпеченням інфраструктурних рішень щодо Управління подіями;

– обробкою подій у межах їх ЖЦ;

– контролем інфраструктурних рішень щодо Управління подіями;

– контролем політики ЕМ;

– з корекцією інфраструктурних рішень щодо Управління подіями, у разі потреби;

– з корекцією політики ЕМ, у разі потреби.

З урахуванням тієї обставини, що в межах даного дослідження нас насамперед цікавлять економічні аспекти організації управління політикою ІБ підприємства, більш детально зупинимося на такому підпроцесі (рис. 4.6) як «Обробка та аналіз подій ІБ в межах їх ЖЦ (наприклад, для КІС компанії)». На рис. 4.6 цей підпроцес показаний зі світло-зеленою заливкою.

Зауважимо, що саме цей підпроцес, більш деталізований на рис. 4.7, дозволяє в кінцевому рахунку на підставі аналізу подій ІБ мінімізувати потенційні ризики, пов’язані з можливими втратами інформаційних ресурсів (ІР) підприємства. А, отже, і мінімізує потенційну економічну шкоду, що викликається недотриманням політики ІБ підприємства.

Блок схема, представлена на рис. 4.7, включає такі основні елементи:

1) фактична поява події. На основі зміни або збереження станів, які мають значення для ІБ. А крім того, можуть вплинути на працездатність компонентів КІС її інфраструктури (наприклад, мережі). Можуть надати або вже впливають на СУІБ підприємства;

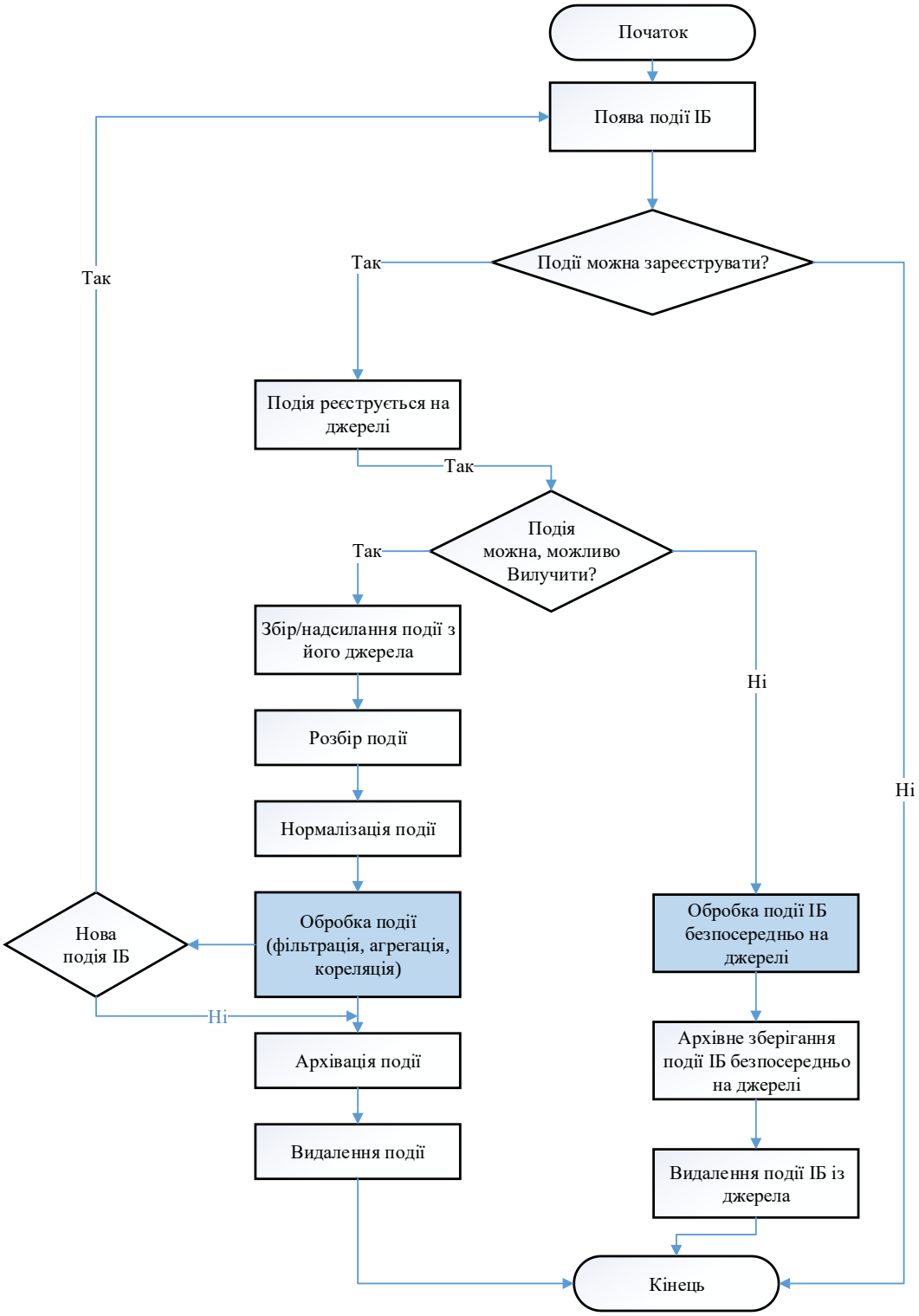


Рис. 4.7. Обробка та аналіз подій ІБ у рамках їх ЖЦ

Джерело: розроблено автором

2) реєстрація подій. На даному етапі виконуються відповідні записи в журналах (наприклад, у файлі лог, таблицях баз даних). На цьому етапі зареєстровані події готові до відправлення;

3) надсилання повідомлення про подію. На даному етапі відбувається передача події «точку», яка виконує роль пункту централізованої обробки. Це може бути апаратно-програмні комплекси класів SIEM [10] чи SIP [55];

4) розбір подій. На цьому етапі з події виділяються метадані;

5) нормалізація події. Цей етап відповідає процедурі конвертації відповідних полів подій у найбільш підходяще для подальшої обробки уявлення;

6) обробка подій, яка включає такі підетапи:

– фільтрування – на цьому підетапі з подій виключаються деякі параметри, наприклад за критерієм важливості джерела подій; це в кінцевому рахунку дозволяє скоротити витрати часу та ресурсів на обробку 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 обробку подій;

– кореляція – цей підетап відповідає пошуку взаємозв’язків між двома чи більше подіями; як основою кореляції виступають спеціальні шаблони на основі правил та/або статистичних значень тощо;

7) збереження архіву;

8) видалення подій.

На етапі обробки подій (на рис. 4.7 цей блок показаний блакитною заливкою) аналітик ІБ може за допомогою відповідного програмного забезпечення (ПЗ) проаналізувати параметри, що характеризують стійкість управління ІБ КИС. При цьому думати, що КІС може виступати як об’єкт кібернетичної атаки. Нижче представлений фрагмент моделі, що становить обчислювальне ядро, призначеного для обробки подій ІБ.

Вважатимемо, що результатом обробки подій ІБ може стати визначення (як окремий випадок) показника, який характеризує можливе зниження функціональної ефективності КІС в результаті деструктивних дій атакуючої сторони.

Справедливо таке ставлення:

$$(\Delta EF, R_c) \to \min_{0<q<1}, \quad (4.1)$$

де $\Delta EF -$ параметр, який характеризує можливе зниження функціональної ефективності КІС внаслідок деструктивних дій атакуючої сторони;

$R_c -$ витрати ресурсів, пов'язані з побудовою ефективної СУІБ компанії (зокрема її КІС);

$q -$ ймовірність забезпечення ІБ КІС (зокрема її КІС).

Дослідженням, присвяченим пошуку оптимальних розв'язків цього завдання, присвячено безліч досліджень різних авторів. При цьому для пошуку рішення можуть застосовувати різні методи та моделі, див. рис. 4.8. Це питання виходить за межі цього дослідження, тому ми не зупиняємося на ньому докладно.

Запропоновані в нашому дослідженні рішення та доповнення, на відміну від аналогічних досліджень інших авторів, наприклад, [47, 48, 54, 56, 57, 58] характеризуються інваріантністю по відношенню до способів реалізації інфраструктурних рішень ІБ компанії. Це твердження справедливе і до ІБ КІС підприємств. Запропоновані доповнення, зрештою, дозволяють, не змінюючи методичний інструментарій, масштабувати даний підхід і адаптувати його СУІБ різних компаній.

Подальшим розвитком досліджень у цьому напрямі можуть стати роботи, пов'язані з організацією процесів Управління подіями ІБ. Дані роботи передують формуванню логічної та комплексної СУІБ компанії.

Синтез процедур адаптивного моніторингу, див. рис. 4.9, та Управління подіями ІБ підприємства в сучасних умовах є нетривіальним завданням. Це не в останню чергу диктується різноманіттям завдань ІБ та динамічними особливостями об'єктів захисту.

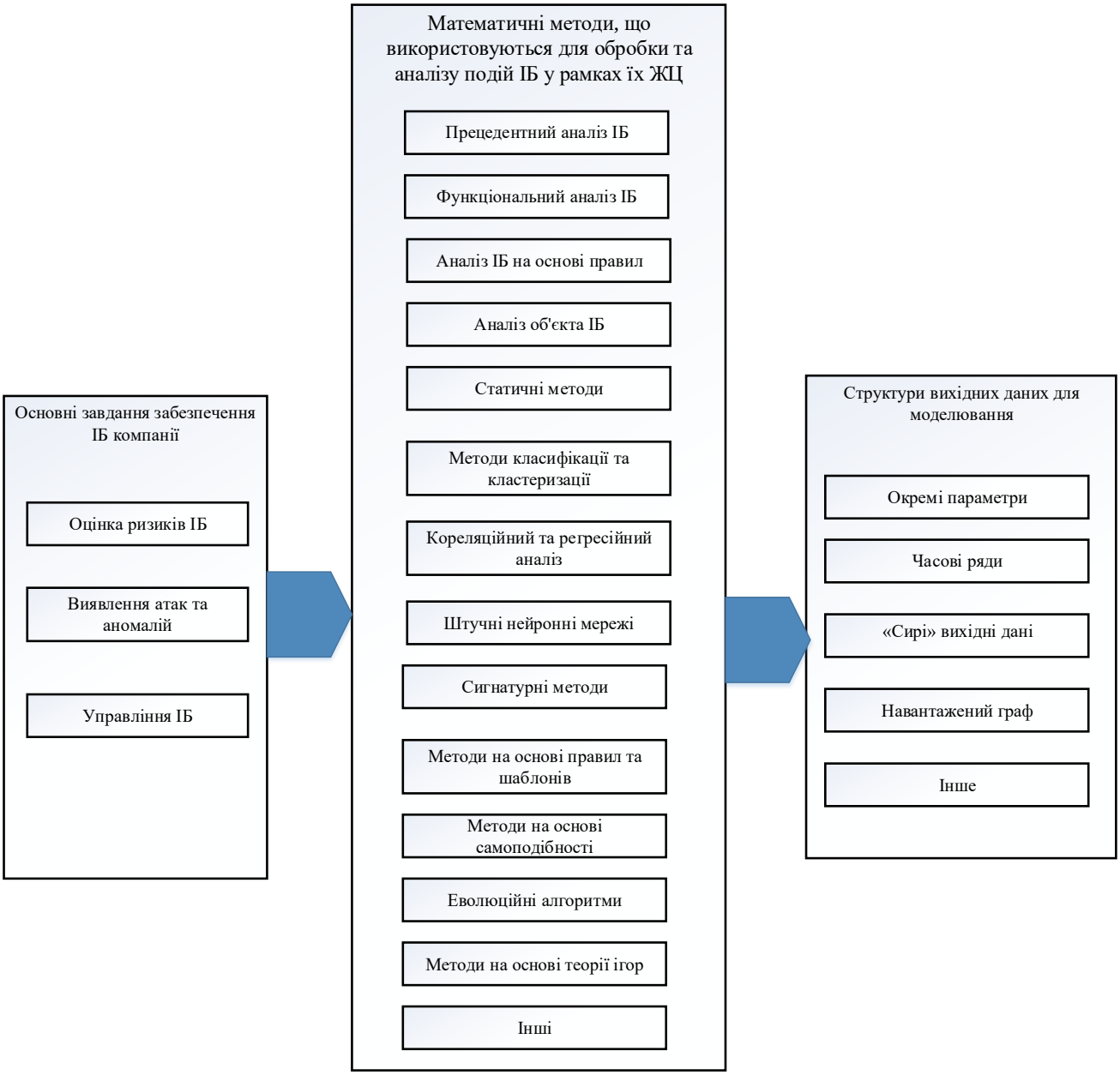


Рис. 4.8. Схема відповідності завдань забезпечення ІБ підприємства та математичних методів їх вирішення

Джерело: розроблено автором

Імплементація методології теорії систем дала можливість сформулювати загальні принципи такого адаптивного моніторингу та управління подіями ІБ: ієрархічна пов’язаність подій ІБ; цілісність; подібність подій ІБ.

У дод. Б концептуально представлено розширену схему адаптивного моніторингу ІБ, включаючи процедури оброблення та аналізу подій ІБ в межах їх ЖЦ.

4.3 Оцінка економічної ефективності системи захисту корпоративної інформації

Сьогодні діяльність урядів країн світу, суспільства та бізнес-структури спирається на всебічне використання інформаційних технологій Конвергентні технологічні платформи, інструменти та інтерфейси, підключені через Інтернет, який швидко переходить до більш децентралізованої версії 3.0, одразу створюючи складніший ландшафт загроз системі захисту корпоративної інформації і зростаючу кількість критичних точок відмов. Оскільки суспільство продовжує мігрувати в цифровий світ, загрози системі інформаційного захисту набирають масштабних розмірів, що зазвичай коштує організаціям десятки або сотні мільйонів доларів. Втрати не лише фінансові: критична інфраструктура, суспільство та психологічне благополуччя також знаходяться під загрозою.

За останні 20 років різко зросла залежність від цифрових систем організації бізнесу. Перехід до віддаленої роботи, спричинений COVID-19, прискорив упровадження платформ і пристроїв, які дозволяють ділитися конфіденційними даними з третіми особами, – хмарні сервіси, провайдери, інтерфейси прикладного програмування та інші пов’язані з технологією посередники [59].

Ці системи, будучи потужними інструментами для обробки даних і обробки загалом, надають додатковий рівень залежності від постачальників послуг. Віддалена робота також перемістила цифрові обмінники з офісних мереж у житлові, які мають більше різноманітних підключених пристроїв із меншим захистом від кібервторгнення [69].

Паралельно, прагнення до можливостей ґрунтувалося на використанні кількох технологій узгодженої роботи, включаючи штучний інтелект, периферійні обчислення, блокчейн і 5G, лише зростає [60]. Хоча ці можливості надають величезні переваги для бізнесу і суспільства за рахунок використання інформаційних технологій, що стають драйверами підвищення ефективності, якості і продуктивність їх діяльності, одночасно породжуючи більш згубні форми цифрового та кіберризику.

Сучасний розвиток бізнесу спонукає корпорації до активного розвитку та максимального використання інформаційних технологій. Стрімке та динамічне бізнес-середовище, у свою чергу, неминуче призводить до невизначеності бізнес-процесів і виникнення нових ризиків у системі захисту корпоративної інформації. Система захисту корпоративної інформації є одним із найважливіших аспектів комплексної безпеки, як на рівні окремих корпоративних структур, так і на регіональному та національному рівнях загалом. [61].

Фундаментом процесу управління розвитком корпоративних структур є його інформаційна система, яка є взаємопов'язаною сукупністю даних технічного та програмного забезпечення, персоналу, інтерактивних процедур, призначених для збору, обробки, розподілу, зберігання, надання інформації відповідно до цільових вимог (рис. 4.10). [69]

Якість управління розвитком корпоративних структур визначається надійністю та ефективністю його інформаційної системи.

Надійність – це здатність інформаційної системи зберігати протягом певного часу в установлених межах значення всіх параметрів, які характеризують здатність системи виконувати покладені на неї функції в заданих режимах. При цьому, надійність інформаційна система матиме лише тоді, коли вона характеризуватиметься безвідмовністю та довговічністю.

При цьому рівень надійності інформаційної системи управління розвитком корпоративних структур залежить від:

– складу та рівня надійності технічних засобів, їх взаємодії та надійності структури;

– складу та рівня надійності програмних засобів, їх можливостей та взаємодії у структурі програмного забезпечення інформаційної системи;

– раціонального розподілу завдань між технічними засобами, програмним забезпеченням та персоналом, що обслуговує цю систему;

– режимів, параметрів та організаційних форм експлуатації комплексу технічних засобів. [69]

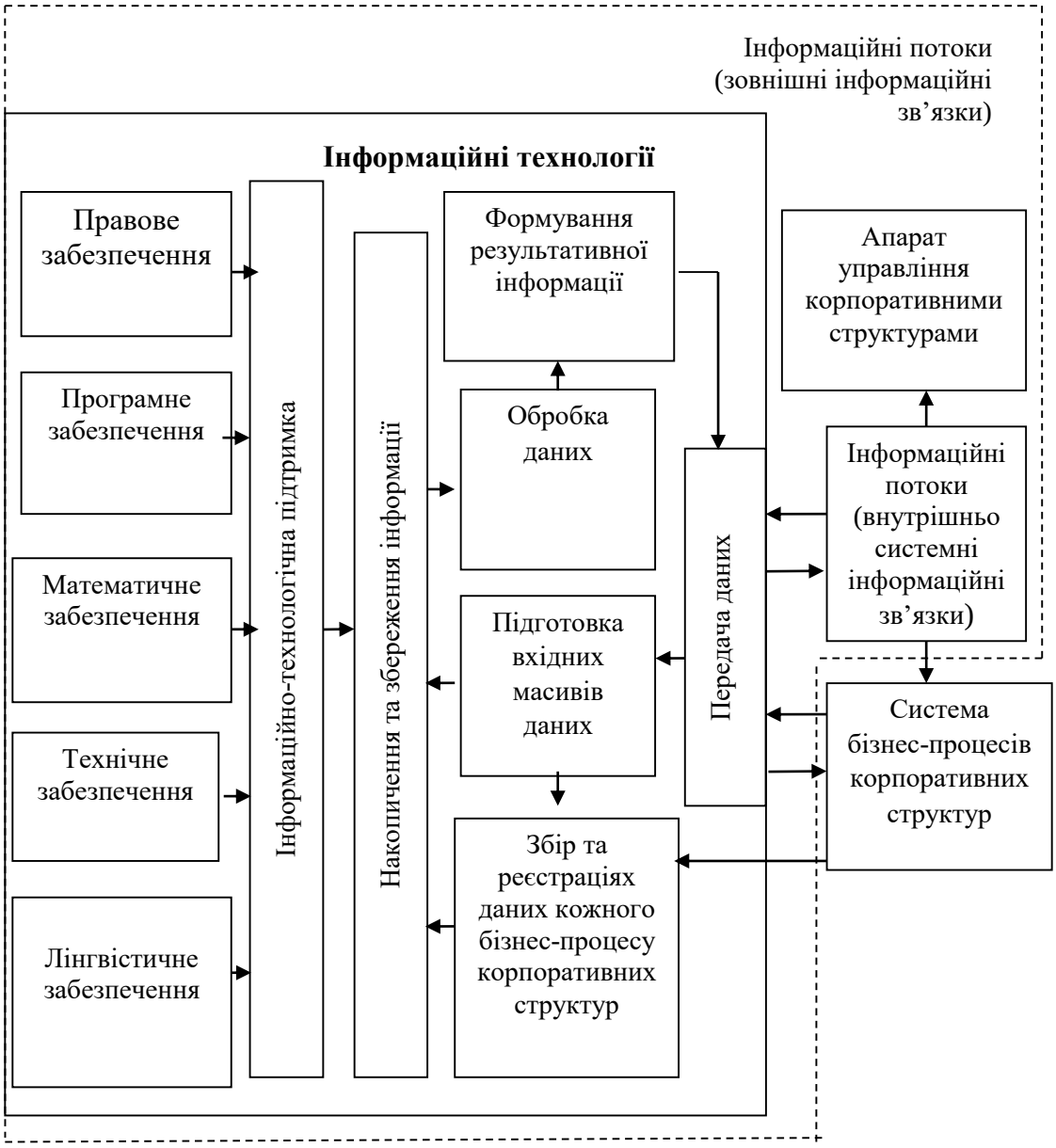


Рис. 4.10. Інформаційна система процесу управління розвитком корпоративних структур

Джерело: розроблено автором

Ефективність системи захисту корпоративної інформації визначається порівнянням отриманих результатів із витратами всіх видів ресурсів (технічних, технологічних, кадрових, організаційно - економічних), що необхідні для розвитку аналізованої системи. [69]

Система захисту корпоративної інформації, як і будь-яка інша система, що діє всередині корпоративних структур, має свою структуру.

Структура інформаційної системи в управлінні розвитком корпоративних структур визначається розміщенням та взаємозв’язками елементів у процесі виконання покладених на неї функцій [62].

Структура інформаційної залежить від розміру системи та її складу. Розмір системи характеризується як кількістю елементів, так й зв’язками між ними. Структура інформаційної системи управління розвитком корпоративних структур визначає її функції:

– збір та реєстрація даних;

– підготовка інформаційних масивів даних;

– обробка, накопичення та зберігання даних;

– формування результатної інформації;

– передача даних від джерел виникнення до місця обробки та надалі споживачам інформації для прийняття управлінських рішень;

– захист інформації.

Таким чином, інформаційна система є найважливішою складовою системи управління розвитком корпоративних структур, завдяки якій можна своєчасно та в повному обсязі визначити значення показників, що відстежуються, а також тенденції їх розвитку на найближчу перспективу з метою здійснення своєчасних управлінських коригуючих дій, спрямованих на досягнення поставлених стратегічних цілей. [69]

Метою класифікації корпоративної інформації є диференціація заходів безпеки відповідно до важливості інформації про корпорацію після її оцінки. Зараз більшість корпорацій використовують тріаду конфіденційності, цілісності та доступності як стандарт при оцінці важливості корпоративної інформації [63]. Конфіденційність означає збереження інформації в таємниці; цілісність, збереження інформації незмінною; доступність для негайного використання інформації незалежно від географічних або часових обмежень [64].

Стрімкий розвиток інформаційних технологій вимагає постійного вдосконалення системи захисту інформації та аналізу ефективності їх впровадження. [62].

Оцінка ефективності витрат на заходи, які необхідно вжити для забезпечення системи захисту корпоративної інформації, є важливою проблемою, вирішення якої має спиратися на комплексний підхід, що враховує специфіку конкретної корпорації чи галузі.

Забезпечення інформаційної безпеки стає важливим елементом динамічного та збалансованого розвитку підприємства. У цьому зв'язку дуже важливим для кожної корпоративної структури стають питання проведення релевантної оцінки системи захисту інформаційної корпоративної інформації. Саме впровадження в діяльність сучасних організацій інструментів кількісного аналізу та моделювання, які дозволять здійснювати перманенту ідентифікацію, оцінювати ризики та загрози інформаційної безпеці є одним з головних детермінант формування прогресивності розвитку сучасних систем захисту корпоративної інформації.

Однак, на практиці реалізація комплексу інструментів та моделей ідентифікації, оцінки ризиків системи захисту корпоративної інформації, що дає у підсумку можливість корпоративним структурам визначити її ефективність, в більшості випадків, значно ускладняється через дуже диференційовану специфіку роботи організацій. Це створює методологічні проблеми, коли рішення щодо створення ефективної системи захисту корпоративної інформації має враховувати особливості галузі чи сфери діяльності корпорацій [65].

Отже, метою формування ефективної системи захисту корпоративної інформації є диференціювання дій щодо безпеки відповідно до важливості корпоративної інформації після її оцінки. Більшість корпорацій в даний час використовують тріаду конфіденційності, цілісності та доступності (CIA) як стандарт при оцінці системи захисту корпоративної інформації [66]. Конфіденційність стосується збереження таємниці інформації; цілісність, характеризує характеризую здатність ефективної системи захисту інформації зберігати її незмінною; доступність передбачає наявність можливості негайного використання інформації незалежно від географічних або тимчасових обмежень. Однак, слід зазначити, що використання стандарту конфіденційності, цілісності та доступності в процесі формування ефективної системи захисту корпоративної

інформації викликає протиріччя при використанні конфіденційності для оцінки важливості корпоративної інформації, різні стандарти (наприклад, цілісність або доступність) для також мають однакове значення для оцінки ступеня конфіденційності. Іншими словами, оцінку ступеня конфіденційності можна інтерпретувати як оцінку рівня корпоративної інформації. Крім того, оцінка системи захисту корпоративної інформації, яка базується на вищезазначеної тріаді може бути обмежувальною, оскільки вона не враховує пріоритетність задач корпорації, цілі та особливості протікання корпоративних бізнес-процесів. Більша частина корпоративної інформації може бути захищена вибором залежно від оточуючого бізнес-середовища та корпоративної стратегії.

Нове осмислення процесів формування ефективної системи захисту корпоративної інформації свідчить про необхідність вибору показників на етапах життєвого циклу корпоративної інформації. Сам факт, що на сьогоднішній день не існує єдиного підходу до визначення показників, наголошує на особливій значущості та складності даної проблеми. Складність формування ефективної системи захисту корпоративної інформації обумовлюється швидким розвитком в інформаційних технологіях та різноманітних методах вимірювання інформаційної безпеки; нездатністю достовірно передбачити всі можливі сценарії несанкціонованого доступу; недостатньо достовірної оцінкою вартості інформаційних ресурсів, а також грошовою оцінкою наслідків правопорушень у цих галузях.

Головною метою формування ефективної системи захисту корпоративної інформації є підтримка її в актуальному стані, тобто досягнення постійної відповідності інформаційної системи цілям діяльності корпоративних структур шляхом формування ефективних управлінських впливів.

В умовах високих темпів науково-технічного прогресу та розвитку інформаційних технологій цілі корпоративних структур та параметри інформаційних ресурсів та технологій, якими вона потенційно може бути оснащена, змінюються. Причому темпи зміни цілей системи та параметрів, як правило, різні, а можливості своєчасного оснащення системи необхідними

засобами обмежені зовнішніми та внутрішніми факторами. Ці обставини суттєво ускладнюють вироблення та реалізацію зазначених управлінських впливів.

Насамперед необхідно відповісти на питання про структуру інформаційних ресурсів, тобто про склад та взаємозв'язки елементів, що характеризують ці ресурси.

Інформаційні ресурси повинні характеризувати можливості корпоративних структур, що відкриваються параметрами встановлених засобів інформаційно-технологічного оснащення, властивостями і специфікою параметрами різних джерел відтворення елементів інформаційної системи.

Залежно від цілей та можливостей корпоративних структур створення ефективної системи захисту корпоративної інформації має бути орієнтоване на оптимізацію поєднання різних напрямків із пріоритетним розвитком інтенсивних напрямків. Реалізація такого підходу може бути представлена у вигляді реалізації певних етапів життєвого циклу корпоративної інформації. Відповідно, багатовимірна перспектива економічної ефективності системи захисту корпоративної інформації базується на врахуванні різних типів корпоративної інформації та її компонентів з огляду на життєвий цикл корпоративної інформації та результативність бізнес-потоків.

Американський вчений-дослідник в галузі створення системи захисту корпоративної інформації та оцінки її економічної ефективності Рей Бернард у своєму досліджені «Оцінка ризиків безпеки життєвого циклу інформації: інструмент для усунення прогалин у безпеці» у 2007 році визначив основні етапи життєвого циклу корпоративної інформації та довів необхідність оцінки її економічної ефективності відповідно до цих етапів. При цьому, автором обґрунтовано, що на етапі створення корпоративної інформації відбувається встановлення рівня якості, доступності, зручності тощо. Саме ці параметри формують відповідні результативні (вихідні) інформаційні потоки, які потім використовується на різних рівнях корпоративного управління, відповідно до стандартів їх використання і, нарешті, всередині та зовні для бізнесу (результат)

або приходить до природного кінця терміну служби корпоративної інформації (знищення її відповідно до цілей да задач корпоративних структур) [67].

При цьому слід звернути увагу на оцінку досягнутого рівня інформаційних ресурсів, визначення цілей системи захисту корпоративної інформації, вибір оптимальних варіантів вдосконалення корпоративної інформації, процес вдосконалення інформаційної бази корпорацій.

Найважливішою характеристикою системи захисту корпоративної інформації є ступінь її прогресивності, яка вказує на залежність збільшення прибутку від впровадження в діяльність корпорацій ефективної системи захисту корпоративної інформації.

У діяльності сучасних корпоративних структур використовується велика кількість різних методик оцінки економічної ефективності системи захисту корпоративної інформації, які зазвичай називають методиками оцінки рівня інформаційної безпеки. Ці методики передбачають чи поодинокі показники, чи його набори, за допомогою яких робляться спроби кількісно оцінити стан системи захисту корпоративної інформації. Проте, існуючи методики не дають можливість оцінити стан системи захисту корпоративної інформації та її економічну ефективність з погляду їх можливостей реалізації цілей діяльності корпоративних структур, тобто з погляду ресурсного підходу та врахувати особливості життєвого циклу корпоративної інформації.

Відсутність поки що єдиної методики чи рекомендацій, регламентуючих універсальні для всіх галузей національної економіки принципи визначення економічної ефективності системи захисту корпоративної інформації ускладнює роботу зі створення надійних методів вимірювання ступеня досконалості та прогресивності інформаційної системи. Головним недоліком для більшості застосовуваних методів оцінки системи захисту корпоративної інформації є відсутність економічного змісту у показниках оцінки, що використовуються. Зазвичай застосовують показники, що мають умовний характер. Такий підхід не дозволяє простежити економічні наслідки зміни корпоративної інформаційної

системи та швидко здійснювати трансформацію її елементів від конкретних умов функціонування корпорацій.

Показники системи захисту корпоративної інформації дуже складно взаємопов'язані з економічними показниками і не завжди заздалегідь можна визначити, в який бік та наскільки їх слід змінювати. Елементи інформаційної системи корпорації традиційно віднесене до групи прогресивних ресурсів, незважаючи на їх високі технічні характеристики, у конкретних умовах функціонування корпорацій може виявитися неефективним з економічної точки зору.

Отже, розробка корпоративної політики щодо впровадження ефективної системи захисту корпоративної інформації з урахуванням цієї оцінки орієнтує на «максимізацію» рівня системи захисту корпоративної інформації та у деяких випадках може призвести до великого спотворення відповідності цієї системи умовам функціонування корпоративних структур. Ця невідповідність – невикористана, нереалізована частина ефекту. Зазначене явище якісно можна зобразити так (рис. 4.11).

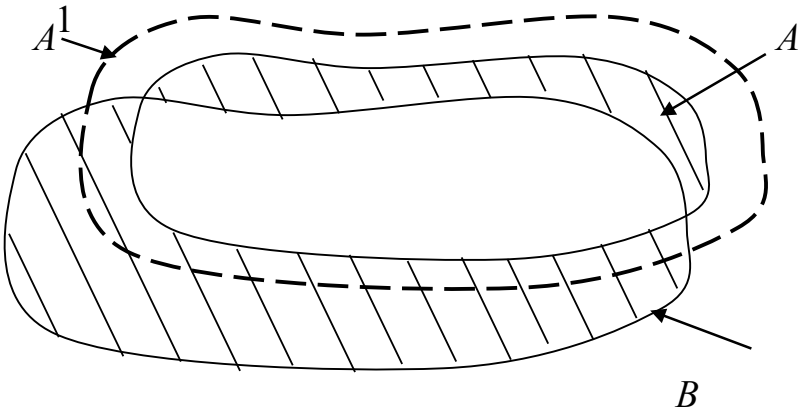


Рис. 4.11. Співвідношення між станом системи захисту корпоративної інформації та умовами функціонування корпорацій

Джерело: розроблено автором

На рис. 4.11 співвідношення між станом системи захисту корпоративної інформації та умовами функціонування корпорацій відображено у вигляді двох множин А та В, де А та В – множини, сукупність елементів яких в цілому відображає відповідно стан системи захисту корпоративної інформації та певні умови функціонування корпорацій. Заштриховані області зображують зазначений вище розрив, який неможливо виявити з урахуванням розглянутого підходи до оцінки системи захисту корпоративної інформації. A^1 – характерне для цього підходу спотворення корпоративної інформаційної політики у результаті «максимізації» параметрів системи захисту корпоративної інформації.

Таким чином, розглянутий підхід до оцінки та формування ефективної системи захисту корпоративної інформації є недостатньо обґрунтованим та характеризується великим емпіризмом.

Одним з підходів, що дозволяють виявити і звести зазначений розрив (невідповідність) до мінімуму на основі визначення стану системи захисту корпоративної інформації, що повністю відображає умови функціонування корпоративних структур, є економічний підхід до оцінки ефективності системи захисту корпоративної інформації.

Концепція економічної оцінки системи захисту корпоративної інформації виходить з принципу – рівень системи захисту корпоративної інформації є передумовою, умовою його ефективності. Високий рівень системи захисту корпоративної інформації – високі економічні показники функціонування корпорацій. Прогресивними (ефективними) є такі елементи системи захисту корпоративної інформації, форми та методи організації та управління діяльністю корпорацій, за допомогою яких можна забезпечити виконання заданих результатів з мінімальними сукупними витратами живої та уречевленої праці за обов’язкового дотримання нормативів соціальних та екологічних відповідальності корпоративних структур.

В основу економічного підходу до оцінки системи захисту корпоративної інформації та вибору корпоративної інформаційної політики на базі цієї оцінки закладено принцип оптимізації стану системи захисту корпоративної інформації за

умовами функціонування на рівні конкретної корпорації. Ступінь відхилення від цього оптимального стану визначає рівень ефективності системи захисту корпоративної інформації. Чим вище рівень системи захисту корпоративної інформації, тим ближчий фактичний стан до оптимального.

Таким чином, підхід до оцінки економічної ефективності системи захисту корпоративної інформації на основі економічного критерію прогресивності інформаційної системи корпорацій створює передумови визначення її оптимального стану. На рис. 4.12 показано реалізацію аналізованого підходу на базі визначення областей економічно ефективного використання інформаційних ресурсів і технологій.

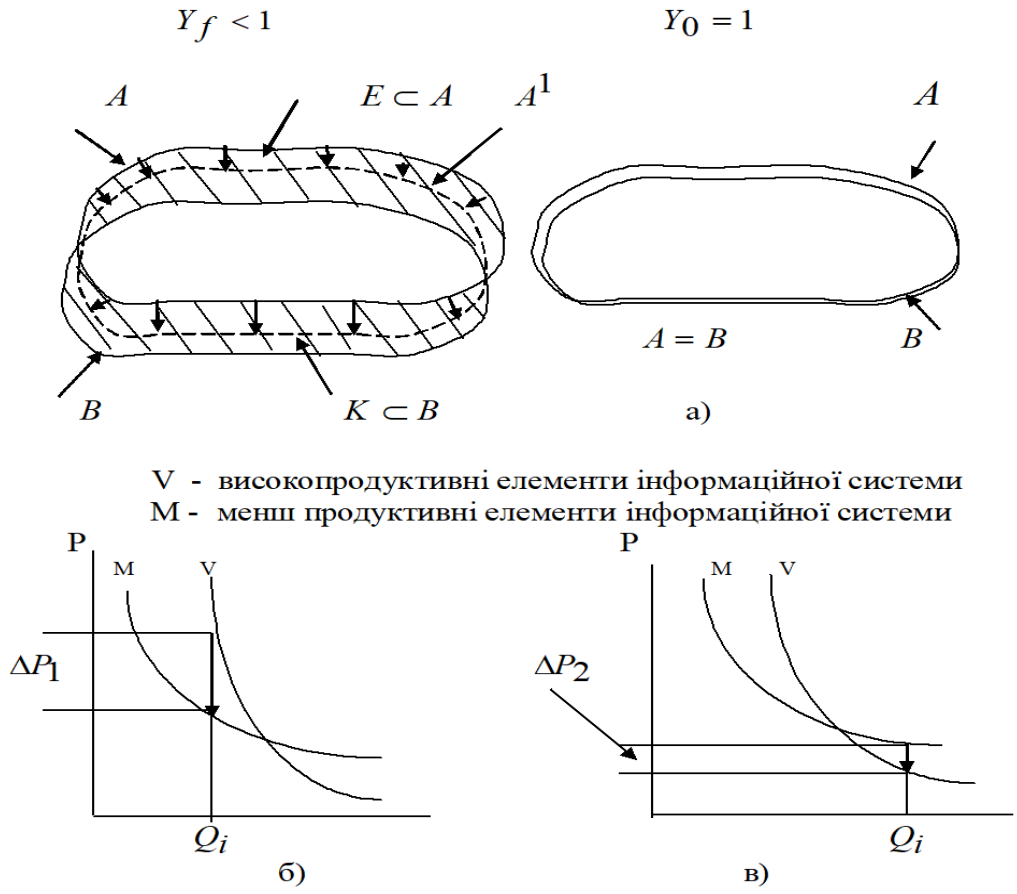


Рис. 4.12. Області ефективного використання обладнання

Джерело: розроблено автором

Так, у заштриховану область E множини $A(E \subset A)$, сукупністю елементів якого визначається стан системи захисту корпоративної інформації, потрапляють

ті елементи інформаційної системи, які за умов діяльності корпорації, що визначаються елементами множини $K(K \subset B)$ є непрогресивними. При цьому до розряду непрогресивних слід віднести:

1. Елементи інформаційної системи, потенційні можливості яких не можуть бути реалізовані ефективно за умов функціонування корпорацій. ΔP^1- пов'язані із цим зайві витрати (рис. 4.12, б).

2. Елементи інформаційної системи корпорацій, замість яких можуть бути поставлені відповідно до умов функціонування корпорацій, що склалися, на які слід замінити наявну по причині її ширших функціональних можливостей. ΔP^2– витрати, пов'язані з зазначеною невідповідністю (рис. 4.12, в).

Як параметр, що визначає умови функціонування корпорацій, прийнятий заданий обсяг подолань загроз та ризиків інформаційної безпеки корпорацій $Q_i \in B$ за певний період; P – питомі витрати, пов'язані з використанням взаємозамінних елементів інформаційної системи корпорації.

Таке розмежування дозволяє розкривати конкретні шляхи $(A \to A^1)$ та засоби підвищення рівня системи захисту корпоративної інформації. Співвідношення між $A \bigcap B$ і B характеризує ступінь поширення у діяльності корпорацій прогресивних засобів і методів, що належать області $A \bigcap B$, в загальній їх кількості в корпорації (B).

$A = B$ – оптимальний стан, при якому існуюча система захисту корпоративної інформації повністю відповідає об'єктивно сформованим умовам функціонування корпорацій.

Y – показник кількісної оцінки ступеня близькості фактичного стану існуючої системи захисту корпоративної інформації до оптимального.

Таким чином, економічна ефективність системи захисту корпоративної інформації кількісно оцінюється ступенем відхилення фактичних річних приведених витрат (P_f), пов'язаних з існуючою системою захисту корпоративної інформації від рівня витрат, що відповідає оптимальному її стану (P_o).

$$Y = 1 - \frac{P_f - P_0}{P_f} \quad (4.2)$$

при цьому: $Y_o = 1$ – оптимальне значення;

$0 \le Y_f \le 1$ – фактичне значення.

Графічну інтерпретацію показника Y наведено на рис. 4.13.

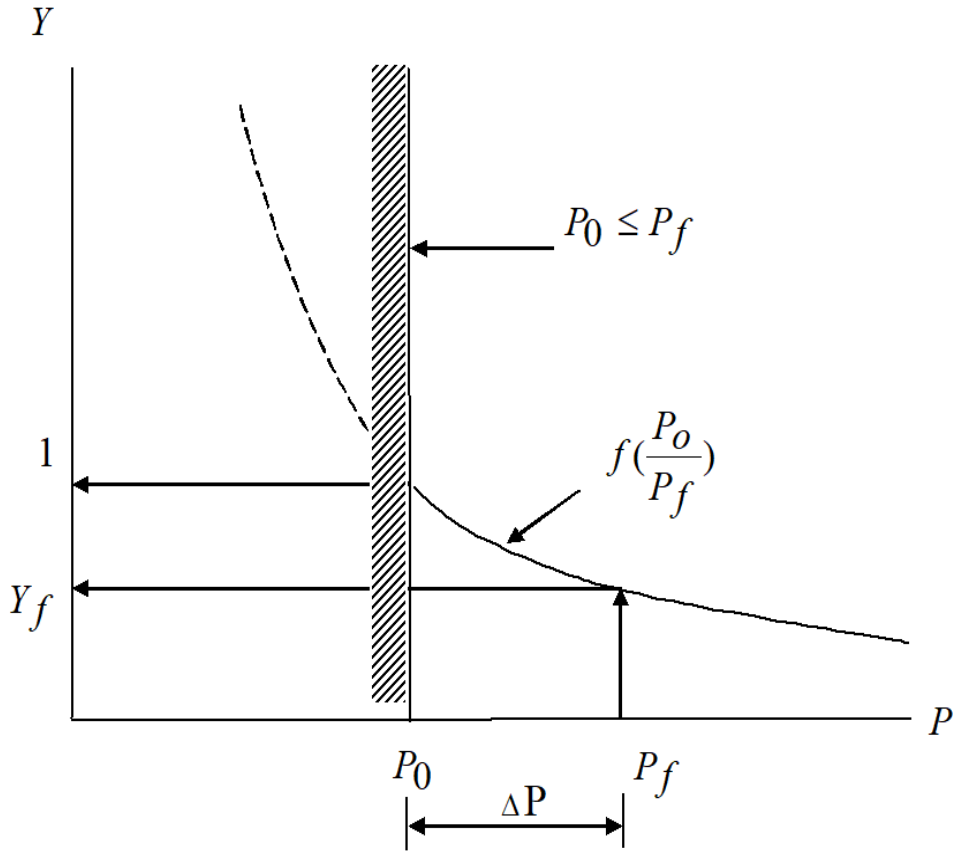


Рис. 4.13. Графічна інтерпретація показника економічної ефективності системи захисту корпоративної інформації

Джерело: розроблено автором

Такий підхід до оцінки економічної ефективності системи захисту корпоративної інформації є доцільним при централізованому розподілі інвестицій та ресурсів корпорацій.

Враховуючи динамічність сучасного бізнес-середовища корпорацій показник економічної ефективності системи захисту корпоративної інформації має визначатися як рівень досягнення нормативу потенційної можливості системи

захисту корпоративної інформації. За наявності таких нормативів рівень потенційних можливостей системи захисту корпоративної інформації Y_{ib} може бути оцінений економічно як ступінь досягнення максимально можливого прибутку корпоративної структури:

$$Y_{ib} = 1 - \frac{D_n - D_f}{D_n} \quad (4.3)$$

де: D_n – прибуток, який може бути отриманий в умовах функціонування корпорації, що відповідають нормативу потенційної спроможності системи захисту корпоративної інформації;

D_f – прибуток, який отримує корпорація при фактично досягнутих умовах функціонування системи захисту корпоративної інформації.

Отже, економічний підхід до оцінки прогресивності системи захисту корпоративної інформації дозволяє не тільки оцінити існуючий стан (A), але і націлює на вибір і досягнення оптимального (найкращого) її стану$(A \to A^1 \to B)$ в конкретних умовах функціонування корпорацій.

Внаслідок високого рівня мінливості умов функціонування корпорацій за порівняльної стійкості їх інформаційних систем об’єктивно існує процес постійної розбіжності фактичного значення економічної ефективності системи захисту корпоративної інформації від його досягнутого оптимального рівня. Отже, вирішення цього завдання передбачає кількісну оцінку факторів, що визначають рівень інформаційної безпеки, їхнього безпосереднього впливу та зв’язку з ефективністю функціонування корпорацій.

Оцінка швидкості реагування на зміни у зовнішньому середовищі характеризує властивість ефективної системи захисту корпоративної інформації забезпечувати адаптивність корпоративних структур від зовнішніх та внутрішніх загроз. Наявність виявлених проблем доводить необхідність розробки методики оцінки економічної ефективності системи захисту корпоративної інформації.

Об’єктом оцінки є 250 вітчизняні підприємств з чисельністю працівників понад 250 осіб, до складу яких входять підрозділи чи служби інформаційної

безпеки. Діагностика проблем оцінки економічної ефективності системи захисту корпоративної інформації проводилася методом діагностичного інтерв'ю. Інтерв'ю проводилося з керівниками підприємств та керівникам служб (департаментів) інформаційної безпеки з метою отримання відповідей на дослідницькі питання:

1. Чи є проблема оцінки ефективності та релевантна існуюча система захисту корпоративної інформації?
2. Чи існує на підприємстві локальний нормативний акт, який регулює систему захисту корпоративної інформації та визначає методику оцінки її ефективності?
3. Як часто на Вашому підприємстві здійснюється оцінка ефективності системи захисту корпоративної інформації?
4. Які цілі оцінки економічної ефективності системи захисту корпоративної інформації?
5. Які методології та індикатори використовуються для оцінки економічної ефективності системи захисту корпоративної інформації?
6. Які проблеми оцінки економічної ефективності системи захисту корпоративної інформації виникають на Вашому підприємстві?
7. Який із підходів, запропонованих у науковій літературі для оцінки економічної ефективності системи захисту корпоративної інформації є найкращім?

Керівники підприємств та керівники служб (департаментів) інформаційної безпеки великих та середніх підприємств вказують на актуальність оцінки економічної ефективності системи захисту корпоративної інформації. Однак вони не виділяють чітко відмінних рис оцінки ефективності цих систем. Крім того, на більшості досліджуваних підприємств взагалі відсутні методики оцінки економічної ефективності системи захисту корпоративної інформації, в окремих випадках локальними нормативними актами визначається склад узагальнюючих показників оцінки ефективності. тому, основні висновки ґрунтуються на суб'єктивних оцінках.

Однак, практично на всіх підприємствах для оцінки економічної ефективності системи захисту корпоративної інформації розраховуються такі показники, як: витрати на забезпечення системи захисту корпоративної інформації, рівень виконання бюджету видатків департаменту інформаційної безпеки, розмір попереджуючої, виявленої та відшкодованої шкоди.

У цілому, слід зазначити, що керівники не вважають оптимальними підходи, що використовуються для оцінки економічної ефективності системи захисту корпоративної інформації, та вказують на недостатню теоретичну та методологічну опрацьованість даного напряму.

Проведене дослідження дозволило виявити та систематизувати проблеми оцінки економічної ефективності системи захисту корпоративної інформації на підприємствах:

– недостатня розробленість методики оцінки рівня інформаційної безпеки підприємства, адаптованої до цілей оцінки ефективності та ефективності системи захисту корпоративної інформації;

– існуючі методики оцінки рівня інформаційної безпеки підприємства не враховують витрати ресурсів, що спрямовуються на функціонування системи захисту корпоративної інформації;

– недостатня розробленість методики оцінки попередженого збитку, який є результатом посилення захисту економічних інтересів та інформаційного потенціалу підприємства від зовнішніх загроз. Високий рівень суб’єктивності результатів оцінювання;

– це орієнтує працівників служби економічної безпеки на блокування більшості управлінських рішень, пов’язаних з ризиком, що негативно позначається на швидкості прийняття управлінських рішень і результатах діяльності підприємства;

– наявні системи захисту корпоративної інформації не враховують ефект від заходів, спрямованих на підвищення безпеки від внутрішніх загроз.

Оцінка ефективності та результативності системи захисту корпоративної інформації повинна здійснюватися керівництвом підприємства з метою контролю

за досягненням цілей та завдань функціонування інформаційної безпеки та визначення напрямків необхідних змін.

Методика оцінки ефективності та економічності системи захисту корпоративної інформації базується на дотриманні низці принципів:

– комплексності – облік кінцевих та безпосередніх результатів функціонування системи захисту корпоративної інформації;

– з урахуванням стадії розвитку корпоративних систем та життєвого циклу корпоративної інформації;

– об’єктивності – виключення суб’єктивних чинників, які впливають результати оцінки;

– рентабельності – витрати ресурсів на оцінку повинні бути меншими за отриманий ефект;

– цифровізації – використання процедур та інформаційних технологій для збирання та обробки даних у процесі оцінки економічної ефективності системи захисту корпоративної інформації.

Кінцевим результатом функціонування системи захисту корпоративної інформації є забезпечення захищеності економічних інтересів корпоративних структур від зовнішніх та внутрішніх загроз у короткостроковій та довгостроковій перспективі. Досягнення кінцевого результату вимагає реалізації комплексу процесів розробки, прийняття та реалізації управлінських рішень, що мають різну тривалість та заплановані терміни реалізації. Для того, щоб спрогнозувати кінцевий результат і виявити потенційні ризики недосягнення цілей у довгостроковій перспективі, необхідно оцінити безпосередні результати функціонування системи захисту корпоративної інформації – результати процесів, вкладених у досягнення цільового рівня економічної ефективності інформаційної безпеки.

Оцінка ефективності системи захисту корпоративної інформації включає порівняння рівня продуктивності з рівнем виконання бюджету щодо створення такої системи.

Запропонований підхід до оцінки ефективності виходить із того, що бюджет витрат на експлуатацію системи захисту корпоративної інформації виправданий і

дозволяє повністю фінансувати заплановані заходи щодо забезпечення інформаційної безпеки корпорацій.

Інформаційною базою для оцінки економічної ефективності системи захисту корпоративної інформації виступили дані 250 українських підприємств, зокрема:

– дані внутрішнього управлінського обліку;

– стратегічний та оперативний плани підприємства, звіти про виконання планів;

– граничні значення показників системи захисту корпоративної інформації підприємств;

– плани забезпечення інформаційної безпеки підприємства та звіти про їх виконання;

– результати ревізій, результати судово-економічних експертиз та інші достовірні джерела інформації.

При проведені апробації запропонованого підходу увійшли погрози конфіденційності, цілісності, доступності інформації, загрози несанкціонованого доступу (НСД), загрози шкідливих програм, з використанням уразливості системного та прикладного програмного забезпечення. Для оцінки економічної ефективності системи захисту корпоративної інформації було залучено сім експертів, з яких сформували експертну комісію з трьох осіб, коефіцієнт конкордації рішень експертів дорівнює W = 0,9. Експерти оцінюють ступінь досягнення максимально можливого прибутку корпоративної структури Y_{ib} для трьох варіантів системи захисту корпоративної інформації за обраними показниками цілісності, доступності та конфіденційності (табл. 4.3).

Після опитування експертів, представленого в таблиці 4.3, отримуємо песимістичні нижнє та верхнє значення, та найбільш очікувані значення ступеня досягнення максимально можливого прибутку корпоративної структури Y_{ib} мінімальні значення означають кращі оцінки. Експерти дають ці значення по сітці від 0 до 1 з кроком 0,1.

Таблиця 4.3

Варіанти системи захисту корпоративної інформації

Характеристика системи захисту корпоративної інформації	Найменш очікувана нижня оцінка	Найбільш очікувана мінімальна оцінка	Найбільш очікувана максимальна оцінка	Найменш очікувана верхня оцінка
конфіденційність				
цілісність				
доступність				

Джерело: розроблено автором

При оцінюванні ступеня досягнення максимально можливого прибутку корпоративної структури Y_{ib} для першої системи, дано кожним експертом оцінки в опорних точках для об'єктів за критеріями цілісності, конфіденційності та доступності. Застосовуючи принцип узагальнення, отримано вихідну функцію приналежності трьох вхідних функцій приналежності для системи захисту корпоративної інформації за трьома критеріям, на основі якої сформовано табл. 4.4.

Таблиця 4.4

Варіанти системи захисту корпоративної інформації

Характеристика системи захисту корпоративної інформації	Найменш очікувана нижня оцінка	Найбільш очікувана мінімальна оцінка	Найбільш очікувана максимальна оцінка	Найменш очікувана верхня оцінка
конфіденційність	0,267	0,300	0,500	0,533
цілісність	0,367	0,400	0,700	0,733
доступність	0,367	0,400	0,667	0,700

Джерело: розроблено автором

Далі визначивши математичне очікування системи захисту корпоративної інформації отримуємо значення ступінь досягнення максимально можливого прибутку корпоративної структур.

Результати проведених розрахунків показника Y_{ib} за результатами діяльності 250 вітчизняних підприємств дозволили оцінити ступінь досягнення максимально можливого прибутку корпоративної структур та визначити рейтингову шкалу оцінки ефективності системи захисту корпоративної інформації, а саме:

– $Y_{ib} \geq 100$ % характеризує високу економічну ефективність системи захисту корпоративної інформації (жодне підприємство не продемонструвало зазначений рівень);

– 75 % $\leq Y_{ib} <$100 % характеризує середню економічну ефективність системи захисту корпоративної інформації (43 з 250 підприємства досягли відповідного значення);

– $Y_{ib} <$ 75 % характеризує низьку ефективність системи захисту корпоративної інформації (207 підприємств продемонстрували низьку економічну ефективність та потребують впровадження заходів щодо підвищення її рівня для досягнення відповідного значення).

Отже, оцінка економічної ефективності системи захисту корпоративної інформації здійснюється з метою моніторингу досягнення цілей і завдань функціонування системи інформаційної безпеки та визначення напрямів необхідних змін.

Кінцевим результатом оцінювання результативності та результативності є формування адекватних заходів, спрямованих на виявлення та усунення проблем функціонування системи захисту корпоративної інформації, зменшення негативного впливу викликів і загроз інформаційної безпеці підприємства, попередження або мінімізацію можливих збитків.

Реалізація зазначених завдань оцінки економічної ефективності системи захисту корпоративної інформації з урахуванням економічного підходу є найважливішим елементом постійно діючого механізму управління розвитком корпоративних структур.

Висновки до розділу 4

1. У ході процесу алгоритмізації процедур, пов’язаних з обробкою та аналізом подій ІБ у межах їх ЖЦ, та відповідно до принципу цілісності, об’єкти захисту (зокрема, КІС підприємств) слід 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 обробка та подій ІБ у рамках їх ЖЦ полягає у побудові взаємних відображень між завданнями ІБ та відповідними методами їх вирішення. У цьому основну роль грають доступні дані, необхідних залучення потенціалу конкретного методу чи моделі у процесах обробка та аналіз 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 ІБ. Така ієрархічна пов’язаність дозволяє отримати біоактивне відображення ІБ об’єкта захисту, маючи необхідні дані моніторингу подій ІБ. Запропонована схема адаптивного моніторингу ІБ, включаючи процедури обробки та аналізу подій ІБ у межах їх ЖЦ, відповідає принципам ієрархічної пов’язаності, цілісності та подібності подій ІБ.

2. Запропоновано доповнення до способу організації процесом управління подіями інформаційної безпеки (ІБ) для підприємства. На відміну від існуючих рішень, деталізований алгоритм підпроцесу «Обробка подій». Дана деталізація носить комплексний характер. Крім того, вона охоплює життєвий цикл події ІБ, це дає моживість в реаліях заповнити потенційні прогалини інформації в створюваній системі управління. Додатковою перевагою, пропонованого рішення, є можливість задіяння даного підпроцесу як незалежний, це дозволяє спростити процедуру управління ІБ підприємства в цілому і знизити витрати на її побудову для невеликих підприємств.

3. Доповнено схему адаптивного моніторингу ІБ, яка включає процедури оброблення та аналізу подій ІБ у межах їх ЖЦ. Запропонована схема відповідає принципам ієрархічної пов’язаності, цілісності та подібності подій ІБ.

4. Запропоновані рішення та доповнення на відміну від аналогічних досліджень характеризуються інваріантністю по відношенню до способів реалізації інфраструктурних рішень ІБ підприємства та, зокрема, його КІС. Це, зрештою, дозволяє, не змінюючи методичний інструментарій, масштабувати даний підхід і адаптувати його для СУІБ різних підприємств.

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

Основні результати розділу опубліковані у наукових працях автора: [1, 2, 3, 4, 8, 11, 12, 24, 27, 29, 33, 34] – відповідно до списку опублікованих праць за темою дисертації на початку роботи.

Список використаних джерел до розділу 4

1. 2021 Cyber Security Statistics the Ultimate List Of Stats, Data & Trends. URL: https://purplesec.us/resources/cyber-security-statistics (дата звернення 03.10.2022).
2. 15 Important Cybersecurity Statistics in 2021 – TitanFile. URL: https://www.titanfile.com/blog/15-important-cybersecurity-statistics-in-2021 (дата звернення 03.10.2022).
3. Goddard W. Cyber Security Statistics 2020 / William Goddard // Information Security. 2021. May 27. URL: https://itchronicles.com/information-security/cyber-security-

statistics-2020/#:~:text=There%20were%20nearly%20550%2C000%20cyber,related%20keywords%20to%20lure%20victims (дата звернення 03.10.2022).

4. State of Cybersecurity 2021. URL: https://www.isaca.org/go/state-of-cybersecurity-2021 (дата звернення 03.10.2022).
5. В Україні в 2020 році зафіксували 1 мільйон кібератак – РНБО. URL: https://ms.detector.media/kiberbezpeka/post/25227/2020-08-07-v-ukraini-v-2020-rotsi-zafiksuvaly-1-milyon-kiberatak-rnbo (дата звернення 03.10.2022).
6. Infosec named an IT training Leader. URL: https://www.infosecinstitute.com/form/infosec-2021-idc-marketscape (дата звернення 03.10.2022).
7. Cyber Observer. 29 must-know cybersecurity statistics for 2020 // Cyber Observer. 2020. March 8.
8. Dimov I. Security awareness statistics // Infosec. 2017. August 29.
9. Widdup S. 2019 Verizon Data Breach Investigations Report. NIST. 2019.
10. Meharchandani D. Staggering phishing statistics in 2020 // Security Boulevard. 2020. December 7.
11. Fior Market Research LLP. Global healthcare cyber security market is expected to reach USD 33.65 billion by 2027: Fior Markets // GlobeNewswire. 2020, September 30.
12. Morgan S. Healthcare industry to spend $125 billion on cybersecurity from 2020 to 2025 // Cybercrime Magazine. 2020. September 8.
13. Seh A. H., Zarour M., Alenezi M., Sarkar A. K., Agrawal A., Kumar R., Ahmad Khan R. Healthcare data breaches: Insights and implications // Healthcare. 2020. № 8(2). P. 133.
14. Fayi S. Y. A. What Petya/NotPetya ransomware is and what its remidiations are // In Information Technology-New Generations. Springer, Cham, 2018. P. 93–100.
15. 10 Cybersecurity Trends for 2022/2023: Latest Predictions You Should Know. URL: https://financesonline.com/cybersecurity-trends (дата звернення 03.10.2022).

16. Deorankar A. V., Thakare S. S. Survey on anomaly detection of (iot)-internet of things cyberattacks using machine learning // In 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2020. P. 115–117.
17. Abdalrahman G. A., Varol H. Defending against cyber-attacks on the internet of things. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS). IEEE, 2019. P. 1–6.
18. The Cybersecurity 202: Global losses from cybercrime skyrocketed to nearly $1 trillion in 2020, new report finds. URL: https://www.washingtonpost.com/politics/2020/12/07/cybersecurity-202-global-losses-cybercrime-skyrocketed-nearly-1-trillion-2020 (дата звернення 03.10.2022).
19. 2019 Official Annual Cybercrime Report / Herjavec Group. URL: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf (дата звернення 03.10.2022).
20. Patel N. Cyber and TRIA: Expanding the Definition of an" Act of Terrorism" to Include Cyber Attacks // Duke L. & Tech. Rev. 2021. № 19. P. 23.
21. Hasan M. F., Al-Ramadan N. S. Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case // Social Science and Humanities Journal. 2021. № 5(8). P. 2312-2323.
22. Ibrahim E. K., Saeed R. N. Organization of Cyber Wars in International Law // Review of International Geographical Education Online. 2021. № 11(4). P. 28–42.
23. Mansurov G. International Legal Mechanisms for Ensuring Digital Security // In SHS Web of Conferences. EDP Sciences, 2021. Vol. 93.
24. Kaushik K., Dahiya S. An Automated Abstract Approach for Investigating Bitcoin Balances and Wallet Addresses // In 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART) IEEE, 2021. P. 444–448.
25. Paul J. A., Zhang M. Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker // European Journal of Operational Research. 2021. № 291(1). P. 349-364.

26. Sawik T., Sawik B. A rough cut cybersecurity investment using portfolio of security controls with maximum cybersecurity value // International Journal of Production Research. 2021. P. 1-17.
27. Wang P., D'Cruze H. Honeypots and knowledge for network defense // Issues in Information Systems. 2021. № 22(3). P. 241–254.
28. Pasdar A., Meghdadi M., Medi A. Stabilisation of multi-loop amplifiers using circuit-based two-port models stability analysis // IET Circuits, Devices & Systems. 2021. № 15(6). P. 553–559.
29. Saleem K., Fisal N., Hafizah S., Rashid R. A. An intelligent information security mechanism for the network layer of WSN: BIOSARP // In Computational intelligence in security for information systems. Berlin, Heidelberg : Springer, 2011. P. 118–126.
30. Lakhno V., Akhmetov B., Chubaievskyi V., Desiatko A., Palaguta K., Blozva A., Chasnovskyi Y. Information Security Audit Method Based on the Use of a Neuro-Fuzzy System // In Proceedings of the Computational Methods in Systems and Software. Springer, Cham, 2021. P. 171–184.
31. White G. Generation Z: Cyber-Attack Awareness Training Effectiveness // Journal of Computer Information Systems. 2021. P. 1–12.
32. 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.
33. 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.
34. 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.
35. 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.

36. 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.
37. Хох В. Д., Мелешко Е. В., Смірнов О. А. Дослідження методів аудиту систем управління інформаційною безпекою // Системи управління, навігації та зв'язку : Збірник наукових праць. 2017. № 1(41), С. 38–42.
38. Бегун А. В. Про одну з ситуаційних моделей управління інформаційною безпекою підприємства / А.В. Бегун, О.І. Осипова, О.Г. Урденко // 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.
39. 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.
40. 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.
41. Kang K., Kim J. (2015). 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.
42. 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.
43. Siponen M., Willison R. Information security management standards: Problems and solutions // Information & management. 2009. № 46(5). P 267–270.
44. Ključnikov A., Mura L., Sklenár D. Information security management in SMEs: factors of success // Entrepreneurship and Sustainability Issues. 2019. № 6(4). P. 2081.

45. Shatnawi M. M. Applying Information Security Risk Management Standards Process for Automated Vehicles // Bánki Közlemények (Bánki Reports). 2019. № 2(1). P. 70–74.
46. 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.
47. Кожедуб Ю. Аналіз документів з керування ризиком кібербезпеки // Information Technology and Security. 2017. Т. 5. № 1. С. 82–95.
48. Овчаренко М. Ю. Аналіз правил кореляції в системах управління інформаційною безпекою та подіями безпеки / М. Ю. Овчаренко, О. В. Сєвєрінов // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доповідей одинадцятої міжнародної науково-технічно ї конференції, 8–9 квітня 2021 р. ВА ЗС АР; НТУ "ХПІ"; НАУ, ДП "ПДПРОНДІ-АВІАПРОМ"; УмЖ, 2021. Т. 2, секції 3-5. С. 46.
49. Ушатов В., Сєвєрінов О.В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. Харків : ХНУРЕ, 2019. С. 104–105.
50. 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.
51. Miller D. et al. Security information and event management (SIEM) implementation. McGraw-Hill, 2011.
52. National Institute of standards and technology. Special Publication 800-92. Guide to Computer Security Log Management. 2006. 61 p.
53. ITIL Service Operation Second edition. 2011. P. 58–72.
54. Печенюк А. Особливості організації інформаційної безпеки сучасного підприємства // Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації. 2014. № 2. С. 165–168.
55. 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.

56. 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.
57. 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.
58. Yakymenko Y., Muzhanova T., Lehominova S. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FIREEYE // Електронне фахове наукове видання «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).
59. Check Point Software Technologies Ltd. 2021. The Biggest Cloud Security Challenges of 2021. https://pages.checkpoint. com/2020-cloud-security-report.html?utm_term=cyber-hub; Kent, J. 2020. “APIs are the next frontier in cybercrime”. Security. 3 September 2020. URL: https://www.securitymagazine.com/articles/93239-apis-are-the-next-frontier-in-cybercrime (дата звернення: 08.10.2022).
60. Hoster B., Sequeira T. Harnessing Technology Convergence: Lessons from Smart Manufacturers. Marsh McLennan. 2021. URL: https://www.marshmclennan.com/insights/ publications/2021/may/harnessing-technology-convergence.html (дата звернення: 08.10.2022).
61. Solyanoy V. N. Features in Building an Expert System for Economic Efficiency Assessment of Information Security Measures // Information and Technology Bulletin. 2017. Vol. 13, № 3. P. 127–136.
62. Hohan A. I., Olaru M., Pirnea I.C. Assessment and Continuous Improvement of Information Security Based on TQM and Business Excellence Principles // Emerging Markets Queries in Finance and Business. 2015. Vol. 32. P. 352–359.

63. Kim M. A study on a model of convergence security compliance management for business security. Journal of Information and Security. 2016. № 16 (5). P. 81–86.
64. Von Solms R., Niekerk J. V. From information security to cyber security // Computers & Security. 2013. № 38. P. 97–102.
65. Обсяг піратського програмного забезпечення в Україні становить понад 80% – дослідження / Інститут масової інформації. URL: https://imi.org.ua/news/obsyagpiratskogo-programnogozabezpechennya-v-ukrajini-stanovitponad-80-doslidjennya-i14894 (дата звернення: 08.10.2022).
66. Kim H., Ko K., Lee J. Status of corporate information protection system according to amendment of information and communication network act and comparison of certifcation standard of information protection management system // Korea Institute of Information Security And Cryptology. 2013. № 23 (4). P. 53–58.
67. Bernard R. Information lifecycle security risk assessment: A tool for closing security gaps // Computers & Security. 2007. № 26 (1). P. 26–30.
68. Chubaievskyi V. Svitova praktyka upravlinnja podijamy informacijnoi' bezpeky korporacij. Zovnishnja torgivlja: ekonomika, finansy, pravo. 2022. No 6. S. 73-82. Serija. Ekonomichni nauky. https://doi.org/ 10.31617/3.2022(125)05
69. Чубаєвський В. І. Особливості формування системи захисту інформаційних ресурсів корпоративних структур // Фаховий електронний науково-практичний журнал «Проблеми сучасних трансформацій. Серія: економіка та управління». 2022. № 5. URL: https://reicst.com.ua/pmt/article/view/2022-5-04-10/2022-5-04-10 (дата звернення: 01.11.2022).

РОЗДІЛ 5
МЕТОДИ ПІДВИЩЕННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ

5.1. Організаційно-економічне забезпечення ефективного захисту корпоративної інформації

Реалізація концепції інформаційної безпеки потребує створення та впровадження в практику корпоративного управління належного організаційно-економічного забезпечення.

В сучасних наукових дослідженнях спостерігається плюралізм підходів до визначення та тлумачення змісту поняття «організаційно-економічне забезпечення».

Так, Л. Довгань визначає організаційно-економічне забезпечення функціонування підприємств як «систему формування цілей і стимулів, які дозволяють перетворити у процесі трудової діяльності рух (динаміку) матеріальних і духовних потреб членів суспільства на рух засобів виробництва і його кінцевих результатів, спрямованих на задоволення платоспроможного попиту споживачів» [1]. Таким чином, автор асоціює організаційно-економічний механізм з системою цілей та стимулів. На наш погляд, така трактовка є досить вузькою і не відображає повною мірою змісту цього поняття.

Г. Пономарьова при визначенні змісту організаційно-економічного забезпечення зазначає, що він ґрунтується на «тенденціях розвитку підприємства, враховує досягнутий науково- технічний рівень його розвитку, соціальні, правові та психологічні відносини в колективі підприємства в процесі управління» [2], а основний акцент при його вивченні робиться на правовому забезпеченні. На наше переконання зазначений підхід з одного боку чітко не визначає сутність цього поняття, а з іншого боку обмежує його змістовні компоненти, так як правові засоби забезпечення функціонування підприємства не вичерпують його організаційно-економічне забезпечення.

С. Кучер розглядає організаційно-економічне забезпечення підприємства як «сукупність заходів і засобів, створення умов, які сприяють протіканню економічних процесів, реалізації намічених планів, програм, проектів тощо» [3]. На наш погляд, такий підхід з-поміж інших найбільшою мірою відображає зміст цього поняття.

О. Шилова, навпаки, пропонує розуміти під організаційно-економічним забезпеченням розвитку підприємства тільки «процес управління для досягнення мети розвитку шляхом реалізації системи цілей підприємства як результату використання його ресурсів» [4]. На нашу думку, ототожнення організаційно-економічного забезпечення з процесом управління є дещо хибним підходом. Така трактовка по суті означає відсутність потреби у виокремленні цього поняття та його подальшого вивчення.

М. Молла досліджує організаційно-економічне забезпечення функціонування крізь призму вивчення його компонентів. Авторка виокремлює організаційну та економічну складові з подальшим розподілом на організацію виробничого процесу, виробничої інфраструктури, забезпечення контролю якості продукції, праці та організацію комерційної діяльності; на персонал підприємства, виробничі можливості підприємства, ділову активність підприємства, фінансову стійкість, платоспроможність підприємства, прибутковість підприємства [5]. Проте складно погодитись, що компонентами організаційно-економічного забезпечення виступають, по суті елементи ресурсного забезпечення та параметри фінансового стану.

В. Грицишин визначає організаційно-економічне забезпечення з позицій системного підходу, розглядаючи його як: «сукупність підсистем та елементів ринкового середовища, до яких можна віднести фінансову, організаційну, кадрову, інформаційну та правову підсистеми» [6]. Зазначений підхід розширює межі організаційно-економічного забезпечення, включаючи в нього не лише внутрішньокорпоративні елементи, а і елементи зовнішнього середовища.

Аналогічний підхід постулюється у дослідженні Т. Лебедика, який зазначає, що структура організаційно-економічного забезпечення за функціональною

ознакою повинна включати три підсистеми: «державне регулювання, саморегулювання на мікрорівні, громадське регулювання... форму поєднання елементів ринкової саморегуляції з елементами демократичного державного регулювання» [7]. Таким чином, важливою ознакою організаційно-економічного забезпечення є взаємодія його окремих елементів.

В окремих дослідженнях автори ототожнюють поняття організаційно-економічного забезпечення з поняттям економічного механізму. Так, зокрема, В. Семенов, С. Галасюк, О. Шишкіна вважають, що «визначальним базовим поняттям для з'ясування сутності організаційно-економічного забезпечення є поняття «механізм» у безлічі інтерпретацій в залежності від складових: економічні, політичні, правові, соціальні, культурні, інноваційні, інвестиційні механізми тощо, які будуть змінюватися, залежно від відносин власності й способів виробництва, застосовуваних у тій або іншій суспільній формації, кожний з яких є за своєю суттю механізмом управління в умовах змін, що відбуваються, відповідно до критерію динаміки» [8]. Виходячи з цього, під організаційно-економічним забезпеченням автори розуміють «системну реакцію, адекватну зовнішнім і внутрішнім впливам, а також механізми, важелі, інструменти та заходи з планування, фінансування, управління, які дають можливість не тільки узгоджувати, коригувати, враховувати та реалізовувати інтереси підприємства, але й сприяти синергетичному ефекту від розширення функціональних можливостей … підприємств …» [8]. Погоджуючись з тим, що базисом дослідження сутності та змістовного наповнення організаційно-економічного забезпечення є економічний механізм, ми не поділяємо думку щодо необхідності ототожнення цих понять. На наш погляд, організаційно-економічне забезпечення є важливою складовою економічного механізму підприємства, яке спрямоване на практичну реалізацію поставлених перед підприємством завдань в цілому, та за окремими функціональними напрямами управління.

М. Богославський акцентує увагу на необхідності інтеграції організаційно-економічного забезпечення корпоративної безпеки в систему корпоративного управління, зазначаючи, що «характерна риса та відмінність підходу щодо вирішення питання забезпечення економічної безпеки АТ полягає в необхідності

розгляду корпоративної безпеки саме як важливої характеристики організаційно-економічної побудови системи корпоративного управління на основі обов'язкового та повного дотримання ключових принципів розбудови системи корпоративних відносин» [9]. Виходячи з цього у комплексі організаційно-економічного забезпечення корпоративної безпеки акціонерного підприємства автором виділено три складові: соціально-економічну, корпоративно-організаційну, соціокультурну, елементи яких мають бути розподілені та систематизовані за трьома рівнями (нормативно-організаційний, інструментально-методичний, операційний) [9].

На думку А. Нашинець-Наумової складниками єдиної системи забезпечення інформаційної безпеки корпорацій є [10]:

– державна система, представлена правоохоронними органами та спецслужбами (наприклад, Служба безпеки України, Рада національної безпеки і оборони України);

– недержавна система, представлена приватними охоронними, охоронно–технічними підприємствами, комерційними службами безпеки, підприємствами різної форми власності, інформаційними бюро, службами безпеки банків, профільними факультетами, кафедрами вищих навчальних закладів [10].

Таким чином, в системі такого забезпечення автор по суті виокремлює організаційні структури не лише внутрішнього, а і зовнішнього по відношенню до підприємства характеру, які безпосередньо, або опосередковано забезпечують корпоративну інформаційну безпеку.

На думку З. Валіулліної ефективне функціонування інформаційної безпеки корпоративної економіки в умовах глобалізаційних процесів необхідно розглядати як сукупність державної та недержавної системи захисту. А основними компонентами її забезпечення авторка вбачає: законодавчу, економічну, програмно-технічну та адміністративно-управлінську складові [11].

Розуміння сутності та змісту організаційно-економічного забезпечення інформаційної безпеки суттєво залежить і від тенденцій розвитку інформаційного суспільства та тих загроз, що генерує процес цифровізації економіки.

За оцінками експертів, основні тенденції кібербезпеки в майбутньому будуть наступними [12, 13]:

1) Гібридні кібернетичні загрози (кібер-холодна війна) будуть посилюватися.

2) Подальший розвиток і використання досягнень штучного інтелекту.

3) Засоби зв'язку будуть використовуватися з більш наступальними цілями.

4) Розробки 5G мереж і впровадження пристроїв інтернету речей (IoT) будуть підвищувати вразливість до атак.

5) Організації переосмислять свій підхід до хмарних технологій.

Таким чином, на сьогоднішній день постає завдання інтегрованого впровадження інформаційних технологій одночасно з вбудованим модулем інформаційної безпеки, що потребує синхронного запровадження організаційно-економічних заходів підтримки інформаційної безпеки поряд із запровадженням самих інформаційних технологій в корпоративну практику. Так, Ю. Борсуковський розглядає таке забезпечення крізь призму побудови відповідної організаційної структури служби інформаційної безпеки та заходів, які реалізуються нею щодо захисту корпоративної інформації. При цьому автор класифікує такі заходи за організаційним, процедурним та програмно-технічним рівнями, деталізуючи кожен з них [14].

Р. Грищук та С. Євсєєв організаційно-економічне забезпечення інформаційної безпеки розглядають крізь призму сучасних методологічних підходів її забезпечення, зокрема синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси, оцінки рівня захищеності державних ресурсів від соціотехнічних атак; оцінювання шкоди національній безпеці у сфері охорони державної таємниці, побудови та застосування безпечних бездротових сенсорних мереж з випадковими параметрами мережі, захисту державних інформаційних ресурсів, аналізу стану комплексу технічного захисту інформації, аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів, побудови систем виявлення аномалій породжених кібератаками, систем аналізу та оцінки ризиків втрат інформаційних ресурсів, комплексного захисту людини та соціальних груп від негативного

інформаційно-психологічного впливу, адаптивних систем оцінювання ризиків безпеки ресурсів інформаційних систем та ін. Виокремлюючи недоліки та прогалини цих методів автори пропонують власну методологію побудови системи забезпечення інформаційної безпеки, яка включає п’ять етапів з відповідним методичним наповненням: 1) визначення ймовірності впливу загроз на інформаційну безпеку; 2) визначення узагальненого показника рівня інформаційної безпеки;3) оцінювання ефективності інвестицій в інформаційну безпеку; 4) побудова інтегрованих механізмів забезпечення конфіденційності, цілісності, автентичності та вірогідності загроз інформації; 5) визначення стану та формування стратегій інформаційної безпеки [15].

І. Маркіна та Ю. Гарічев в системі організаційних заходів забезпечення інформаційної безпеки виокремлюють їх три рівні залежно від частоти та постійності реалізації: організаційні разові заходи; заходи за потребою; періодичні заходи, що проводяться при здійсненні, або виникненні певних змін у автоматизованій системі або зовнішньому середовищі; необхідні заходи, які проводяться постійно (безперервно або дискретно) [16]. Автори детально висвітлюють склад організаційних заходів за кожною виокремленою групою. Проте, на наш погляд інтенсивність запровадження і використання окремих заходів інформаційної безпеки суттєво детермінується станом та динамікою зовнішнього середовища та індивідуальними особливостями функціонування підприємства. Тому, більш доречними нам вбачаються інші критерії поділу таких заходів.

Аналіз, узагальнення та розвиток наявних підходів до визначення та структуризації організаційно-економічного механізму підприємства та забезпечення інформаційної безпеки, зокрема, дозволили нам виокремити його наступні сутнісні характеристики:

– складова економічного механізму підприємства;

– комплекс узгоджених елементів, які перебувають у щільній взаємодії;

– цільова спрямованість;

– охоплює елементи внутрішнього та зовнішнього корпоративного середовища;

– окремі елементи мають різну функціональну спрямованість та частоту застосування.

Окрім вищевідзначених характеристик, нами пропонується додати наступні:

1. Елементи забезпечення відповідають окремими контурам управління, з огляду на те, що формування корпоративної безпеки та її інформаційної складової реалізується за усіма контурами управління: стратегічному, тактичному та оперативному;

2. Організаційно-економічне забезпечення інтегроване в загально–корпоративну структуру управління і є її невід'ємною складовою з огляду, на необхідність постійної взаємодії та координації дій служби безпеки з іншими функціональними підрозділами підприємства.

Таким чином, в узагальненому вигляді концепт організаційно-економічного забезпечення безпеки корпоративної інформації можна представити наступним чином (рис. 5.1).

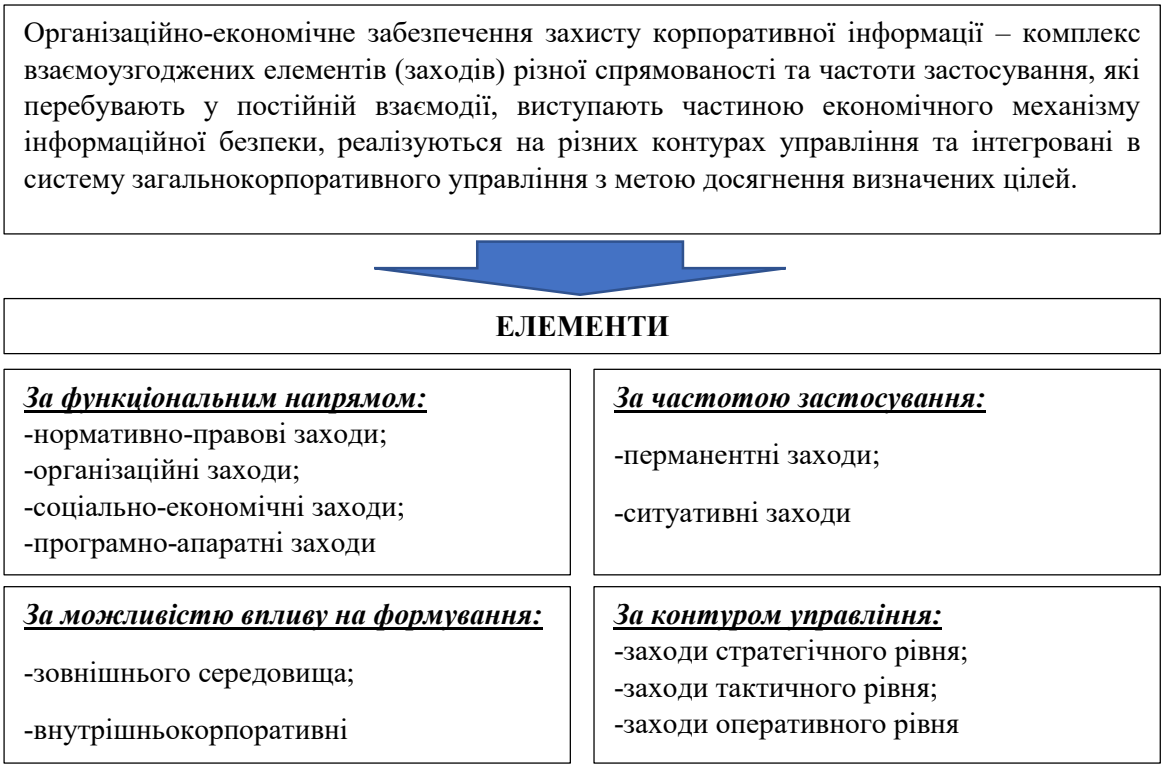


Рис. 5.1. Концепт організаційно-економічного забезпечення захисту корпоративної інформації

Джерело: розроблено автором

У більш розгорнутому вигляді склад елементів організаційно-економічного забезпечення захисту корпоративної інформації представлено в дод. В.

На стратегічному контурі управління реалізуються інструменти зовнішнього та внутрішньокорпоративного характеру. Так, серед зовнішніх елементів організаційно-економічного забезпечення захисту корпоративної інформації варто виокремити міжнародне та національне законодавство у сфері безпеки та інформації; національні стратегії економічного розвитку та розбудови інформаційного суспільства, систему державного регулювання в інформаційній сфері.

Внутрішньокорпоративні елементи цього рівня включають: задокументовані цілі та концепцію інформаційної безпеки, політику управління інформаційними ризиками, організаційну структуру служби безпеки, структуру розподілу корпоративного контролю, загальнокорпоративну стратегію розвитку, архітектуру та холархію корпоративних відносин, мотиваційні комплекси учасників корпоративного управління, заходи з формування програмно-технічного комплексу, що забезпечує збір, обробку, зберігання та захист інформації. Особливістю заходів стратегічного контуру є їх постійний характер. Саме вони визначають архітектоніку застосування всіх наступних заходів, що реалізуються на тактичному та оперативному рівнях.

На тактичному рівні реалізується система заходів у межах визначеної стратегічної канви, яка по суті є ядром захисту корпоративної інформації. Так, у частині нормативно-правових заходів здійснюється формування та запровадження основних політик та процедур, що стосуються інвентаризації інформаційних активів, застосування превентивних та коригуючих заходів захисту; антивірусної, парольної політик, регламентів розмежування доступу до систем тощо.

У частині організаційних заходів здійснюється та фіксується розподіл обов’язків із захисту корпоративної інформації, організуються тренінги та навчальні програми щодо цифрових компетентностей та захисту інформації, організується фіксація інформації про інциденти безпеки.

У системі соціально-економічних заходів реалізуються основний комплекс заходів із планування, аналізу, контролю та обліку витрат та вигід від запровадження заходів захисту корпоративної інформації.

У системі програмно-апаратних заходів здійснюються процедури ідентифікації/аутентифікації, розмежування доступу до інформації та систем, протоколювання та аудит інформаційних систем, екранування та сегментація, тунелювання та шифрування інформації. Зазначені заходи також здебільшого варто здійснювати на постійній основі.

У системі оперативних заходів правового та організаційного характеру варто виокремити формування інструкцій щодо здійснення окремих операцій та процедур з інформаційної безпеки, заходи щодо їх коригування, фізичне управління доступом до інформації, захист підтримуючої інфраструктури, процедури реагування на інциденти безпеки, спецперевірки тощо.

В економічно-соціальному елементі оперативних заходів реалізуються процедури із документування втрат від інцидентів безпеки, моніторинг грошових потоків, пов’язаних із процедурами захисту корпоративної інформації, заходи з коригування бюджетів інформаційної безпеки.

Програмно-апаратні заходи оперативного рівня передбачають резервне копіювання, управління носіями інформації, контроль цілісності та захищеності, організація явного та прихованого контролю за роботою користувачів та персоналу системи. Як видно, система заходів оперативного рівня є більш «лабільною», частина з них може носити ситуативний характер.

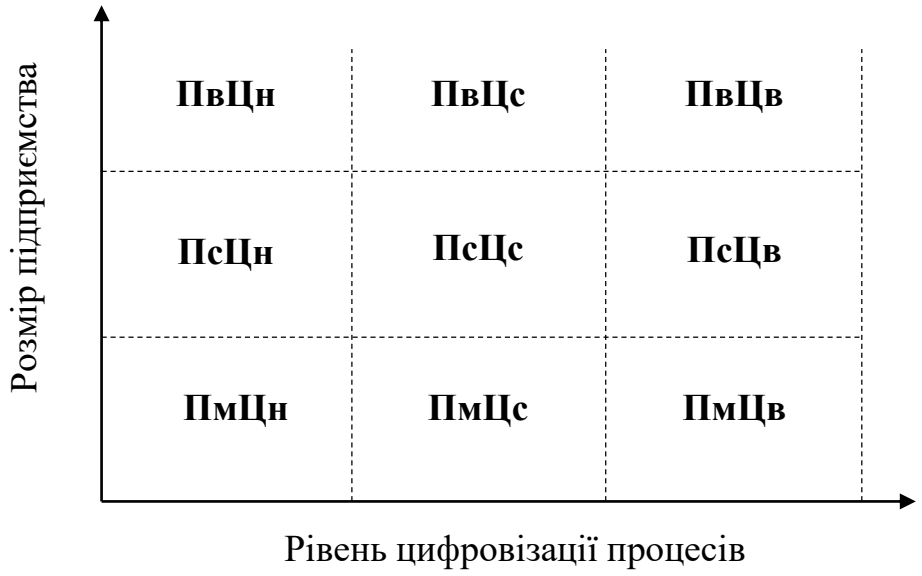
У цілому представлений комплекс заходів організаційно-економічного забезпечення захисту корпоративної інформації не є сталим за переліком заходів та фіксованим щодо різних підприємств. Набір таких заходів визначається цілою низкою факторів, основними з яких, на наш погляд, є:

– розмір підприємства, який часто визначає і рівень цифровізації процесів, кваліфікацію персоналу тощо;

– рівень інтернаціоналізації підприємства: чим вищий рівень інтернаціоналізації, тим вищі вимоги до стандартів комунікації з іноземними партнерами, що призводить також до вищого рівня цифровізації компанії;

– рівень цифровізації підприємства.

Таким чином, основними факторами вибору та формування системи організаційно-економічного забезпечення захисту корпоративної інформації є дві принципові змінні «розмір підприємства – рівень його цифровізації», що формує шкалу вибору таких заходів (див. рис.5.2).



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

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

Рис. 5.2. Типологія підприємств, що визначає вибір організаційно-економічних заходів захисту корпоративної інформації

Джерело: складено автором

Так, підприємства різного розміру з низьким рівнем цифровізації процесів реалізують досить обмежене організаційно-економічне забезпечення корпоративної інформаційної безпеки. Якщо на великому підприємстві може виокремлюватись фахівець із захисту корпоративної інформації в межах служби

безпеки, то на середніх і малих ці функції покладаються на окремих посадових осіб, які не є фахівцями в даній галузі.

На підприємствах із середнім рівнем цифровізації варто виокремлювати фахівця із захисту корпоративної інформації, або в межах служби безпеки, або як окрему штатну позицію, з огляду на те, що такий рівень уже передбачає помірний набір заходів із забезпечення інформаційної безпеки. Її перелік та номенклатура обумовлюються специфікою діяльності підприємства, рівнем уразливості підприємства до інформаційних загроз та розміром підприємства.

Підприємства з високим рівнем цифровізації потребують розширеного переліку заходів із забезпечення інформаційної безпеки. У великих корпоративних структурах може формуватися підрозділ із забезпечення інформаційної безпеки (як окремий, так і в межах служби безпеки), з відповідними цифровими компетентностями та реалізовуватися широкий комплекс заходів. Середні та малі підприємства з високим рівнем цифровізації також потребують запровадження широкого спектру організаційно-економічного забезпечення захисту корпоративної інформації. Тим більше, що малі підприємства з високим рівнем цифровізації часто представлені стартапами, процеси яких повністю цифровізовані, підприємствами e-commerce, які потребують високого рівня захисту інформації. Відмінністю середніх та малих компаній цього сегменту є більш проста організаційна структура служби безпеки. На таких підприємствах доцільно запроваджувати посаду відповідального за інформаційну безпеку.

Таким чином, створення організаційно-економічного забезпечення захисту корпоративної інформації є необхідним елементом досягнення ефективності цього процесу, а набір елементів такого забезпечення диференціюється залежно від розміру, структури, рівня цифровізації процесів підприємства.

5.2. Методика аудиту інформаційної безпеки підприємства

Динаміка збільшення кількості та складності кібератак на різні об’єкти інформатизації (ОБІ) лише за останні кілька років [17, 18] показує, що, не дивлячись на всі зусилля сторони захисту, протиставити атакуючим все більш технічно досконалі апаратно-програмні засоби інформаційної безпеки (ІБ) та 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 [19]. Адже несанкціоноване втручання в комп’ютерні системи (КС) може спричинити збій у бізнес-процесах і позначитися на безпеці людей. Наприклад, навіть короткочасна відмова КС, зокрема, підприємств комунальної сфери здатна викликати перебої в постачанні електроенергії, води, перебої в постачанні в 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 (СУІБ). Якийсь важливий об’єкт інформатизації апріорі передбачає необхідність мати сучасну систему управління, зокрема, у питаннях, що стосуються ІБ. Такі системи сьогодні стали невід’ємною частиною систем менеджменту (СМ). А інтеграція подібних СМ 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 (АІБ) для різних ОБІ присвячено чимало робіт. У цій черзі можна згадати роботи, що стали класичними для вирішення завдань АІБ [20, 21].

У роботі [22] 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 роботі [23] аналізується взаємозв’язок процедур внутрішнього аудиту ІБ та зовнішнього аудиту. Проте авторами не прийнято до уваги постійний розвиток систем захисту ІБ. Зауважимо, що в контури ІБ нових передових систем ІБ здатна змінити перелік базових метрик ІБ, прийнятих в організації.

У [24] аналізуються особливості 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).

У [25, 26] авторами також помічено, що, хоча постійне вдосконалення СЗІ необхідне, проте це «вигідно» переважно виробникам ЗЗІ. І лише одне вдосконалення ЗЗІ не здатне самостійно вирішити проблему постійного протистояння СЗІ та загроз ІБ. Більше того, як показано в [27, 28], якщо сторона захисту стикається із цільовою (таргетованою) атакою, то покладатися лише на ЗЗІ буде помилкою.

У зв’язку із цим багатьма експертами [24, 29, 30] наголошується на необхідності застосування не тільки технічних підходів (використання ЗЗІ) для протидії кібернетичним загрозам, але впровадження комбінованих методів. Авторами детально не розкрито поняття комбінованих методів, але згадується необхідність їх побудови на базі сімейства стандартів ISO серії 27001 та 19011 [31–35].

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 залежить від ландшафту кіберзагроз, сформованих практиками забезпечення ІБ ОБІ [77].

Вирішення зазначеної проблеми, зокрема, передбачає необхідність перегляду існуючих статичних моделей управління ІБ. Як одне з підзавдань, слід згадати необхідність удосконалення системи АІБ. Отже, процедура прийняття рішень особою, яка приймає рішення при фіксованій кількості альтернатив, передбачає необхідність створення нових підходів до процедур аудиту ІБ [77].

Зазначимо, що методологія проведення аудиту ІБ добре відома та відпрацьована фахівцями, але поки що не до кінця відпрацьованими 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). І це робить завдання підвищення ступеня захищеності і навіть отримання поточних і прогнозних оцінок ІБ ОБІ релевантної.

Вирішення завдання підвищення ступеня захищеності, а також отримання поточної та прогнозної оцінки ІБ ОБІ найбільш доцільно, застосовуючи точні чисельні оцінки – метрики ІБ [20, 21].

Це відповідає основним положенням «базового» стандарту системи управління інформаційною безпекою 27004:2009 [33]. Як джерела даних у ході реалізації процедур аудиту ІБ (як внутрішнього, так і зовнішнього) можуть бути використані такі відомості [22]:

– 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 [77].

Таким чином, 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;

– розробка та апробація інтелектуальної системи підтримки прийняття рішень, спрямованих на збільшення ступеня ІБ з можливістю синтезу чисельної оцінки результативності аудиту ІБ ОБІ.

При розробці програми проведення аудиту ІБ (далі ПАІБ) не всі зв’язки між свідченнями АІБ можуть ураховуватися в конкретній ситуації. Це, передусім, зумовлено відсутністю необхідної інформації [77].

Під час проведення аудиту ІБ великих компаній чи підприємств об’єкт аудиту повністю розглянути цілком досить складно. Аудиторам доцільніше вибрати найважливіші інформативні свідоцтва аудиту або метрики ІБ. Дані відібрані метрики матимуть велику значущість і вартість їх отримання буде невисока.

Зазвичай для того побудувати модель об’єкта АІБ (далі ОАІБ) доцільно задіяти вагові коефіцієнти значущості свідчень аудиту.

Як показала реальна практика проведення аудитів ІБ, облік значущості свідоцтв аудиту є складним завданням. При цьому важливим фактором є досвід аудитора і, насамперед, особи, яка відповідає за складання програми АІБ і системний аналіз результатів, що одержуються в процесі аудиту. Не коректна постановка вихідних завдань АІБ може звести до нуля головну мету АІБ ОБІ, що проводиться, або дати недостовірні результати. Усе вищесказане й обумовлює ефективність комбінації експертних та математичних методів обробки отриманих експертних оцінок. Як показав аналіз літературних джерел [26, 36], на вирішення зазначеного вище завдання можуть застосовуватися такі методи: парних порівнянь; бальних оцінок; векторів переваг; аналізу ієрархій (МАІ) та ін.

Досить докладний аналіз результативності застосування цих методів представлений у [36].

Ураховуючи, що відбір метрик ІБ для кожного ОБІ має свої особливості, що диктуються як галуззю ОБІ, так і ступенем його критичності, далі формалізуємо типове завдання відбору метрик АІБ. У цьому пропонується керуватися таким алгоритмом, див. рис. 5.3.

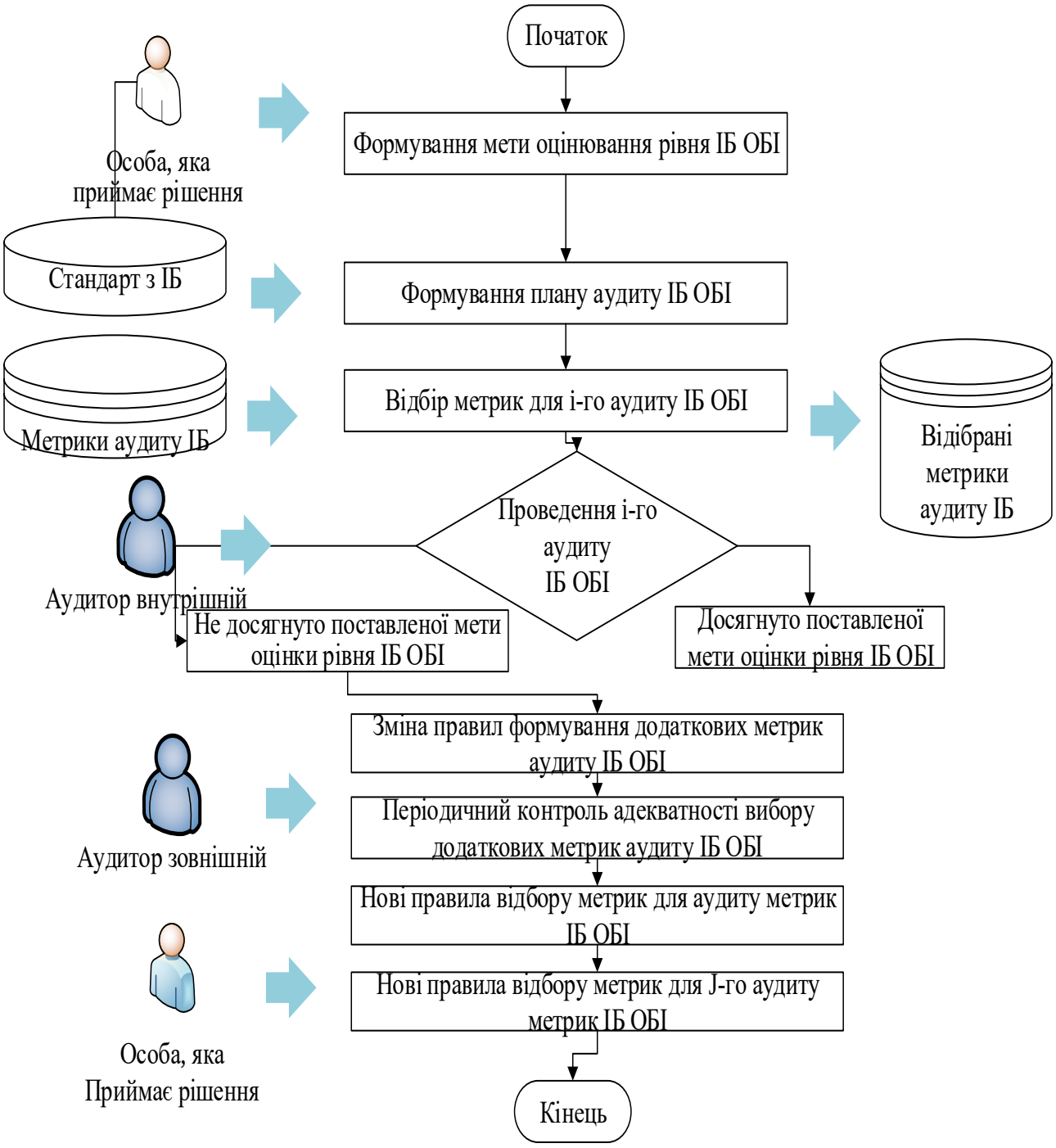


Рис. 5.3. Блок-схема алгоритму відбору індивідуальних критеріїв (метрик ІБ)

Джерело: розроблено автором

У модифікованому алгоритмі проведення аудиту ІБ порівняно з базовими процедурами необхідно брати до уваги такі нові обставини [77]:

1. Слід орієнтуватися, насамперед, на відібрані аудиторами пріоритетні метрики ІБ. Ці відібрані аудиторами метрики могли раніше не зустрічатися протягом попереднього циклу процедури аудиту ІБ ОБІ;

2. Слід контролювати відхилення, що з’явилися, у якісних характеристиках відібраної метрики ІБ.

3. Слід формувати правила відбору та заміни раніше відібраних метрик ІБ, наприклад, керуючись результатами попередніх аудитів ІБ, або у зв’язку із зміною ландшафту 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. Наприклад, сюди відносяться 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 [36–39] модифікувати МАІ за рахунок додаткового застосування наступних кроків:

крок 1. Оцінюємо стійкість локальних ранжирувань на основі векторів змін елементів матриць парних порівнянь;

крок 2. Знаходимо експертні оцінки парних порівнянь, які найбільше впливають на зміну локальних ранжирувань альтернатив рішень та зміну рівнів узгодженості множини оцінок;

крок 3. Оцінюємо чутливість глобального ранжирування 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 [77].

У MAI для того, щоб знайти ранг p_i об’єкта застосовують формулу:

$$p_i = \sum_{j=1}^{n} g_j \cdot v_{ij}, \quad (5.1)$$

де n – кількість критеріїв (метрик ІБ);

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 [40]:

$$y = f\left(\sum_{i=0}^{N} w_i \cdot u_i\right), \quad (5.2)$$

де N – кількість входів нейрона;

w_i – синаптичні ваги входів;

w_0 – порогове значення;

u_i – вхідний сигнал i-го нейрона; u_0 = -1;

y –вихідний сигнал нейрона.

Очевидно 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.

Ураховуючи специфіку завдання проведення аудиту ІБ, пропонують такі зміни для модифікації MAI. Це дозволяє не тільки врахувати специфіку предметної області проведення АІБ ОБІ, а й наступної адаптації запропонованих змін

практичної реалізації інтелектуальної СППР з допомогою методів об’єктно-орієнтованого проєктування.

По-перше, уведемо 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. Це залежить від призначення та функціоналу, які реалізовані інформаційними системами ОБІ. Уважаємо, що множина загальних критеріїв, наприклад, надійність, вартість, є обмеженою та постійною.

Водночас кожна процедура АІБ ОБІ має враховувати його специфіку. Ураховуємо ці індивідуальні критерії (метрики ІБ) в окремій множині. Індивідуальні критерії є виключно важливими для конкретного ОБІ. Якщо хоча б один критерій не виконаний, стан захисту ОБІ не задовольняє необхідному рівню 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 стає можливим, тому обставини, що кількість загальних критеріїв щодо забезпечення ІБ ОБІ порівняно невелика. Як показала практика, більшість практик забезпечення ІБ вирішальними стають відібрані чотири – п’ять критеріїв (метрик ІБ).

По-третє, унесемо 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 даному нейрону. Крім того, беремо до уваги індивідуальні критерії ІБ ОБІ [77].

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 $\{Z_j\}$, $j \in [1, m]$, яка містить індивідуальні критерії (метрики ІБ) ОБІ, m – кількість індивідуальних критеріїв.

Виконання порівняльної оцінки важливості загальних критеріїв передбачає такі етапи [77].

Етап 1. Керуючись необхідним рівнем ІБ ОБІ, експерт представляє важливість усіх 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 за рахунок нормалізації елементів на інтервал:

$$u_i = \frac{Y_i}{\sum_{j=1}^{n} Y_j}. \quad (5.3)$$

Отримана множина $\{u_i\}$ буде містити порівняльні показники важливості загальних критеріїв ІБ, які аналізуються в ході проведення АІБ ОБІ [77].

Нейронна мережа (НС), 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 із нейронів має кількість входів, що дорівнює кількості загальних вимог n. На виході нейронів буде формуватися значення, яке і визначить ранг відповідного об'єкта аудиту [77].

База нечітких правил (БНП) відбору індивідуальних метрик аудиту ІБ, що дозволяє розрахувати синаптичні ваги входів кожного з нейронів, включатиме правила виду [77]:

$$\{R^k\}:\ IF\ (x_k\ this\ A_k)\ THEN\ w_k = c_k,$$

$$w_i = \frac{\sum_{k=1}^{K} \mu_{A_k}\cdot(x_k)\cdot w_k}{\sum_{k=1}^{K} \mu_{A_k}\cdot(x_k)} \cdot \prod_{j=1}^{m} \mu_{z_j} \cdot (z_j), \qquad (5.4)$$

де $\{R^k\},\ k \in [1, K]$ – БНП, яка містить K нечітких правил;

$c_k,\ k \in [1, K]$ – константа, яка залежить від конкретного правила, $c_k \in (0,10]$;

$A_k = \{x_k, \mu_{Ak}(x_k)\},\ k \in [1, K]$ – нечіткі множини, які задані функціями належності $\mu_{Ak}(x_k)$ 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 належності $\mu_{Zj}(z_j)$, 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 випадках, 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 усіх типів; інформація про інциденти ІБ; інформація про нові переваги в 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 деталізації.

При цьому зберігається простота та наочність моделі, що вдосконалює класичний МАІ [77].

Множину індивідуальних критеріїв АІБ Z задаємо на множині групових та індивідуальних властивостей усіх об'єктів, що входять до контурів ІБ ОБІ. Функція належності $\mu_{zj}(z_j)$ множини дорівнюватиме одиниці тих властивостей об'єктів АИБ, які забезпечують реалізацію індивідуальних критеріїв. Відповідно, нульове значення буде в разі решти властивостей.

Множина z індивідуальних критеріїв, які ставляться у відповідність окремим об'єктам АІБ, являють 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 дозволить урахувати 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, див. рис. 5.4.

Така схема передбачає об'єднання нейронної мережі, у якій здійснюються порівняння об'єктів контурів ІБ, а також нечіткої системи, яка заснована на застосуванні бази нечітких правил, описаних вище [77].

Нечітка система, відповідно до розробленої схеми, буде здійснювати обчислення синаптичних ваг входів нейронів. При цьому враховуються й індивідуальні критерії (див. таблицю 5.1), відібрані для процедур аудиту ІБ конкретного ОБІ [77].

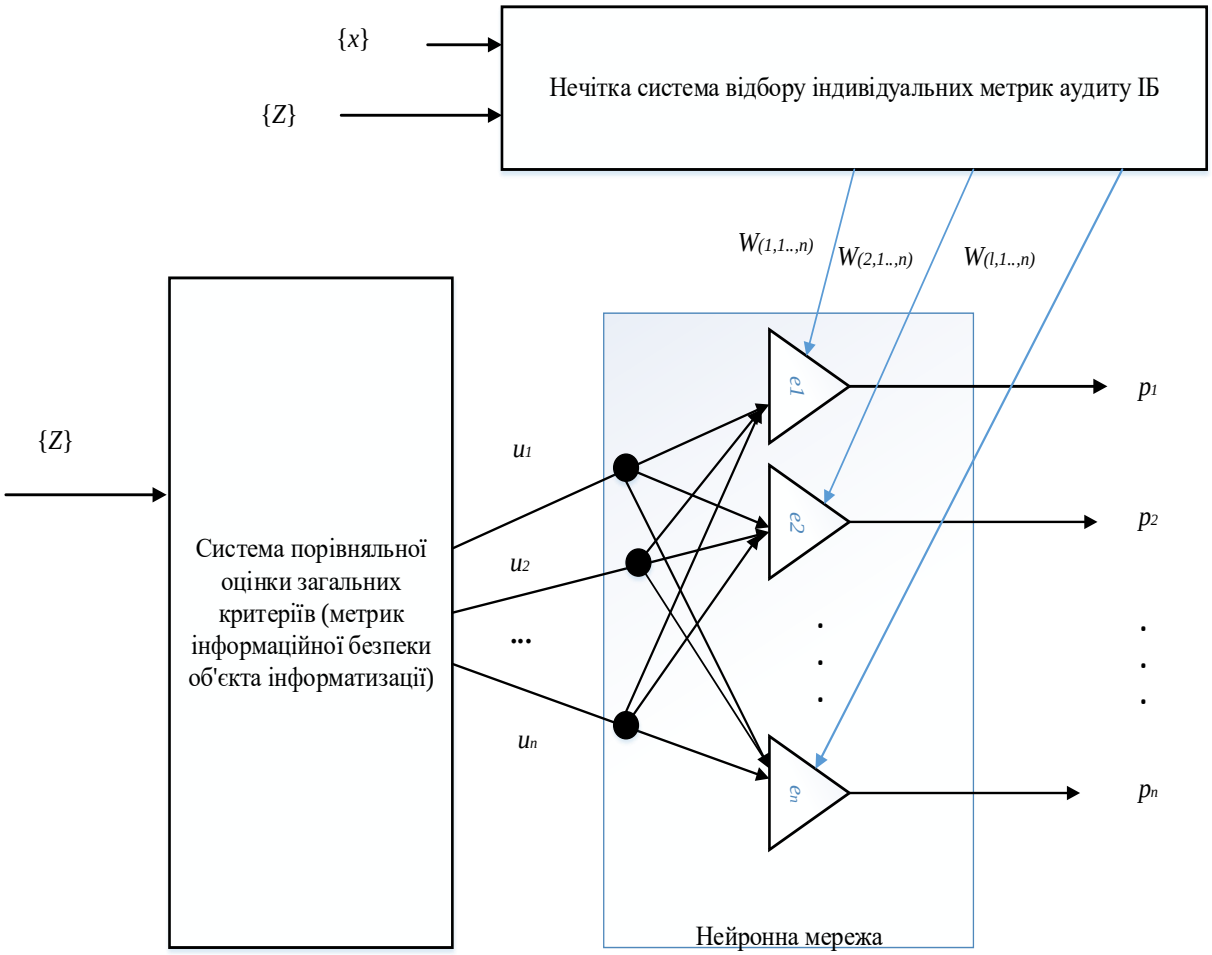


Рис. 5.4. Концептуальна структура нейро-нечіткої системи для модифікованого методу аналізу ієрархій

Джерело: розроблено автором

На вхід нейро-нечіткої системи подаватимуться експертні оцінки важливості критеріїв для конкретного ОБІ, а на виході зчитуються ранги $p_1, \ldots, p_n$ об’єктів контурів ІБ [77].

Інтелектуальна СППР забезпечує введення індивідуальних критеріїв та експертних оцінок важливості загальних критеріїв, що перевіряються під час аудиту ІБ ОБІ. Результати порівняння об’єктів представляються у вигляді графіка (див. рис. 5.5) [41].

В основу виконаних досліджень були покладені ідеї, що дозволили 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.

Таблиця 5.1

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 для аудиту ІБ для конкретного ОБІ)	
1	Імовірнісні заходи вразливості, що показують наскільки ймовірне виникнення вразливості нульового дня за певний період часу
2	Забезпечення максимальної повноти переліку інформаційних активів в аспекті додаткової інформації про загрози ІБ
3	Визначення ступеня реалізації міри (засобу) забезпечення ІБ
	….
M	Встановлений бізнес ризик

Джерело: розроблено автором

Як видно на рис. 5.5, застосування модифікованого МАІ дозволило отримати графік поточного стану ІБ обстеженого об’єкта інформатизації (лінія блакитного кольору). Причому відібрані критерії ІБ приблизно на 25–30 % нижче від еталонних значень. Хоча при застосуванні класичного МАІ не дало таких розбіжностей. Метод апробований під час виконання аудитів ІБ низки підприємств України та Казахстану [77].

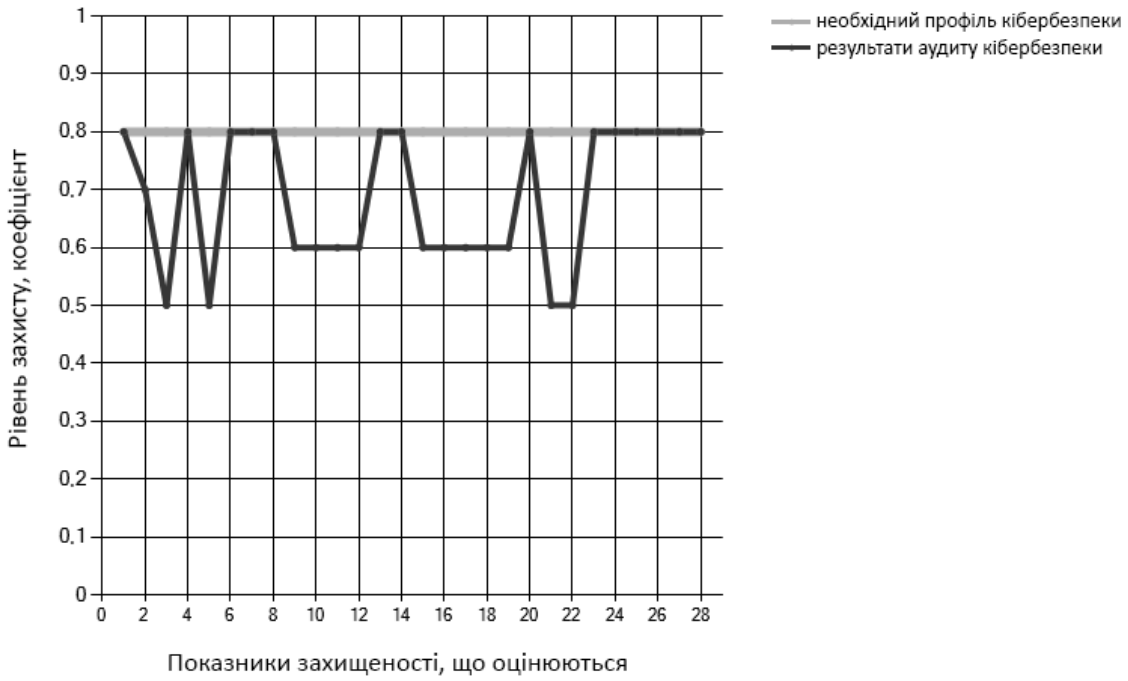


Рис. 5.5. Результати проведення аудиту ІБ ОБІ та зіставлення еталонних вимог до метрик ІБ та досягнутого рівня

Джерело: розроблено автором

Не вдаючись у детальний аналіз відомих і технічно складно реалізованих кібератак, наприклад, Stuxnet [42] або «Лабіринт місячного світла» [43] 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 відносяться заходи, спрямовані на:

– пошук оптимальної стратегії інвестування в 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 [44, 45] включають питання організації ефективного аудиту ІБ (далі – АІБ) для ОБІ.

Однак, якщо питання технічного забезпечення ІБ ОБІ на сьогоднішній день добре вивчені і, більш того, багато нових підходів до забезпечення ІБ, засновані на інноваційних технологіях, то процеси проведення АІБ все ще залишаються новою сферою для дослідників. І справді, сучасні технології привнесли у сферу ІБ підходи, засновані на когнітивних технологіях [46, 47], нейронних мережах [48, 49], еволюційних алгоритмах [50, 51] 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 розробці нових методів і моделей АІБ, заснованих на нових технологіях, наприклад, на застосуванні апарату штучних нейронних мереж (ІНС) у процедурах АІБ ОБІ.

Усе вищесказане 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.

5.3. Вдосконалення оцінки ризиків інформаційної безпеки підприємства в автоматизованих системах захисту корпоративної інформації

Зупинимось на найбільш значущих дослідженнях у галузі автоматизації оцінювання ризиків для ІБ підприємств. Так, у роботах [52, 53] показано, що організація ефективної системи управління інформаційною безпекою (СУІБ) ОБІ має бути орієнтована на пріоритетність завдання управління ризиками ІБ.

У роботах [54–56] показано, 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 роботах [56, 57] автори відзначають, 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.

Роботи [58, 59] акцентують увагу на принципах та завданнях АІБ підприємств. Проте у цих роботах залишається не розкритим питання потенціалу застосування нових ІТ підвищення ефективності АІБ.

У роботах [60, 61] пропонується модель оцінки ризиків порушення політики ІБ (далі ПІБ) ОБІ, що ґрунтується на застосуванні нечітких когнітивних карт. Проте такий підхід хоч і дає змогу враховувати безліч загроз ІБ, залишається складно алгоритмізованим. Це перекладає всю основну роботу на експерта, а відтак підвищує ймовірність суб’єктивної оцінки результатів АІБ ОБІ.

У [62–64] розглянуто практичні аспекти реалізації АІБ на основі штучної нейронної мережі (ШНМ). Крім того, розглянуто питання навчання ШНМ та її тестування під час АІБ конкретного ОБІ. Проте багато питань у роботі не розкрито. Наприклад, у роботі відсутня статистична оцінка результатів навчання ШНМ. Відсутнє також узагальнення можливості, розробленої ШНМ завдань АІБ різних ОБІ.

Можливість автоматизації процедур АІБ шляхом застосування різноманітних систем підтримки прийняття рішень (СППР) та інших ІТ розглянуто на роботах [65–67]. Проте автори зазначають, що ці дослідження ще не завершені і про повномасштабну автоматизацію АІБ ОБІ говорити поки що передчасно.

Як було показано в роботах [68, 69], невід’ємною частиною процедур АІБ є аналіз та оцінка ризиків ІБ для ОБІ. Оцінка ризиків ІБ також має бути виконана на стадії проєктування ІС для ОБІ. Для вирішення цього завдання авторами [68, 69] використовується апарат нечіткої логіки (НЛ) та ШНМ. Однак авторам 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 вищесказане зумовило актуальність нових досліджень, спрямованих на розробку нових моделей та розвиток методики проведення АІБ ОІБ. Акцент у дослідженні робиться на залучення потенціалу ШНМ та НЛ під час проведення АІБ.

Ландшафт 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 [70–72], присвячених перспективам застосування ШНМ для завдань аудиту ризиків ІБ, акцент робиться на ситуації, коли аудитори мають досить великі вибірки даних. Зауважимо, що в 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 [73, 74] розмір ризику ІБ для ОБІ можна визначити так:

$$R = f(A, T, V), \tag{5.5}$$

де $A, T, V -$ параметри, відповідно, що характеризують цінність активу, ймовірність реалізації загроз та ймовірність наявності вразливостей.

Як правило, у ході АІБ обчислюють значення ризиків порушення ІБ для ОБІ загалом – R_{FR}.

Для цього можна використовувати таку залежність:

$$R_{FR} = \sum_{n=1}^{N} R_{FR_{cu}}, \tag{5.6}$$

де N −кількість сегментів розподілених обчислювальних мереж (РОМ);

R_{FRcu} – рівень ІБ для окремого сегмента РОМ.

Значення R_{FRcu} можна визначити, використовуючи таку залежність:

$$R_{FR_{cu}} = \sum_{st=1}^{ST} P_{\sum}^{T} \cdot \left(\frac{IAV_{ST}}{IAV_{\sum}} \right), \quad (5.7)$$

де ST – кількість джерел загроз ІБ для сегмента РОМ ОБІ;

$P_{\sum}^{T}$ – – результуюче значення ймовірності реалізації загроз ІБ сегменту РОМ;

$IAV_{ST}, IAV_{\sum}$ – відповідно, вартість інформаційних активів сегмента та ОБІ (РОМ) у цілому.

Значення $P_{\sum}^{T}$ може бути найдено так:

$$P_{\sum}^{T} = 1 - \prod_{st} \left(1 - P_{ST}^{T}\right); \quad (5.8)$$

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.

При проведенні АІБ і, відповідно, аналізі ризиків, експерт оцінює апріорну імовірнісну інформацію про можливість реалізації загрози. Однак у ході вивчення нової інформації, отримані в ході АІБ, можуть як підтвердити, так і спростувати апріорну інформацію.

У запропонованому рішенні оцінки ризиків ІБ пропонується застосовувати Байєсовські мережі (БМ) довіри [75].

Наприклад, нехай для БМ були задані апріорні умовні ймовірності виникнення тих чи інших подій. Після цього було проведено навчання мережі на основі статистичних даних [76]. 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, як показано на рис. 5.6, дискретні. Кожна змінна (або загроза) може набувати одного з п’яти значень, кожне з яких відповідає ймовірності її реалізації: trivial, low, medium, high, critical (відповідно, несуттєва,

низька, середня, висока, критична). Інші змінні в БМ є характеристиками. Набір цих характеристик дозволяє ідентифікувати загрозу та визначити її ймовірність. Дані змінні поділені на категорії, що класифікують загрози ІБ або описують різні види комп'ютерних зловмисників.

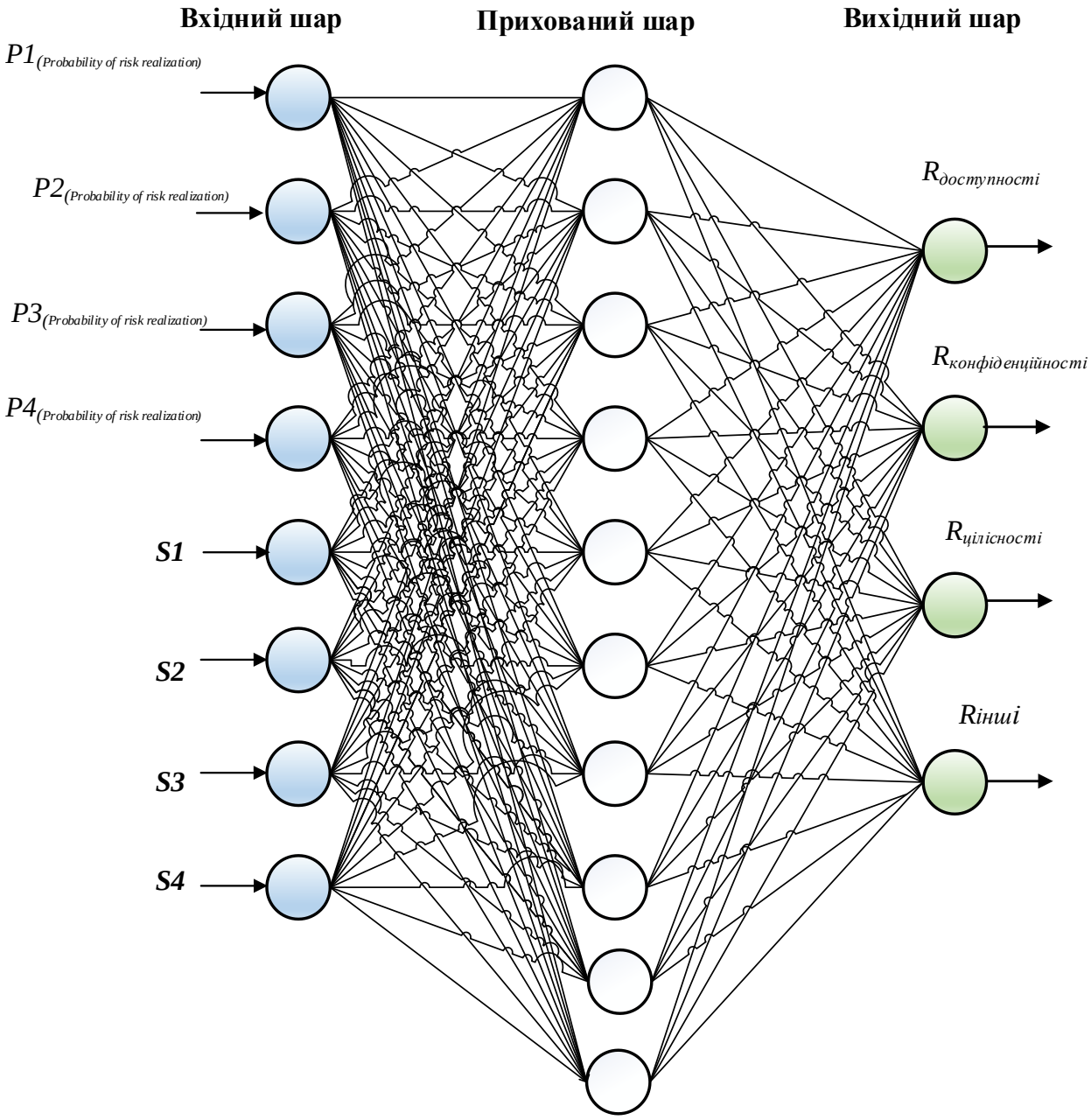


Рис. 5.6. Топологія ШНМ для автоматизації АІБ підприємства

Джерело: розроблено автором

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 таблиці 5.2 наведено приклад частини даних для опису умовних ймовірностей для загрози «Модифікація даних в інформаційній системі» ОБІ.

Таблиця 5.2

Приклад частини таблиці умовних ймовірностей для загрози «Модифікація даних в інформаційній системі»

Ідентифікатор змінної для загроз		Оцінка умовної ймовірності					
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: складено автором на основі статистичних даних [76]

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 показаний на рис. 5.7 та в табл. 5.3.

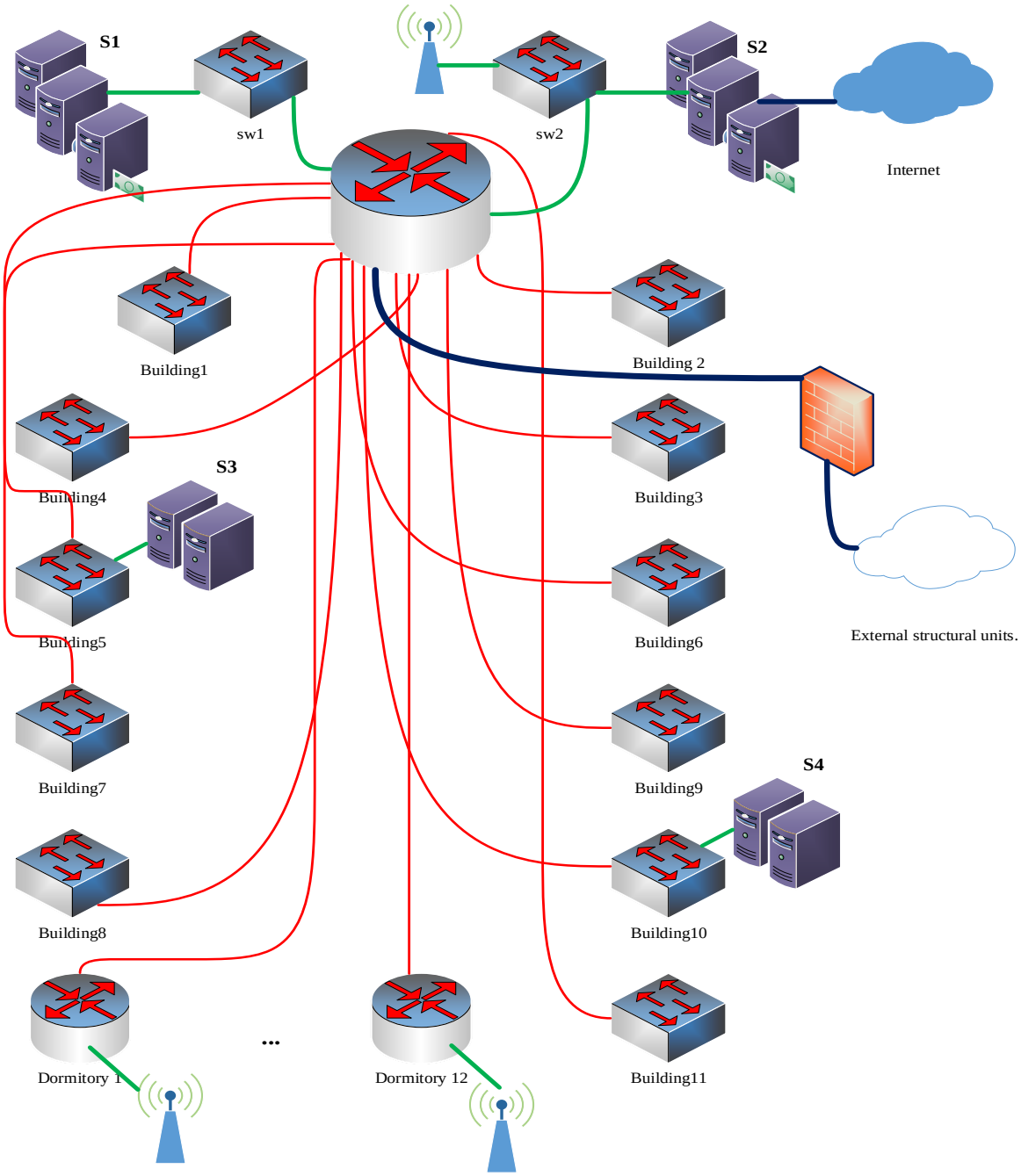


Рис. 5.7. Архітектура мережі умовного підприємства (топологія РОМ ДТЕУ)

Джерело: розроблено автором

Таблиця 5.3

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: розроблено автором

РОМ умовно була розбита на 4 сегменти – кожен сегмент відповідає мережі головного офісу та відокремлених структурних підрозділів.

ШНМ включає 10 нейронів у прихованому шарі та чотири нейрони у вихідному шарі. При навчанні багатошарового персептрона використано алгоритм зворотного поширення помилки.

Цінність інформаційних масивів (ІМ) може задати власник. Власник ІМ визначає їх цінність, керуючись їх корисністю для своїх бізнес-процесів, а також ураховуючи важливість ІМ та потенційні втрати в разі їх втрати.

Зауважимо, що при розробці ШНМ враховувалася специфіка навчальної вибірки. Входом такої ШНМ є дані, що отримані, наприклад, з антивірусного ПЗ, фаєрволів, системи виявлення вторгнень і т.п. Ці дані, відповідно, виступають як вихідна інформація 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. 5.7).

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 рисунку 5.8.

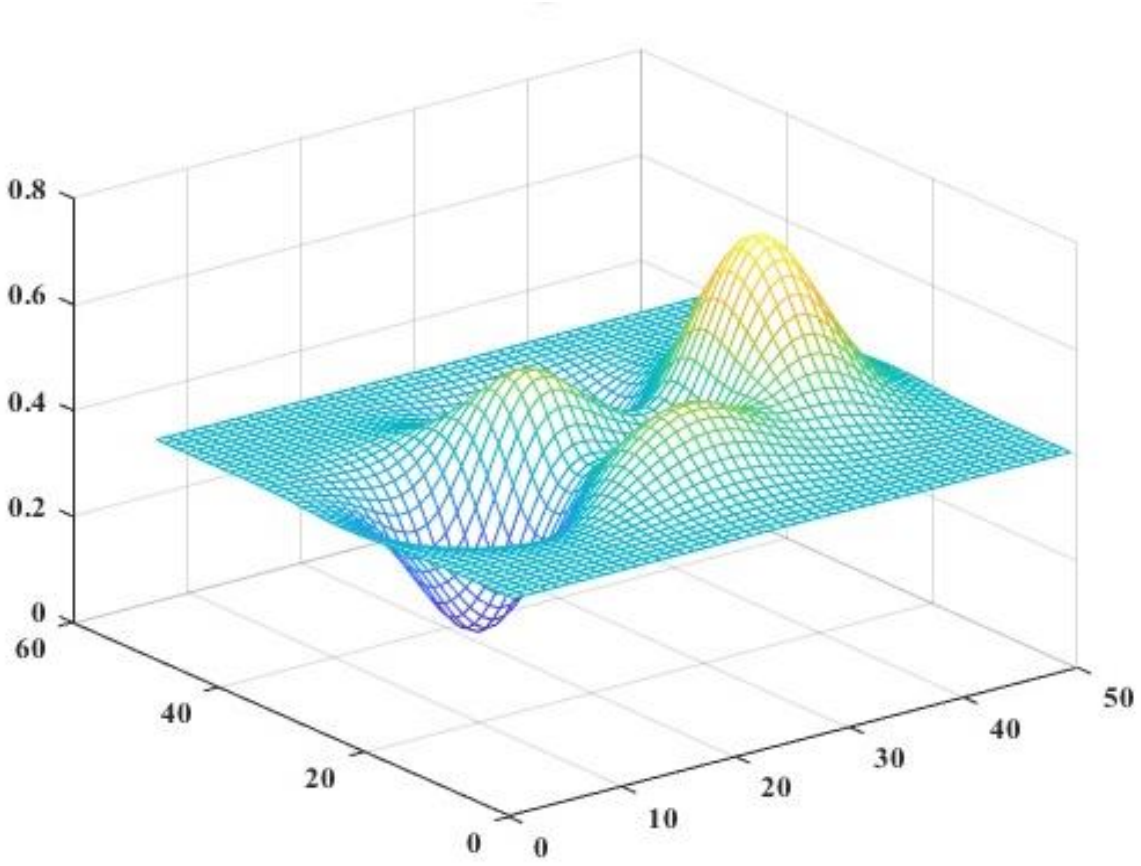


Рис. 5.8. Графік поверхні вихідних значень ризиків ІБ підприємства

Джерело: розроблено автором

Результати обчислювальних експериментів показали, що вихідні залежності (5.5) – (5.8) 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, доцільно скоротити число нейронів. Це дозволяє не перенавчати ШНМ.

У результаті обчислювальних експериментів у середовищах Genie і Matlab також було показано, що запропонований 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 не тільки дозволяє ефективно підібрати контрзаходи захисту ІБ ОБІ, але в цілому побудувати ефективну СУІБ, що адаптується до нових загроз. Зниження витрат становило не менше 15 % порівняно з методами оцінки ризиків у ході АІБ, які описані в роботах [70–74].

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: зупинку або перезапуск серверів, перезапуск віртуальних машин і т. ін.

Комбіноване використання апарата БМ та ШНМ дозволяє автоматизувати процедури АІБ, у тому числі для досить складних сценаріїв проведення атак на РОМ.

Висновки до розділу 5

Таким чином, у цьому розділі дисертації отримано такі результати:

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

2. Доповнено методику розрахунку показників від інвестиційних заходів у межах підвищення метрик ІБ підприємства (ОБІ). На відміну від існуючих рішень, у запропонованій методиці передбачено оцінку попередженої шкоди від кібератаки. Розмір попередженого збитку від кібератаки покладено в основу розрахунку показника економічного ефекту від інвестування в ЗЗІ. Проведено

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

3. Показано, що оцінка рівня ІБ для ОБІ досягається результативності шляхом використання множини критеріїв методу аналізу ієрархій (МАІ). За основу визначення метрики ІБ взято стандартні чисельні метрики ІБ: метод експертних оцінок в оцінюванні ІБ, що не ідуть в розріз з менеджементом ОБІ.

4. Вперше запропоновано модифікований метод аналізу ієрархій, який відрізняється від стандартного, застосуванням апарату теорії нечітких множин та нейронних мереж, що забезпечує прийняття обґрунтованих управлінських рішень стосовно ІБ ОБІ. Отримані рішення, спрямовані на підвищення не лише власне ІБ ОБІ, у кінцевому підсумку оптимізують систему управління ОБІ, скорочують витрати й підвищують ефективність бізнес процесів загалом. Доведено, що підвищення ступеня достовірності підрахунків показників комплексного аудиту забезпечується за рахунок впровадження математичного апарату МАІ інтелектуальної системи, яка проходить апробацію. Даний підхід застосовують як для внутрішніх процедур АІБ ОБІ, так і зовнішніх.

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

Основні результати розділу опубліковані в наукових працях автора: [1, 6, 14, 15, 22, 31, 37] – відповідно до списку опублікованих праць за темою дисертації на початку роботи.

Список використаних джерел до розділу 5

1. Довгань Л. Є., Лулукало О. Г. Формування організаційно-економічного механізму ефективного управління підприємством // Економічний вісник НТУУ «КПІ».2012. С. 48–56.
2. Пономарьова Г. О. Організаційно-економічне забезпечення випереджувального управління підприємством: Автореф. дис... канд. экон. наук : 08.06.01 / Східноукраїнський національний університет імені Володимира Даля. Луганськ, 2004. 25 с.
3. Кучер С. Ф. Організаційно-економічне забезпечення перетворень у курортно-рекреаційній системі приморського міста: Автореф. дис... канд. экон. наук: 08.00.05 / НАН України, Ін-т екон.-прав. дослідж. Донецьк, 2009. 24 с.
4. Шилова О. Ю. Організаційно-економічне забезпечення розвитку підприємства: Автореф. дис... канд. экон. наук : 08.00.04 / Донецький національний технічний університет. Донецьк, 2009. 24 с.
5. Молла М. Г. Формування системи показників оцінки організаційних складових конкурентоспроможності підприємства // Вісник соціально-економічних досліджень ОДЕУ. 2012. № 44. С. 252–257.
6. Грицишин В. О. Організаційно-економічне забезпечення управління підприємствами соціально-економічної інфраструктури міста: Автореф. дис... канд. екон. наук : 08.06.01 / Східноукраїнський національний університет імені Володимира Даля. Луганськ, 2004. 23 с.
7. Лебедик Т. М. Організаційно-економічне забезпечення регіонального розвитку підприємництва в сфері послуг: Автореф. дис... канд. экон. наук: 08.10.01 / Рада по вивченню продуктивних сил України Національної Академії Наук України. Київ, 2006. 23 с.

8. Семенов В. Ф., Галасюк С. С., Шишкіна О. В. Поняття та зміст організаційно-економічного забезпечення функціонування готельних підприємств малої місткості // Актуальні проблеми економіки. 2015. № 10 (172). С. 201–212.
9. Богославський М. Ю. Організаційно-економічне забезпечення корпоративної безпеки акціонерного товариства. Автореферат дисертації на здобуття наукового ступеня кандидата економічних наук. Спеціальність 08.00.04 економіка та управління підприємствами (за видами економічної діяльності). Університет митної справи та фінансів. Дніпро. 2021. 22 с.
10. Нашинець-Наумова А. Ю. Правове регулювання інформаційної безпеки корпорацій / А. Ю. Нашинець-Наумова // Правова інформатика. 2014. № 4 (44). С. 95–99.
11. Валіулліна З. В. Інформаційна безпека корпоративної економіки в умовах глобалізаційних процесів // Вісник Дніпропетровського університету. Серія: Менеджмент інновацій. 2016. Випуск 6. С. 34-43.
12. Про кіберзагрози в Давосі. [Електронний ресурс]. Режим доступу: http://bit.ly/2V5cbj9 (дата звернення 01.09.2022).
13. These will be the main cybersecurity trends in 2020. [Електронний ресурс]. Режим доступу: http://bit.ly/2HEfV3d (дата звернення 01.09.2022).
14. Борсуковський Ю. В. Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Частина 3 // Кібербезпека: освіта, наука, техніка. 2020. № 4. С. 33–46.
15. Грищук Р., Євсєєв С. Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах // Ukrainian Scientific Journal of Information Security. 2017. Vol. 23. Issue 3. P. 204–214.
16. Маркіна І. А. Інформациина безпека підприємства та організациині заходи її забезпечення / Ірина Анатоліївна Маркіна, Юрій Миколаиович Гарічев // Український журнал прикладної економіки. 2019. Том 4. № 4. С. 209–215.
17. 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. Vol. 105. 102248.

18. 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. 2021. URL: https://arxiv.org/abs/2102.07969 (дата звернення: 01.09.2022).
19. Yamin M. M., Ullah M., Ullah H., Katt B. Weaponized AI for cyber attacks // Journal of Information Security and Applications. 2021. Vol. 57. 102722.
20. 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.
21. 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.
22. Griffiths P. Where next for information audit? // Business Information Review. 2010. № 27(4) P. 216–224.
23. 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.
24. Kaur R., Singh M. A survey on zero-day polymorphic worm detection techniques // IEEE Communications Surveys & Tutorials. 2014. № 16(3). P. 1520–1549.
25. 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.
26. 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.semanticscholar.org/paper/Effective-Information-Security-Requires-a-Balance-Kayworth-Whitten/f29f258b0508d8ceba0a8e3942656df294127784 (дата звернення: 01.09.2022).

27. 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.
28. Suduc A. M., Bîzoi M., Filip F. G. Audit for information systems security // Informatica Economica. 2010. № 14(1). P. 43.
29. Herath H. S., Herath T. C. IT security auditing: A performance evaluation decision model // Decision Support Systems. 2014. № 57. P. 54–63.
30. 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.
31. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. International Organization for Standardization, 2013. 23 p.
32. ISO/IEC 27000:2014. Information technology. Security techniques. Information security management systems. Overview and vocabulary. International Organization for Standardization, 2014. 31 p.
33. ISO/IEC 27004:2009. Information technology. Security techniques. Information security management systems. Measurement. International Organization for Standardization, 2009. 55 p.
34. ISO/IEC 27005:2011. Information technology. Security techniques. Information security management systems. International Organization for Standardization, 2011. 68 p.
35. ISO 19011:2011. Guidelines for auditing management systems. International Organization for Standardization, 2011. 44 p.
36. Roy Y. V., Mazur N. P., Skladannyi P. M. Аудит інформаційної безпеки – основа ефективного захисту підприємства // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2018. № 1(1). С. 86–93. URL:

https://csecurity.kubg.edu.ua/index.php/journal/article/view/23 (дата звернення: 01.09.2022).

37. 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.
38. Kryvoruchko O., Desiatko A., Synichuk O. Моделювання інформаційної системи проведення незалежного аудиту інформаційної безпеки // Управління розвитком складних систем. 2020. № 43. С. 67–75.
39. 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.
40. De Wilde P. Neural network models: theory and projects // Springer Science & Business Media. 2013.
41. 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.
42. Langner R. Stuxnet: Dissecting a cyberwarfare weapon // IEEE Security & Privacy. 2011. № 9(3). P. 49–51.
43. 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.
44. Humphreys E. Information security management standards: Compliance, governance and risk management // Information security technical report. 2008. № 13(4). P. 247–255.
45. 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.

46. 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. URL: https://dl.acm.org/doi/abs/10.1155/2015/762403 (дата звернення: 01.09.2022).
47. 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.
48. 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.
49. 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. № 02CH37290). IEEE, 2002. Vol. 2. P. 1702–1707.
50. Kirta T., Kivimaab J. Optimizing it security costs by evolutionary algorithms // In Conference on Cyber Conflict Proceedings. 2010. P. 145–160.
51. 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.
52. 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.
53. 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.

54. Mataracioglu T., Ozkan S. Governing information security in conjunction with COBIT and ISO 27001. arXiv preprint arXiv:1108.2150. 2011.
55. 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.
56. 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.
57. 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.
58. 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.
59. 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.
60. Хох В. Д., Мелешко Є. В., Смірнов О. А. Дослідження методів аудиту систем управління інформаційною безпекою // Системи управління, навігації та зв'язку : Збірник наукових праць. 2017. № 1(41). С. 38–42.
61. Волот О. І. Інформаційна та кібернетична безпека сучасного підприємства: забезпечення та моделювання // Центральноукраїнський науковий вісник. Економічні науки. 2019. № 3 (36). С. 238–247.
62. Лахно В., Блозва А., Часновський Є., Криворучко О., Десятко А. Аудит інформаційної безпеки на основі застосування нейро-нечіткої системи // Технічні науки та технології. 2021. № 3 (25). P. 125–137.
63. Казакова Н. Ф., Плешко Е. А., Айвазова К. Б. Міжнародна регламентація правового регулювання та стандартизації аудиту інформаційної безпеки //

Вісник Східноукраїнського національного університету імені Володимира Даля. 2013. № 15 (1). С. 172–181.

64. 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.
65. 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.
66. 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.
67. 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.
68. 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.
69. 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.
70. Мельниченко О. В. Аудит інформаційної безпеки банку при роботі з електронними грошима // Проблеми економіки. 2013. № 4. С. 341–347.
71. 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.
72. 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.

73. 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.
74. 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.
75. 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.
76. US National Vulnerability Database. URL: https://nvd.nist.gov (дата звернення: 01.09.2022).
77. Лахно В., Блозва А., Часновський Є., Криворучко О., Десятко А. Аудит інформаційної безпеки на основі застосування нейро-нечіткої системи Технічні науки та технології : науковий журнал / Національний університет «Чернігівська політехніка». – Чернігів : НУ «Чернігівська політехніка», 2021. – № 3(25). – с.125-138

ВИСНОВКИ

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

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

2. Розвиток корпоративного інформаційного простору впливає на трансформацію структури самої корпорації: її межі розмиваються, формуються сучасні мережеві організаційні структури, що мають більш демократичний, гнучкий та адаптивний характер. Ідентифіковано основні етапи еволюції корпоративного інформаційного простору, зокрема: «паперовий», «автоматизований» і «мережевий». Доведено, що мережевість та розмитість меж

корпоративного інформаційного простору розширює уявлення про його функціонування та зумовлює трансформацію самих корпорацій, що розширює уявлення про його функціонування та стає теоретичним підґрунтям для розроблення концепції формування корпоративної інформаційної безпеки, вироблення практичних рекомендацій щодо її формування на корпоративному рівні.

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

4. Досягнення цільових параметрів системи захисту корпоративної інформації потребує розробки та впровадження в діяльність корпорацій дієвих механізмів протидії загрозам інформаційній безпеці підприємства, які

узгоджуватимуться із сучасними концептуальними положеннями ефективності функціонування економічних систем. Постійне нарощення загроз інтересам підприємства, високий рівень флуктуацій зовнішнього середовища, необхідність постійної ідентифікації достатності зусиль в удосконаленні системи управління та здійснення їх порівняльної оцінки обумовили систематизацію видової трансформації економічної ефективності управління підприємством ефективності управління підприємством за елементами його управління: ефективність структурних підрозділів управління; ефективність процесів управління; ефективність центрів відповідальності; ефективність управлінського персоналу; ефективність управлінських рішень, яка суттєво детермінує ефективність функціонування підприємства та дозволяє сформулювати нову парадигму «економічної ефективності захисту корпоративної інформації», як міри економічного ефекту витрачених ресурсів на реалізацію системи заходів з ідентифікації, аналізу, попередження та нейтралізації загроз порушення функціонування корпоративного інформаційного поля.

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

взаємодії із зовнішніми суб’єктами інформаційної безпеки, ефективнішому використанню наявного ресурсного забезпечення та пошуку нових невикористаних раніше резервів для виконання поставлених завдань.

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

7. Важливою складовою системи управління інформаційною безпекою корпорацій є забезпечення економічної ефективності корпоративної інформаційної безпеки. Складність застосування єдиної методики для формування вичерпного висновку щодо ефективності корпоративної інформаційної безпеки обумовлюється необхідністю виявлення та розв’язання ряду проблем, зокрема: необхідності обґрунтування принципів оцінювання та систематизації показників економічної ефективності; визначення чітких критеріїв оцінювання окремих показників; обґрунтування рекомендацій щодо логічної послідовності аналізу окремих показників; необхідності формування інтегрального або узагальнюючого показника ефективності корпоративної інформаційної безпеки. Методологічний підхід до оцінювання економічної ефективності захисту корпоративної інформації включає: принципи оцінювання та систематизації показників; систему часткових показників економічної ефективності та критеріальну шкалу їх інтерпретації; узагальнюючу оцінку економічної ефективності захисту корпоративної інформації на основі поєднання інтегрального показника та показника прогресивності

розвитку системи захисту КІ, структурно-логічну послідовність етапів оцінювання, дозволяє структурувати процес оцінки та запровадити дієві системи оцінювання економічної ефективності захисту корпоративної інформації ефективності захисту корпоративної інформації.

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

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

10. Оцінка реального ефекту від інвестування в ІБ ОБІ є складним процесом, в зв'язку з тим, що існує великий перелік факторів для сегменту захисту інформації (ЗІ) та кібернетичної безпеки (КБ), зокрема: ландшафт кіберзагроз, що постійно

змінюється; різноваріантні стратегії та тактики атакуючої сторони (комп'ютерних зловмисників); швидкий розвиток технічних засобів захисту інформації (ЗІ) та кібербезпеки (КБ) тощо. Ефективність заходів, спрямованих на підвищення ступеня захищеності та ІБ ОБІ не може бути дано лише на основі детермінованих оцінок та вимагає залучення ймовірнісних характеристик. Модель оцінювання економічної ефективності інвестицій на формування системи захисту корпоративної інформації, яка базується на оцінки попереджених збитків від кібератак на основі базисного показника розрахунку економічного ефекту від інвестування у ЗЗІ дозволить усунути суперечливість у питанні оцінювання ефективності заходів, спрямованих на забезпечення ІБ ОБІ.

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

12. Система управління інформаційною безпекою інтегрує окремі, часто розрізнені заходи, спрямовані на забезпечення захисту інформації та інформаційної безпеки підприємства. Ключовим процесом системи управління інформаційною безпекою підприємства є процес «Управління подіями». Діюча практика управління корпоративною інформаційною безпекою доповнена підпроцесом «Обробка подій», який удосконалює підхід до організації процесу управління подіями інформаційної безпеки корпорацій та дозволяє здійснювати комплексну

деталізацію процесу управління подіями інформаційної безпеки корпорацій, врахувати їх життєвий цикл, заповнити потенційні прогалини інформації та спростити процедуру управління інформаційною безпекою корпорації в цілому.

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

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

15. Організаційно-економічне забезпечення захисту корпоративної інформації є комплексом взаємоузгоджених елементів (заходів) різної

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

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

прийняття управлінських рішень у сфері ІБ щодо оптимізації системи управління ОБІ, скорочення витрат та підвищення адаптивності реалізації бізнес-процесів ОБІ.

17. Оцінка ризиків ІБ починається на стадії проєктування ІС для ОБІ з використанням апарату нечіткої логіки (НЛ) та ШНМ у процедурі аудиту ІБ. Методичний підхід оцінки ризиків інформаційної безпеки підприємства в автоматизованих системах захисту корпоративної інформації базується на поєднанні стандартних чисельних та експертних метрик оцінювання ІБ, який дозволяє застосувати контрзаходи захисту ІБ ОБІ та побудувати ефективну СУІБ, що превентивно адаптується до нових загроз. Комбіноване використання апарату Байєсовських мереж та штучної нейронної мережі дозволяє автоматизувати процедури аудиту ІБ. Результатом автоматизації є підтримка варіантів технічних рішень, які забезпечують можливість адміністратору ІБ РОМ діяти на випередження.

ДОДАТКИ

Додаток А

Схема оптимізації прогресивності корпоративної політики інформаційної безпеки

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 та 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 нездійсненних варіантів структури корпоративної політики інформаційної безпеки;

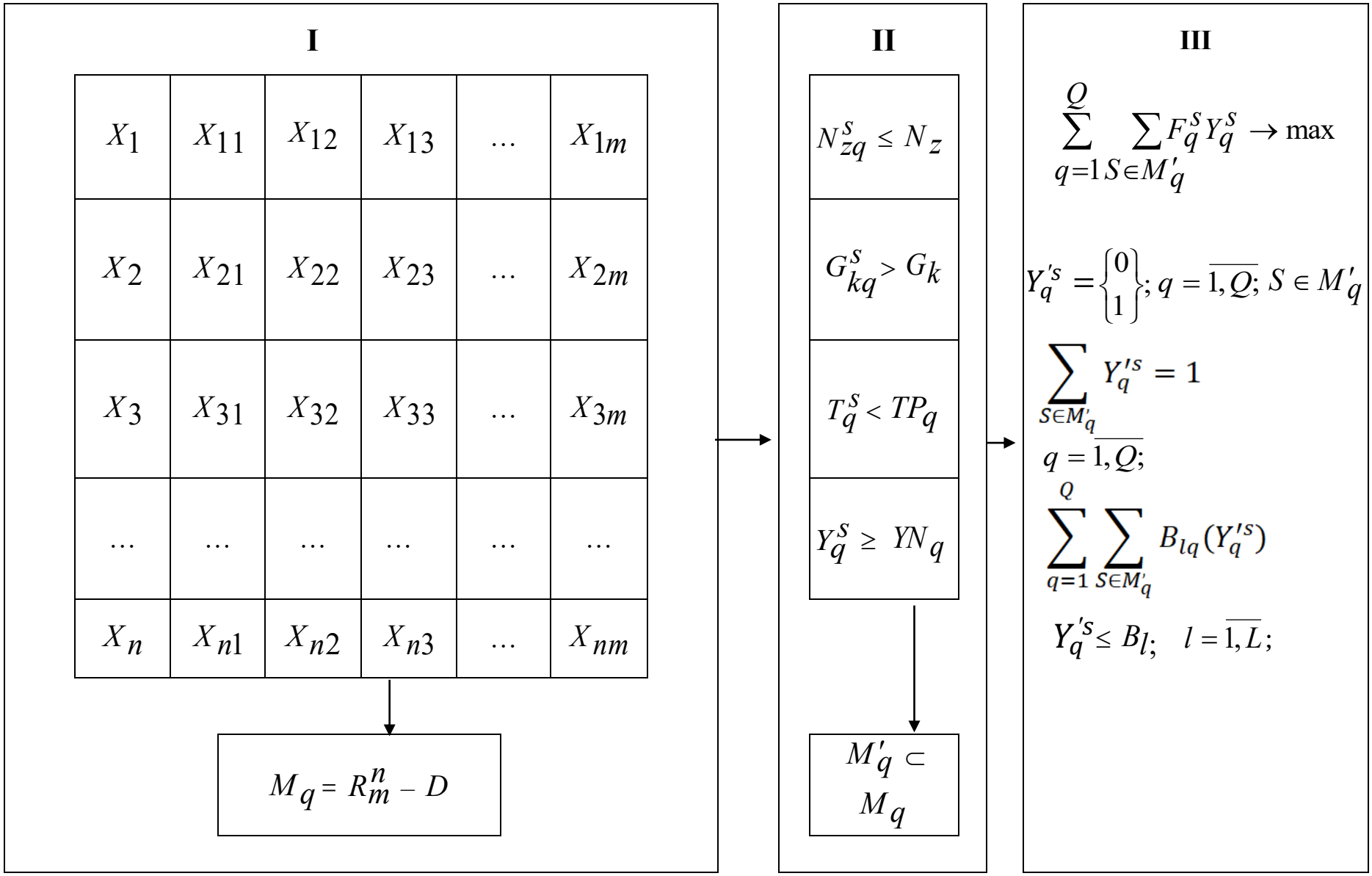


Рис. А.1. Схема оптимізації прогресивності корпоративної політики інформаційної безпеки

Джерело: укладено автором

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 задовольнити 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 за рахунок реалізації корпоративної політики інформаційної безпеки;

$B_{lq}(Y_q'^s)$ – потреба в засобах розширення ресурсів виду l для задоволення потреб виду q в умовах $Y_q'^s$;

B_l – загальний обсяг засобів розширення ресурсів виду l;

L – число видів засобів розширення ресурсів корпоративної політики інформаційної безпеки.

Додаток Б

Розширена схема адаптивного моніторингу інформаційної безпеки

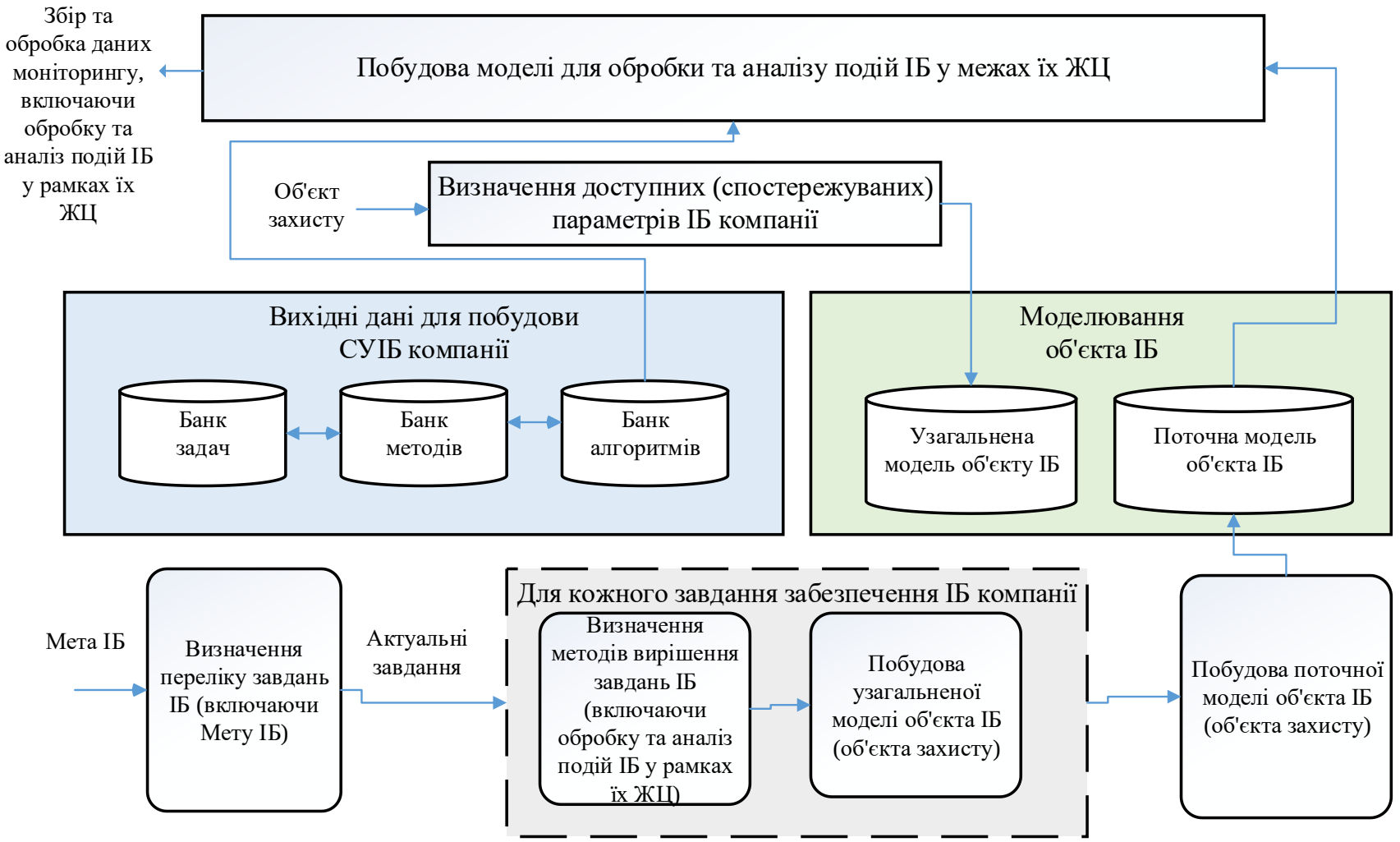


Рис. Б.1. Розширена схема адаптивного моніторингу ІБ, включаючи процедури оброблення та аналізу подій ІБ у рамках їх ЖЦ

Джерело: [58]

Додаток В

Таблиця В.1

Організаційно-економічні заходи забезпечення захисту корпоративної інформації

Контур управління	Заходи			
	нормативно-правові	організаційні	соціально-економічні	програмно-апаратні
Стратегічний	*Зовнішні*: міжнародне та національне законодавство у сфері безпеки та інформації *Внутрішні*: задокументовані цілі та концепція корпоративної інформаційної безпеки; політика управління ризиками інформаційної безпеки	*Зовнішні*: державне регулювання в сфері інформації *Внутрішні*: організаційна структура та підпорядкованість служби інформаційної безпеки; структура розподілу корпоративного контролю	*Зовнішні*: Національна стратегія розвитку економіки та інформаційного суспільства *Внутрішні*: корпоративна стратегія розвитку; архітектура та холархія корпоративних відносин; мотиваційні комплекси учасників корпоративних відносин	*Внутрішні*: заходи з формування автоматизованих системи управління, програмно-технічних засобів
Тактичний	Політика інвентаризації інформаційних активів; процедури застосування превентивних та коригуючих заходів; антивірусна політика; парольна політика; правила розмежування доступу до ресурсів і систем; інші регламентні документи	Розподіл відповідальності; нвчання та тренінги з інформаційної безпеки; фіксація інформації про інциденти безпеки	Планування та аналіз витрат на інформаційну безпеку; контроль витрат на інформаційну безпеку; облік витрат на інформаційну безпеку	Ідентифікація / аутентифікація; розмежування доступу; протоколювання/ аудит; екранування та сегментація; тунелювання; шифрування

Закінчення табл. В.1

Контур управління	Заходи			
	нормативно-правові	організаційні	соціально-економічні	програмно-апаратні
Оперативний	Інструкції щодо регламентування окремих процедур з інформаційної безпеки; коригування регламентних документів	Фізичне управління доступом; захист підтримуючої інфраструктури; реагування на порушення режиму безпеки; проведення спецперевірок застосовуваних в автоматизованих системах засобів обчислювальної техніки і проведення заходів щодо захисту інформації від витоку каналами побічних електромагнітних випромінювань і наведень	Документування втрат (фактичних та потенційних); моніторинг грошових потоків, пов'язаних із забезпеченням інформаційної безпеки; коригування бюджетів на інформаційну безпеку	Резервне копіювання; управління носіями інформації; контроль цілісності та захищеності інформації; організація явного та прихованого контролю за роботою користувачів і персоналу системи

Джерело: узагальнено та розвинено автором на основі [9, 14, 16]

Додаток Г

Довідки

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
ДЕПАРТАМЕНТ КІБЕРПОЛІЦІЇ
вул. Бориспільська, 19, м. Київ, 02093,
тел. 374-37-51, www.cyberpolice.gov.ua,
код згідно з ЄДРПОУ 40116400

26.10.22 № 9305/38/01-2022

Державний торговельно-економічний університет

ДОВІДКА

про впровадження результатів дисертаційного дослідження
ЧУБАЄВСЬКОГО Віталія Івановича
на тему «Економічна ефективність систем захисту корпоративної інформації»

Дана довідка підтверджує, що результати дисертаційного дослідження Чубаєвського Віталія Івановича, були розглянуті провідними фахівцями Департаменту кіберполіції Національної поліції України.

Визначено, що запропоновані наукові та практичні результати дозволяють сформувати рекомендації для створення системи інформаційної безпеки на підприємствах критичної інфраструктури, особливо важливо їх впроваджувати при формуванні систем захисту корпоративної інформації в умовах інформаційного протиборства та запобіганню кіберінцидентів.

Наукові дослідження Чубаєвського В.І. рекомендується взяти за основу при складанні комплексу методик перевірки достовірності інформації, що дозволить сформувати систему управління інформаційним захистом корпоративної інформації на основі реалізації процедур управління достовірною інформацією; розробці рекомендацій щодо удосконалення політики безпеки для суб'єктів господарювання різних форм власності, які функціонують в умовах інформаційного протиборства з боку конкурентів.

Отримані в дисертаційному дослідженні рішення спрямовані не лише на підвищення інформаційної безпеки об'єктів інформації, а й на оптимізацію системи управління об'єктів інформації, скорочення витрат та підвищення ефективності бізнес-процесів об'єктів інформації загалом.

Начальник
полковник поліції **Юрій ВИХОДЕЦЬ**

ДЕПАРТАМЕНТ КІБЕРПОЛІЦІЇ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ
Ідентифікаційний код 40116400
ДЛЯ ДОВІДОК

ЗАСТУПНИК СЕКРЕТАРЯ
РАДИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ
вул. Петра Болбочана, 8, м. Київ, 01601, телефон: (044) 255-06-50, телефакс: (044) 255-05-85

№ 53/11
01.11.2022

ДОВІДКА

про впровадження результатів дисертаційного дослідження на тему: «Економічна ефективність систем захисту корпоративної інформації» докторанта кафедри економіки та фінансів підприємства Державного торговельно-економічного університету Чубаєвського Віталія Івановича

Довідка видана Чубаєвському Віталію Івановичу про те, що його науково-методичні розробки та практичні рекомендації пройшли апробацію та прийняті для практичного використання в діяльності РНБО, зокрема:

– застосовано методику інтегрального показника стану корпоративного інформаційного простору для експрес-діагностування розвитку інформаційно-комунікаційних технологій в країні на заміну показника IDI (The Information and Communication Technology Development Index);

– використано інтегральну методику оцінювання рівня ефективності систем захисту корпоративної інформації підприємств, що передбачає обчислення інтегральних показників за кожною виділеною складовою системи захисту та загального інтегрального показника;

– апробовано шкалу інтерпретації рівня ефективності систем захисту корпоративної інформації підприємств за пропонованою авторською методикою.

Результати проведених апробацій засвідчили практичну цінність отриманих Чубаєвським В.І. науково-практичних результатів та довели можливість і доцільність їхнього впровадження.

Довідка видана для подання до спеціалізованої вченої ради.

Сергій ДЕМЕДЮК

Підпис Демедюка засвідчую
Державний експерт служби управління персоналом Апарату Ради національної безпеки і оборони України
Сидоренко
«01» 11 2022 р.

Україна, 03037, м. Київ, пр. В. Лобановського, буд. 14, оф. 107
тел.: +380 44 406 65 20, факс: +380 406 65 21

14 Valeriy Lobanovskiy ave., office 107, 03037 Kyiv, Ukraine
tel.: +380 44 406 65 20, fax: +380 44 406 65 21

KARMA DIGITAL LTD

Спеціалізованій вченій раді Д 26.055.01
Державного торговельно-економічного університету

Вих. 0111/1-2022
від 01.11.2022р

ДОВІДКА

про впровадження результатів дисертаційної роботи докторанта кафедри економіки та фінансів підприємства Державного торговельно-економічного університету Чубаєвського Віталія Івановича на тему: «Економічна ефективність систем захисту корпоративної інформації»

Керівництво товариства з обмеженою відповідальністю «КАРМА ДІДЖІТАЛ ЛТД», ознайомившись з представленими результатами наукового дослідження Чубаєвського Віталія Івановича, визнає їх актуальність та практичну значущість для забезпечення економічної ефективності систем захисту корпоративної інформації.

Для практичного використання прийнято розроблену автором інтегральну методику оцінювання рівня ефективності системи захисту корпоративної інформації підприємства, яка передбачає розрахунок інтегральних показників за кожною виділеною складовою системи захисту корпоративної інформації підприємства та загального інтегрального показника. Дана методика дозволяє приймати обґрунтовані рішення щодо реалізації заходів підвищення ефективності системи захисту корпоративної інформації підприємства.

Проведена оцінка економічної ефективності системи захисту корпоративної інформації на основі визначення ступеня її прогресивності дозволила оцінити існуючий стан системи захисту корпоративної інформації та сформувати вектор досягнення оптимального (найкращого) її варіанту в конкретних умовах функціонування корпорацій для проведення перманентного моніторингу досягнення цілей і завдань функціонування системи інформаційної безпеки та визначення напрямів необхідних змін.

Представлений у роботі методичний інструментарій та шкала інтерпретації рівня ефективності системи захисту корпоративної інформації підприємства, за запропонованою методикою, були використані в процесі аудиту інформаційної безпеки та обґрунтування комплексу заходів для посилення захисту корпоративної інформації у межах розроблення стратегії розвитку товариства з обмеженою відповідальністю «КАРМА ДІДЖІТАЛ ЛТД» до 2025 року.

Виконавчий Директор **Федір МАХНО**

УКРАЇНА * ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ * КИЇВ *
"КАРМА ДІДЖІТАЛ ЛТД"
Ідентифікаційний код 40206724

ЗАТВЕРДЖУЮ
Заступник Голови
Державної служби спеціального
зв'язку та захисту інформації України
д.ю.н., проф.

Володимир ТРОФИМЕНКО

«03» 11 2022 р.

АКТ
про впровадження результатів дисертаційної роботи
на тему:
«Економічна ефективність систем захисту корпоративної інформації»
на здобуття ступеня доктора економічних наук
за спеціальністю 051 «Економіка»
ЧУБАЄВСЬКОГО Віталія Івановича

Даний акт складено про те, що комісія з економічної та інформаційної безпеки розглянула дисертаційну роботу Чубаєвського Віталія Івановича на тему «Економічна ефективність систем захисту корпоративної інформації» і встановила:

1. Результати дисертаційної роботи є актуальними, теоретично обґрунтованими та представляють наукову цінність для реалізації рішень в проєктах Адміністрації Державної служби спеціального зв'язку та захисту інформації України.

2. Запропонована ієрархічна структура стала основою для подальшого синтезу інтелектуальної системи виявлення спроб несанкціонованого доступу в умовах важкозрозумілих ознак або їх невеликого числа, що дозволило ефективно реалізувати первинну формалізацію неправомірних дій комп'ютерних зловмисників для подальшого математичного опису параметра ймовірності несанкціонованого доступу.

3. Запропоновано методологічний підхід, що дозволив автоматизувати та систематизувати прояви ефекту захищеності інформації від витоків по технічних каналах. Доповнено імовірнісну модель виконання загроз, яка дозволила на основі запропонованого програмного забезпечення залучати кілька експертів для оцінки актуальності загроз витоку інформації щодо технічних каналів просочування інформації в умовах динамічного вдосконалення ТЗР.

4. Розглянуто та запроваджено контур системи підтримки прийняття рішень у процесі розвитку інфраструктури системи захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України.

5. В умовах дефіциту кваліфікованих експертів у галузі інформаційної безпеки, запропоновано доповнення, яке пройшло апробацію в Адміністрації Державної служби спеціального зв'язку та захисту інформації України, до існуючих математичних моделей.

Використані результати дисертаційної роботи Чубаєвського В.І. позитивно впливають на безпеку та функціонування інформаційного простору Адміністрації Державної служби спеціального зв'язку та захисту інформації України.

Голова комісії:
Директор Департаменту кіберзахисту
к.н.держ. упр. Данило МЯЛКОВСЬКИЙ

Члени комісії:
Начальник 2 управління ДЗІ
к.т.н. Борис ГОРЛИНСЬКИЙ

Заступник начальника ДЗ Держспецзв'язку
к.н.держ. упр. Тарас СТАНІСЛАВСЬКИЙ

№01-5479/вс 03.11.2022.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

вул. Кіото, 19, м. Київ, 02156, тел. +38 (044) 531 47 41, e-mail: knute@knute.edu.ua, код ЄДРПОУ 44470624

14.11.2022 № 2000/22

На № _____

ДОВІДКА

Видана Чубаєвському Віталію Івановичу, здобувачу наукового ступеня «доктор економічних наук» кафедри економіки та фінансів підприємства кандидату політичних наук, доценту кафедри інженерії програмного забезпечення Державного торговельно-економічного університету, про те, що окремі положення, висновки та пропозиції, що містяться в дисертаційному дослідженні на тему «Економічна ефективність систем захисту корпоративної інформації», застосовуються в освітньому процесі ДТЕУ.

Чубаєвським В.І. розроблено (у співавторстві) та впроваджено в освітній процес:

- Навчальний посібник англійською мовою «Методи та засоби захисту інформації» (Lakhno V., Kasatkin D.Yu., Dubovyk O., Kryvoruchko O., Desiatko A., Chubaievskyi V. Tutorial «Methods and means of information protection». – Kyiv: NPE Yamchynskyi O.V., 2022. – 267 p. Рекомендований здобувачам вищої освіти спеціальності 125 «Кібербезпека» при вивченні основної освітньої компоненти «Соціотехнічна кібербезпека» і вибіркової освітньої компоненти «Основи кібербезпеки», що внесена до всіх освітніх програм ДТЕУ першого освітнього рівня «бакалавр» (особистий внесок: автор першого розділу «Основи безпеки інформаційних систем» = «Fundamentals of Information Systems Security») та пункту 4.3 «Основні режими алгоритму DES» = «The main modes of operation of the DES algorithm»).
- Збірник тестових завдань з дисципліни «Архітектура та проєктування програмного забезпечення» (Чубаєвський В.І., Криворучко О.В., Десятко А.М., Хорольська К.В., Тищенко Д.О., Франчук Т.М. Збірник тестових завдань з дисципліни «Архітектура та проєктування програмного забезпечення», ДТЕУ, 2022). Рекомендований здобувачам вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 121 «Інженерія програмного забезпечення» як обов'язкова компонента ОП та спеціальності 125 «Кібербезпека» як вибіркова компонента ОП ступеня «бакалавр» (особистий внесок: автор тестових завдань, що розкривають тему «Тестування програмного забезпечення в розрізі А та ППЗ» та тих тестових завдань, що висвітлюють питання забезпечення безпеки ПЗ на відповідних етапах життєвого циклу програмного продукту – у межах всіх тем, внесених до збірника).

- Збірник тестових завдань з дисципліни «Хмарні та GRID технології» (Чубаєвський В.І., Криворучко О.В., Десятко А. М., Хорольська К.В., Тищенко Д.О., Франчук Т.М., Чернишова Д.Д., Захаров Р.Г. Збірник тестових завдань з дисципліни «Хмарні та GRID технології», ДТЕУ, 2022). Рекомендований здобувачам вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 121 «Інженерія програмного забезпечення» як обов'язкова компонента ОП ступеня «магістр» та спеціальності 124 «Системний аналіз» – вибіркова компонента ОП ступеня «бакалавр» (особистий внесок: автор тестових завдань, що висвітлюють теми: «Туманні технології як складова хмарних обчислень», «Безпека даних у хмарних середовищах»).
- Програма дисципліни «Архітектура та проєктування програмного забезпечення» (Чубаєвський В.І., Криворучко О.В., Десятко А.М., Хорольська К.В., Тищенко Д.О., Франчук Т.М. Програма дисципліни «Архітектура та проєктування програмного забезпечення», затверджена вченою радою ДТЕУ від 30.06.2022). Рекомендована здобувачам вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 121 «Інженерія програмного забезпечення» як обов'язкова компонента ОП та спеціальності 125 «Кібербезпека» як вибіркова компонента ОП ступеня «бакалавр» (особистий внесок: визначення та наповнення теми «Тестування програмного забезпечення в розрізі А та ППЗ»).
- Програма дисципліни «Хмарні та GRID технології» (Чубаєвський В.І., Криворучко О.В., Десятко А.М., Хорольська К.В., Тищенко Д.О., Франчук Т.М., Чернишова Д.Д., Захаров Р.Г. Програма дисципліни «Хмарні та GRID технології», затверджена вченою радою ДТЕУ від 30.06.2022). Рекомендована здобувачам вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 121 «Інженерія програмного забезпечення» як обов'язкова компонента ОП ступеня «магістр» та спеціальності 124 «Системний аналіз» – вибіркова компонента ОП ступеня «бакалавр» (особистий внесок: визначення та наповнення тем «Туманні технології як складова хмарних обчислень» та «Безпека даних у хмарних середовищах»).
- Робоча програма дисципліни «Архітектура та проєктування програмного забезпечення» (Чубаєвський В.І., Криворучко О.В., Десятко А.М., Хорольська К.В., Тищенко Д.О., Франчук Т.М. Робоча програма дисципліни «Архітектура та проєктування програмного забезпечення», затверджена вченою радою ДТЕУ від 29.09.2022). Рекомендована здобувачам вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 121 «Інженерія програмного забезпечення» як обов'язкова компонента ОП та спеціальності 125 «Кібербезпека» як вибіркова компонента ОП ступеня «бакалавр» (особистий внесок: наповнення теми «Тестування програмного забезпечення в розрізі А та ППЗ», розробка лабораторних робіт).
- Робоча програма дисципліни «Хмарні та GRID технології» (Чубаєвський В.І., Криворучко О. В., Десятко А. М., Хорольська К.В., Тищенко Д.О., Франчук Т.М., Чернишова Д.Д., Захаров Р.Г. Робоча програма дисципліни «Хмарні та GRID технології», затверджена вченою радою ДТЕУ від 29.09.2022). Рекомендована здобувачам вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 121 «Інженерія програмного забезпечення» як обов'язкова компонента ОП ступеня «магістр» та спеціальності 124 «Системний аналіз» – вибіркова компонента ОП ступеня «бакалавр» (особистий внесок: наповнення тем «Туманні технології як складова хмарних обчислень» та «Безпека даних у хмарних середовищах», розробка лабораторних робіт).

- Програма дисципліни «Комп'ютерні мережі» (Чубаєвський В.І., Миронець С.М., Костюк Ю.В., Шестак Я.І., Самойленко Ю.О., Костюк І.В. Програма дисципліни «Комп'ютерні мережі», затверджена вченою радою КНТЕУ від 25.03.2021). Рекомендована здобувачам вищої освіти спеціальності «Психологія» ОС «бакалавр» (особистий внесок: наповнення тем, що відповідають напряму забезпечення безпеки ПЗ та суб'єктів господарювання).
- Робоча програма виробничої (переддипломної) практики (Криворучко О.В., Чубаєвський В.І., Рзаєва С.Л., Десятко А.М. Робоча програма виробничої (переддипломної) практики, затверджена вченою радою КНТЕУ від 31.10.2019). Рекомендована здобувачам вищої освіти спеціальності 121 «Інженерія програмного забезпечення» ОС «магістр» (особистий внесок: наповнення індивідуальних завдань, що направлені на аудит інформаційної та кібербезпеки суб'єкта господарювання – бази практики здобувача вищої освіти).
- Програма та робоча програма дисципліни «Економічна безпека підприємства» (Блакита Г.В., Богма О.С., Сілакова А.В., Чубаєвський В.І.), затверджена вченою радою КНТЕУ від 25.11.2021. Рекомендована здобувачам вищої освіти спеціальності «Економіка» ОС «магістр» (особистий внесок: наповнення тем щодо інформаційної безпеки підприємства).
- Робоча програма дисципліни «Економічна діагностика підприємства» (Блакита Г.В., Сілакова А.В., Чубаєвський В.І.). Рекомендована здобувачам вищої освіти спеціальності «Економіка» ОС «магістр» (особистий внесок: наповнення тем щодо діагностики економічної безпеки підприємства).

Довідку видано для подання до спеціалізованої вченої ради.

Проректор з наукової роботи **Світлана МЕЛЬНИЧЕНКО**

Божко Тетяна (044) 531 47 33

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

вул. Кіото, 19, м. Київ, 02156, тел. +38 (044) 531 47 41, e-mail: knute@knute.edu.ua, код ЄДРПОУ 44470624

14.11.2022 № 1999/24

На № _____

ДОВІДКА

Видана Чубаєвському Віталію Івановичу, здобувачу наукового ступеня вищої освіти доктора наук Державного торговельно-економічного університету, про те, що він дійсно з 03.05.2021 бере участь у виконанні науково-дослідної роботи «Системи оцінювання економічної ефективності захисту корпоративної інформації» (термін виконання: II кв. 2021 р. – III кв. 2024 р.).

Номер державної реєстрації НДР – 0121U110908.

Особистий внесок Чубаєвського Віталія Івановича:

- запропоновано інтегральну методику оцінювання рівня ефективності системи захисту корпоративної інформації підприємства;
- обґрунтовано шкалу інтерпретації рівня ефективності системи захисту корпоративної інформації підприємства;
- розроблено підходи до математико-алгоритмічної та комп'ютерної підтримки процедури прийняття рішень у задачі організаційно-економічного забезпечення ефективного захисту корпоративної інформації;
- запропоновано методику багатокритеріальної оптимізації витрат на систему захисту корпоративної інформації.

Довідка видана для подання до спеціалізованої вченої ради Д 26.055.01.

Проректор
з наукової роботи **Світлана МЕЛЬНИЧЕНКО**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ Ідентифікаційний код 44470624

Федоренко Олена (044) 531 31 26

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

вул. Кіото, 19, м. Київ, 02156, тел. +38 (044) 531 47 41, e-mail: knute@knute.edu.ua, код ЄДРПОУ 44470624

15.11.2022 № 2005/20

На № _____

ДОВІДКА

Чубаєвський Віталій Іванович, здобувач наукового ступеня вищої освіти «доктор наук» Державного торговельно-економічного університету, з 15 червня 2022 р. і дотепер бере участь у виконанні науково-дослідної роботи № 717/20 «Цифрова трансформація торговельно-економічної та туристичної систем України», що фінансується із коштів загального фонду державного бюджету України, КПКВ 2201390, (термін виконання НДР: 01.06.2022–31.12.2022).

Особистий внесок Чубаєвського Віталія Івановича:

- запропоновано методи оцінки економічної ефективності інформаційної безпеки для підприємств торгівлі;
- систематизовано особливості оцінки економічної ефективності інформаційної безпеки з урахуванням особливостей діяльності оптово-роздрібних підприємств;
- розроблено підходи до розв'язання проблем захисту персональних даних в електронно-інформаційному середовищі торговельно-економічної та туристичної систем України;
- запропоновано генетичний алгоритм розв'язання задачі масштабування хмароорієнтованого об'єкта інформатизації у торговельно-економічній та туристичній системах.

Довідка видана для подання до спеціалізованої вченої ради Д 26.055.01.

Проректор
з наукової роботи **Світлана МЕЛЬНИЧЕНКО**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ Ідентифікаційний код 44470624

Сапітура Людмила (044) 531 31 26