УДК: 338.242:[005.52:005.334]:004.056 **doi: 10.20998/2313-8890.2026.05.09**

Береза Валерій Володимирович, докторант Інституту тваринництва НААН України, доктор філософії (PhD), +38(066)703-25-52, bereza.vv@meta.ua, ORCID ID: 0009-0006-6698-2889
Інститут тваринництва Національної академії аграрних наук України
вул. Тваринників, 1-А, м. Харків, Харківська область, 61026 (Кулиничі)
Сабадаш Інна Олександрівна, кандидат юридичних наук, докторант Інституту тваринництва НААН України, +38(068)606-63-33, inna.sabadash@tuta.com, ORCID ID: 0009-0001-5267-9153
Інститут тваринництва Національної академії аграрних наук України
вул. Тваринників, 1-А, м. Харків, Харківська область, 61026 (Кулиничі)

МОДЕЛЮВАННЯ ПРОЦЕСУ ІНТЕГРАЦІЇ БЕЗПЕКОВИХ ФУНКЦІЙ У БІЗНЕС-ПРОЦЕСИ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

Анотація. *У статті здійснено теоретико-методологічне обґрунтування та побудовано інтегровану соціотехнічну модель процесу впровадження безпекових функцій у бізнес-процеси суб'єктів господарювання в умовах високої турбулентності цифрового простору, стрімкого розширення мережевих периметрів та загострення сучасних геополітичних викликів. Обґрунтовано концептуальний перехід від традиційного статичного захисту фізичного периметра до прогресивної парадигми Security-by-Design, яка передбачає безшовне проектування механізмів контролю безпосередньо всередині операційної, управлінської та допоміжної архітектури підприємства. Запропоновано оригінальний двовекторний підхід до моделювання системи, що забезпечує методологічний синтез високорівневого функціонального структурування діяльності організації на засадах стандарту IDEF0 та деталізованого низькорівневого графічного представлення робочих потоків у сучасних нотаціях BPMN і SecBPMN з візуалізацією руху даних через діаграми DFD. На основі референсної моделі інформаційної безпеки RMIAS математично формалізовано специфікацію безпекових предикатів для ключових аспектів захисту, зокрема конфіденційності, цілісності, доступності, автентичності, підзвітності, аудитованості та невідомовності, що дозволяє виконувати автоматичну верифікацію відповідності моделей процесів загальній корпоративній політиці безпеки. Визначено три технічні рівні інтеграції безпекових контролів (доступ, передача та зберігання даних) на базі передових інфраструктурних рішень SASE, ZTNA, CASB, FWaaS та вітчизняних автоматизованих ERP та ForceBPM платформ, а також детально охарактеризовано супутній економічний ефект автоматизації захищених процесів, що виражається у довгостроковому зниженні операційних витрат на 15–25 % та значному скороченні часу виконання операцій. Особливу увагу приділено побудові комплексної карти індикаторів ризику за чотирма взаємопов'язаними групами (персонал, система, проект, зовнішнє середовище) та доцільності впровадження міжнародних стандартів охорони праці ISO 45001 як фундаментальної складової реалізації сучасної концепції ESG, що безпосередньо мінімізує залишкові ризики, підвищує рівень економічної безпеки, капіталізацію та загальну інвестиційну привабливість суб'єктів господарювання.*

Ключові слова: *моделювання бізнес-процесів, економічна безпека, соціотехнічні системи, фреймворк SecBPMN, методологія IDEF0, безпекові предикати, автоматизація, концепція ESG, індикатори ризику.*

Bereza Valerii, Doctoral Student, Livestock Farming Institute of National Academy of Agrarian Sciences of Ukraine, +38(066)703-25-52, bereza.vv@meta.ua, ORCID ID: 0009-0006-6698-2889
Livestock Farming Institute of National Academy of Agrarian Sciences of Ukraine
1-A Tvarynnykyv Street, Kharkiv, Kharkiv region, 61026 (Kulynichi)
Sabadash Inna, Candidate of Law, doctoral student of Livestock Farming Institute of the National Academy of Agrarian Sciences of Ukraine, +38(068)606-63-33, inna.sabadash@tuta.com, ORCID ID: 0009-0001-5267-9153
Livestock Farming Institute of National Academy of Agrarian Sciences of Ukraine
1-A Tvarynnykyv Street, Kharkiv, Kharkiv region, 61026 (Kulynichi)

MODELING THE PROCESS OF INTEGRATING SECURITY FUNCTIONS INTO BUSINESS PROCESSES OF BUSINESS ENTITIES

Abstract. *The article provides a theoretical and methodological substantiation and constructs an integrated sociotechnical model of the process of embedding security functions into the business processes of economic entities under conditions of high digital space turbulence, rapid expansion of network perimeters, and aggravation of modern geopolitical challenges. A conceptual transition from traditional static physical perimeter defense to the progressive Security-by-Design paradigm is substantiated, which implies seamless design of control mechanisms directly inside the operational, managerial, and supporting architecture of an enterprise. An original two-vector approach to system modeling is proposed, which ensures a methodological synthesis of high-level functional structuring of organizational activity based on the IDEF0 standard and detailed low-level graphical representation of workflows in modern BPMN and SecBPMN notations, with the visualization of data movement via DFD diagrams. Based on the reference model of information security RMIAS, the specification of security predicates for key protection aspects is mathematically formalized, including confidentiality, integrity, availability, authenticity, accountability, auditability, and non-repudiation, which allows performing automatic verification of process models compliance with the general corporate security policy. Three technical levels of security controls integration (access, data transmission, and data storage) based on advanced infrastructure solutions SASE, ZTNA, CASB, FWaaS, and domestic automated ERP and ForceBPM platforms are determined, and the accompanying economic effect of automated secure processes is characterized in detail, which is expressed in a long-term reduction of operational costs by 15–25% and a significant reduction in operation execution time. Particular attention is paid to constructing a comprehensive risk indicator map across four interconnected groups (personnel, system, project, external environment) and the expediency of implementing international occupational health and safety standards ISO 45001 as a fundamental component of the modern ESG concept realization, which directly minimizes residual risks, increases the level of economic security, capitalization, and overall investment attractiveness of economic entities.*
Keywords: *business process modeling, economic security, sociotechnical systems, SecBPMN framework, IDEF0 methodology, security predicates, automation, ESG concept, risk indicators.*

Постановка проблеми. Сучасний етап розвитку глобального економічного простору характеризується високим рівнем турбулентності, динамічністю змін та загостренням конкурентної боротьби, що вимагає від суб'єктів господарювання

безперервної адаптації та підвищення ефективності їхньої діяльності. В умовах цифрової трансформації, стрімкого розширення цифрових периметрів підприємств, поширення хмарних технологій та постійного зростання кіберзагроз традиційні підходи до управління безпекою, що ґрунтувалися на концепції статичного захисту фізичного периметра, виявляються цілковито неефективними. Геополітичні виклики, зумовлені реаліями гібридної війни, дестабілізацією логістичних ланцюгів та регуляторними обмеженнями, змушують вітчизняні підприємства здійснювати стратегічний перерозподіл управлінських ресурсів. Головним завданням стає не просто захист окремих активів, а забезпечення загальної стійкості, живучості та стабільності соціотехнічної системи підприємства в реальному часі.

У цьому контексті особливого значення набуває концепція процесного управління, де бізнес-модель суб’єкта господарювання розглядається як формалізована система формування доданої вартості. Забезпечення життєздатності такої системи можливе лише за умови безшовної інтеграції безпекових функцій безпосередньо в операційні, управлінські та допоміжні бізнес-процеси. Моделювання бізнес-процесів виступає фундаментальним інструментом вирішення цієї проблеми, оскільки воно дозволяє не тільки візуалізувати наявний стан діяльності підприємства (модель as-is), а й спрогнозувати ефективність впровадження системних змін ще до їх фактичної реалізації (модель to-be).

Незважаючи на значний науковий інтерес до цієї проблематики, на практиці інтеграція безпеки в бізнес-процеси часто стикається з серйозними організаційними бар'єрами. Найпоширенішим викликом є функціональна ізольованість («силоси») підрозділів, коли відділи безпеки та операційні департаменти діють неузгоджено, а також дефіцит фінансових та кваліфікованих людських ресурсів. Крім того, відсутність формалізованих моделей та інструментів інтегрованого проектування безпекових контролів ускладнює своєчасне реагування на інциденти. Отже, наукове дослідження процесу моделювання інтеграції безпекових функцій у бізнес-процеси є

актуальним та затребуваним завданням, вирішення якого безпосередньо впливає на рівень економічної безпеки та конкурентоспроможності суб’єктів господарювання..

Аналіз останніх досліджень і публікацій. Дослідження теоретико-методологічних та прикладних засад моделювання бізнес-процесів та забезпечення економічної безпеки підприємств перебуває в центрі уваги багатьох вітчизняних та іноземних науковців. Проведений аналіз публікацій дозволяє систематизувати внесок дослідників за кількома ключовими напрямами.

Перший науковий напрям охоплює фундаментальні засади економічної безпеки суб’єктів господарювання у зв'язку з їхніми бізнес-процесами. Зокрема, Л. В. Рибальченко [1] у своїх працях обґрунтовує сутність економічної безпеки підприємства як стану захищеності його бізнес-процесів та їхнього ресурсного забезпечення від зовнішніх та внутрішніх загроз, що дозволяє досягати стабільного функціонування з мінімальними втратами. А. Ю. Гриненко [2] деталізує структуру економічної безпеки через призму ресурсно-функціонального підходу, виділяючи сім взаємопов'язаних складових (інтелектуально-кадрову, фінансову, техніко-технологічну, політико-правову, екологічну, інформаційну та силову) та наголошуючи на необхідності гармонізації інтересів підприємства із зовнішніми контрагентами. Питання мінімізації втрат та збереження контролю над власністю як основи безпеки також досліджував В. А. Панченко [3].

М. Л. Оніщенко та Б. І. Сюркало [4] здійснюють детальний аналіз управління економічною безпекою, виділяючи цільовий, системний, функціональний та процесний підходи, та обґрунтовують адаптивність системи безпеки як ключову властивість у мінливому середовищі. Особливості забезпечення безпеки бізнес-процесів у специфічних сферах, зокрема у сфері оптової торгівлі та логістики, досліджував О. Ю. Мішин [5], який систематизував види бізнес-процесів торговельних підприємств та обґрунтував пріоритетні напрями їхнього захисту. Своєю чергою, загальну декомпозицію стратегічної економічної безпеки підприємства та класифікацію загроз у бізнес-процесах вдосконалення, розвитку й

основної діяльності представлено у працях вітчизняних економістів В.П. Валікова та В.В. Македона [6].

Другий напрям досліджень присвячений застосуванню моделювання як інструменту управління ризиками та оптимізації процесів. Роль моделювання бізнес-процесів в умовах цифрової трансформації як засобу ідентифікації критичних точок та підвищення прозорості організаційних систем ґрунтовно проаналізовано у працях науковців, які досліджували методології BPMN, EPC та IDEF0. О. Матусова, В. Андрєєва та В. Ягодзінський [7] розробили модель управління ризиками як складову загальної системи менеджменту підприємства на основі процесного підходу, де ключовими компонентами визначено ідентифікацію, аналіз та оцінку ризиків. Особливості цифровізації бізнес-процесів та управління ризиками в електронному бізнесі досліджували Г. Мельничук, О. Марченко [8]. М. Є. Рогоза, Я. В. Вівтоніченко, Р. Ю. Максимчук та В. І. Шило [9] обґрунтували використання гібридних технологій управління проектами (поєднання традиційних та гнучких методів) для забезпечення безпеки та розвитку бізнес-процесів ІТ-підприємств в умовах євроінтеграційних викликів.

Питання оцінювання ризиків та моделювання процесів у контексті економічної безпеки також знайшли відображення у працях С. Легенчук, Н. Валінкевич та І. Вигівської [10], які запропонували сценарії моделювання інноваційних ризиків на основі внутрішньої звітності про резерви. Г. Лоскорих, І. Грабчук та І. Рогаль [11] розробили карту індикаторів ризиків ІТ-проектів за чотирма групами (персонал, система, проект, зовнішнє середовище). Моделювання рівня зрілості бізнес-процесів під впливом діджиталізації як критерію економічної безпеки представлено у дослідженнях Г. М. Коптєвої [12]. Безпекові аспекти використання хмарних технологій для підвищення ефективності бізнес-процесів географічно розосереджених команд детально охарактеризовано у працях І. Малярчук та М. Смолинця [13].

Третій напрям охоплює інструменти графічного та функціонального моделювання безпекових політик. В. В. Радуш, О. Ю. Лебедєва, Н. І. Кушніренко та В. В. Зоріло [14] запропонували поєднувати високорівневий опис процесів у стандарті IDEF0 із низькорівневим деталізованим описом операцій у нотації BPMN для створення та впровадження організаційної політики безпеки підприємства. Застосування структурно-функціональних діаграм IDEF0 та діаграм потоків даних (DFD) для аналізу та оптимізації процесів обслуговування клієнтів в електронній комерції детально описано О. Пустовіт [15]. Особливості побудови імітаційних моделей бізнес-процесів за допомогою системи Arena компанії Systems Modeling та інтеграції діаграм IDEF3 з імітаційним моделюванням досліджено Т. Січко [16].

Серед зарубіжних науковців вагомий внесок у розвиток моделювання безпеки у бізнес-процесах зробили М. Салнітрі, Ф. Далпіаз та П. Джорджіні [17, 18]. Ними було розроблено фреймворк SecBPMN (SecBPMN2), який включає мову моделювання SecBPMN-ml (безпекове розширення стандарту BPMN з графічними анотаціями інформаційної безпеки), мову запитів SecBPMN-Q для представлення політик безпеки та програмний рушій для автоматичної верифікації відповідності моделей бізнес-процесів цим політикам.

Попри значні наукові здобутки, інтегроване двовекторне моделювання процесу впровадження безпекових функцій у бізнес-процеси суб’єктів господарювання з урахуванням сучасних техніко-економічних параметрів автоматизації та інфраструктурних рішень потребує подальшого комплексного дослідження.

Метою статті є теоретико-методологічне обґрунтування та побудова інтегрованої моделі процесу впровадження безпекових функцій у бізнес-процеси суб’єктів господарювання на основі методологічного синтезу високорівневого функціонального моделювання (IDEF0) та низькорівневого графічного представлення робочих потоків (BPMN/SecBPMN) для мінімізації залишкових ризиків та забезпечення економічної стійкості підприємства.

Виклад основного матеріалу. Сучасне підприємство функціонує як складна соціотехнічна система, в якій діяльність людини, організаційні регламенти та технологічні компоненти перебувають у безперервній взаємодії. Забезпечення економічної безпеки такого суб'єкта господарювання вимагає відмови від традиційного «острівного» підходу до захисту, за якого безпекові заходи реалізуються ізольовано від основної діяльності. Ефективна інтеграція безпекових функцій передбачає концепцію Security-by-Design (безпека за проектом), коли кожен елемент бізнес-процесу від самого початку проектується з урахуванням вбудованих механізмів контролю та захисту.

Математично бізнес-процес BP суб'єкта господарювання можна представити як впорядкований кортеж (1):

$$BP = \langle A, F, R, D, C \rangle, \quad (1)$$

де $A = \{a_1, a_2, \dots, a_n\}$ – множина технологічних, управлінських чи допоміжних операцій (активностей); $F \in A \times A \times L$ – орієнтоване відношення послідовності та логіки виконання операцій, що визначається набором логічних шлюзів та умов L; де $R = \{r_1, r_2, \dots, r_m\}$ – організаційні ролі, виконавці та технічні ресурси, закріплені за операціями; де $D = \{d_1, d_2, \dots, d_k\}$ – інформаційні об'єкти (дані, документи, повідомлення), що споживаються або створюються в процесі; C – сукупність керуючих впливів та регламентів, які регулюють виконання процесу відповідно до стратегічних цілей.

У процесі функціонування кожна операція $a_i \in A$ піддається впливу векторів загроз де $T = \{t_1, t_2, \dots, t_p\}$, які можуть реалізуватися через вразливості системи де $V = \{v_1, v_2, \dots, v_q\}$. Інтеграція безпекових функцій полягає у відображенні вихідного процесу BP у захищений процес BP', де до кожної вразливої операції a_i застосовується вектор безпекових функцій контролю де $\sigma_i = \{s_{i1}, s_{i2}, \dots, s_{is}\}$ (2):

$$a_i' = \varphi(a_i, \sigma_i), \quad (2)$$

де φ – оператор безпекової трансформації.

Ефективність впровадження безпекової функції s_{ij} відносно загрози t_y оцінюється коефіцієнтом зниження ризику *Risk*. Якщо початковий рівень ризику операції $Risk(a_i)$ визначається як добуток ймовірності реалізації загрози $P(t_y \cap v_z)$ на величину потенційних збитків $L(a_i)$ (3):

$$Risk \quad = P(t_y \cap v_z) \times L(a_i), \tag{3}$$

то залишковий ризик захищеної операції $Risk_{res}(a_i)$ набуває вигляду (4):

$$Risk_{res} = P(t_y \cap v_z) \times L(a_i) \times (1 - \theta(s_{ij})). \tag{4}$$

Для забезпечення загальної економічної безпеки бізнес-процесу інтегральний залишковий ризик $Risk_{res}(BP)$ не повинен перевищувати гранично допустиме значення толерантності до ризику $Risk_{limit}$ (5):

$$Risk_{res}(BP) = \sum_{i=1}^{n} w_i \cdot Risk_{res}(a_i) \leq Risk_{limit}, \tag{5}$$

де w_i – коефіцієнт важливості i-ї операції для досягнення стратегічної мети бізнес-процесу.

У випадку, коли бізнес-процес вимагає високого рівня доступності (Availability), моделюється надлишковість операцій. Фреймворк соціотехнічного моделювання виділяє два типи стратегій надлишковості: відмовостійку (fall-back redundancy) та активну (true redundancy) [18]. При активній надлишковості паралельно виконуються основна та дублююча операції, а ймовірність успішного виконання кроку дорівнює (6):

$$P_{success} = 1 - (1 - P(a_{main})) \cdot (1 - P(a_{backup})). \tag{6}$$

При відмовостійкій надлишковості перехід до резервної операції відбувається лише у разі збою основної через виключний шлюз, що мінімізує витрати ресурсів.

Інтеграція цих функцій вимагає розбудови інформаційного забезпечення, що поєднує системи обліку, аналізу та аудиту в єдиний інформаційний простір для підтримки прийняття управлінських рішень.

Для практичної реалізації безпекових трансформацій суб'єктам господарювання доцільно застосовувати двовекторний підхід до моделювання, який дозволяє поєднати концептуальне проектування організаційних заходів із детальним описом робочих процесів на операційному рівні.

Перший вектор базується на методології функціонального моделювання IDEF0. Цей стандарт призначений для високорівневого структурування діяльності організації. У рамках нашого дослідження будується контекстна діаграма А-0 «Створення політики безпеки та інтеграція безпекових функцій».

Функціональний блок декомпозується на рівні А0, де визначаються такі елементи системи [14]:

Вхід (Input): вихідні дані про організаційну структуру підприємства, топологію інформаційних ресурсів, класифікацію об'єктів захисту та чинні технологічні регламенти;

Управління (Control): державні та міжнародні регуляторні акти, галузеві стандарти безпеки (ISO/IEC 27001, ISO/IEC 17799, ISO 45001), а також загальна стратегія розвитку підприємства;

Механізми (Mechanisms): персонал (CISO, спеціалісти з інформаційної безпеки, експертна група, керівники підрозділів), а також інструментальне програмне забезпечення моделювання та автоматизації;

Вихід (Output): задокументована політика безпеки, а також оптимізовані та захищені регламенти бізнес-процесів.

Найважливішою перевагою IDEF0 є повнота відображення керуючих впливів та зворотних зв'язків. Проте цей стандарт не містить інструментів для опису часової послідовності та деталізованої взаємодії виконавців на нижньому рівні.

Другий вектор вирішує це обмеження через впровадження стандарту BPMN (Business Process Model and Notation), який спочатку розроблявся організацією BPMI під керівництвом Стівена Уайта (IBM), а згодом був опублікований Object Management Group (OMG). BPMN є міжнародним стандартом для деталізованого

моделювання та документування робочих потоків. Для візуалізації руху інформаційних об’єктів між підрозділами BPMN доповнюється діаграмами потоків даних (DFD).

Для аналізу динамічних параметрів процесів використовують діаграми IDEF3 (послідовності робіт) та імітаційне моделювання (наприклад, у системі Arena), що дозволяє програвати сценарії та виявляти «вузькі місця». Розподіл відповідальності відображається за допомогою Swim Lane діаграм (доріжок), що полегшує міжфункціональну взаємодію.

Порівняльна оцінка методологій моделювання в контексті інтеграції безпекових функцій представлена в табл. 1.

Для безпосереднього вбудовування безпекових вимог у моделі BPMN використовується фреймворк SecBPMN (SecBPMN2), який розширює стандартну нотацію набором спеціалізованих безпекових понять. Кожна безпекова анотація в моделі SecBPMN-ml супроводжується логічним предикатом, що деталізує умови виконання безпекової функції.

Фреймворк базується на референсній моделі інформаційної безпеки RMIAS та охоплює ключові аспекти безпеки [18]:

Confidentiality (Конфіденційність): забезпечує захист даних від несанкціонованого доступу. Предикат Confidentiality(di, Rallowed) обмежує коло ролей, що мають доступ до об’єкта даних di.

Integrity (Цілісність): гарантує відсутність несанкціонованих змін. Предикат Integrity(di, channel_type) вимагає передачі даних di через захищений канал (наприклад, HTTPS/TLS).

Availability (Доступність): визначає вимоги до безперебійності сервісів. Предикат *Availability(a_i, MTBF, redundancy_type)* регламентує показники надійності та стратегію резервування операції a_i.

Таблиця 1 – Порівняльна характеристика методологій моделювання для задач інтеграції безпеки

Методологія моделювання	Основний об’єкт опису	Рівень деталізації	Можливості відображення безпекових контролів	Переваги застосування	Недоліки та обмеження
IDEF0	Функції системи та їхні взаємозв’язки	Високий (концептуаль-ний)	Обмеження через дуги управління та механізмів	Повнота опису зворотних зв'язків з управління	Відсутність часової послідовності та подій
DFD	Потоки та сховища даних	Середній	Маркування захищених каналів та сховищ	Чітка візуалізація руху конфіденційних даних	Не відображає керуючу логіку та умовні розгалуження
IDEF3 / EPC	Послідовність виконання робіт та події	Середній та низький	Зв'язок безпекових операцій із подіями	Орієнтація на подієву логіку процесу	Складність інтеграції з хмарними BPM-рушіями
BPMN / SecBPMN	Робочі потоки, шлюзи, події та ролі	Низький (виконавчий)	Спеціалізовані графічні анотації та предикати	Можливість автоматичної верифікації та виконання	Вимагає високої кваліфікації бізнес-аналітиків

Джерело: узагальнено авторами за [14, 16, 17,18].

Authenticity (Автентичність): підтверджує ідентичність суб’єктів. Предикат *Authenticity(r_j, auth_method)* визначає метод перевірки автентичності ролі r_j (наприклад, двофакторна автентифікація, SSO).

Accountability (Підзвітність): фіксує відповідальність за дії. Предикат *ccountability(a_i, signature_type)* вимагає обов’язкового підписання результатів операції (наприклад, КЕП).

Auditability (Аудитованість): забезпечує можливість постійного моніторингу. Предикат *AuditabilityAct(a_i, log_storage, audit_period)* вимагає фіксації всіх дій з операцією a_i у захищеному сховищі логів кожні N днів.

Non-repudiation (Невідомовність): унеможливлює спростування фактів виконання дій. Предикат *NonRepudiation(a_i, party_k)* гарантує, що сторона *party_k* не зможе відмовитися від виконаного зобов’язання.

Важливою складовою фреймворку є мова запитів SecBPMN-Q, яка дозволяє аналітикам безпеки формалізувати складні корпоративні політики безпеки у вигляді графічних запитів. Програмний рушій верифікації здійснює перевірку моделі бізнес-процесу SecBPMN-ml на відповідність правилам SecBPMN-Q. Алгоритм аналізує всі можливі шляхи виконання процесу та ідентифікує логічні розриви чи невідповідності.

У табл. 2 наведено деталізовану структуру предикатів SecBPMN для ключових соціотехнічних вимог безпеки підприємства.

Моделювання процесу інтеграції безпекових функцій має безпосередній зв'язок із технічною архітектурою та економічними показниками суб'єкта господарювання. На сучасному етапі розвитку IT-технологій інтеграція безпеки реалізується через передові концепції, такі як SASE (Secure Access Service Edge) та ZTNA (Zero Trust Network Access). Використання посередників безпечного доступу до хмари (CASB) та брандмауерів як послуги (FWaaS) дозволяє консолідувати мережеві та безпекові функції, що спрощує IT-інфраструктуру, знижує витрати на її обслуговування та підтримує безпечну гібридну роботу.

Яскравим прикладом практичного впровадження такого підходу є вітчизняні програмні комплекси класу ERP та BPM. Зокрема, платформа IT-Enterprise та її ForceBPM модуль забезпечують інтеграцію безпеки на всіх етапах життєвого циклу розробки та виконання бізнес-процесів (концепції SSDLC та NIST SSDF). Це мінімізує вразливості ще на етапі дизайну завдань. Відповідність міжнародним стандартам підтверджується сертифікацією ISO 27001:2022 та відповідністю вимогам SOC для хмарних сервісів. Застосування low-code/no-code інструментів (ForceBPM Modeler) дає змогу аналітикам самостійно налаштовувати захищені бізнес-процеси без залучення програмістів.

Таблиця 2 – Специфікація безпекових предикатів у фреймворку SecBPMN

Безпековий аспект	**Формальний предикат SecBPMN**	**Опис параметрів та вимог**	**Практичний приклад впровадження**
Confidentiality	*Confidentiality(d, R, encryption_level)*	Об'єкт даних *d* доступний лише для ролей з множини *R*, шифрування рівня *encryption_level*	Доступ до фінансової звітності підприємства мають лише фінансовий директор та головний бухгалтер
Integrity	*Integrity(d, secure_channel, checksum_method)*	Дані *d* передаються через канал *secure_channel* із перевіркою цілісності за методом *checksum_method*	Передача платіжного доручення до банківського клієнта через TLS-протокол із перевіркою SHA-256
Availability	*Availability(a, fallback_strategy, SLA_hour)*	Операція *a* повинна мати резервний сценарій *fallback_strategy* із відновленням у межах *SLA_hour*	Резервне копіювання бази даних замовлень у хмару з відновленням доступу протягом двух годин
Authenticity	*Authenticity(r, MFA_provider, SSO_flag)*	Виконавець ролі *r* проходить автентифікацію через *MFA_provider* з підтримкою єдиного входу *SSO_flag*	Авторизація менеджера з продажу в CRM-системі через Microsoft Entra ID з обов'язковим MFA
Accountability	*Accountability(a, Ɛ, digital_signature)*	Операція *a* виконується суб'єктами з множини *Ɛ* та скріплюється підписом *digital_signature*	Погодження договору оренди керівником юридичного відділу за допомогою КЕП у мобільному додатку
Auditability	*AuditabilityAct(a, log_vault, N_days)*	Всі дії з операцією *a* логуються у сховищі *log_vault* із проведенням аудиту кожні *N_days*[3]	Запис історії змін лімітів дебіторської заборгованості в аудит-лог з перевіркою внутрішнім аудитором кожні 30 днів
Non-repudiation	*NonRepudiation(a, role, log_record)*	Виконання операції *a* роллю *role* не може бути спростовано завдяки запису *log_record*	Реєстрація факту відвантаження товару зі складу комірником у системі WAF/ERP з незмінним часовим штампом

Джерело: розроблено авторами.

Інтеграція безпеки реалізується на трьох ключових технічних рівнях:

– рівень доступу: контроль доступу на основі ролей (RBAC), багатофакторна автентифікація (MFA) та єдиний вхід (SSO);

– рівень передачі даних: шифрування каналів за протоколом TLS та захист веб-додатків за допомогою WAF;

– рівень зберігання: криптографічне перетворення конфіденційних полів баз даних (шифрування за стандартом AES-256) та захищене медіа-сховище.

Економічний ефект від якісного моделювання та подальшої автоматизації бізнес-процесів із вбудованими функціями безпеки є досить значним. Відповідно до узагальнених статистичних даних господарської практики, суб'єкти господарювання досягають суттєвого покращення операційних показників, що відображено у фінансових результатах діяльності підприємств. Основні економічні результати автоматизації бізнес-процесів представлені такими показниками:

– скорочення операційних витрат у довгостроковій перспективі: 15–25 %;

– зменшення часу виконання бізнес-процесів: 30–50 %;

– підвищення загальної продуктивності праці персоналу: 25–35 %;

– зростання доходів від продажів завдяки якості обслуговування: 10–20 %.

Для забезпечення відповідності інтегрованих безпекових заходів загальній бізнес-стратегії суб'єкта господарювання критично важливою є роль керівника з безпеки (CISO або віртуального vCISO). Такий фахівець повинен досконало розуміти логіку операційних бізнес-процесів для виявлення неочевидних вразливостей, розробляти специфічні заходи контролю та забезпечувати юридичну відповідність національному й міжнародному законодавству.

Управління економічною безпекою бізнес-процесів потребує надійної системи оцінювання, яка базується на індикаторному підході. Індикатори розглядаються як порогові значення показників, що характеризують діяльність підприємства у різних функціональних сферах.

У контексті нашого дослідження оцінювання безпеки бізнес-процесів (зокрема для ІТ-підприємств та високотехнологічних суб'єктів господарювання) здійснюється за допомогою адаптованої карти індикаторів ризику, що охоплює чотири взаємопов'язані групи:

– персонал: коефіцієнт плинності кадрів та витрати на професійне навчання персоналу з питань безпеки протягом звітного періоду;

– система: коефіцієнт накладних витрат, відношення накладних витрат до собівартості реалізованої продукції, рівень невиконання замовлень та динаміка скарг чи негативних відгуків клієнтів щодо завершених проектів;

– проект: кількість днів відхилення у виконанні проекту порівняно з плановим графіком та відсоток виявлених помилок від загальної кількості операцій;

– зовнішнє середовище: рівень податкового навантаження та відповідність регуляторним вимогам.

Окремим важливим аспектом економічної стійкості є інтеграція стандартів охорони та безпеки праці (зокрема ISO 45001) у загальну систему бізнес-процесів. Безпека праці виступає невидимим, але критично важливим фундаментом концепції ESG (Environmental, Social, and Governance).

Для міжнародних партнерів та інвесторів наявність прозорого аудиту безпеки праці є ключовим індикатором надійності компанії. До звітів включаються такі показники, як частота виявлення потенційно небезпечних випадків (Near Miss), загальний рівень виробничого травматизму та відсоток виконання рекомендацій аудитів.

Висновки. Проведене дослідження дозволяє сформувати комплексне теоретико-методологічне та прикладне обґрунтування особливостей моделювання процесу впровадження безпекових функцій у бізнес-процеси суб'єктів господарювання в умовах високої турбулентності цифрового та геополітичного середовища. Доведено, що традиційні підходи до статичного захисту фізичного периметра втратили свою ефективність, актуалізуючи перехід до концепції Security-by-Design, за якої механізми контролю безшовно інтегруються безпосередньо в операційну, управлінську та допоміжну архітектуру підприємства. Запропонований двовекторний підхід до моделювання дозволяє успішно поєднати високорівневе концептуальне проектування організаційних заходів на засадах методології IDEF0 із деталізованим описом і виконанням робочих потоків на операційному рівні за допомогою стандартів BPMN, SecBPMN та діаграм DFD. Застосування

спеціалізованого фреймворку SecBPMN, що базується на референсній моделі інформаційної безпеки RMIAS, забезпечує формалізацію ключових соціотехнічних вимог через систему предикатів конфіденційності, цілісності, доступності, автентичності, підзвітності, аудитованості та невідомовності, уможливлюючи автоматичну верифікацію відповідності моделей бізнес-процесів загальній корпоративній політиці безпеки.

Установлено, що практична реалізація захищених бізнес-процесів тісно пов'язана з сучасною IT-архітектурою підприємства (зокрема концепціями SASE, ZTNA, CASB) та технічними рівнями контролю доступу, передачі й зберігання даних, які успішно масштабуються у вітчизняних ERP та BPM-платформах. Економічний ефект від інтеграції безпекових функцій та автоматизації на базі моделей «to-be» підтверджується суттєвим покращенням операційних показників господарської практики, зокрема зниженням операційних витрат на 15–25 % та підвищенням продуктивності праці на 25–35 %. Управління економічною безпекою соціотехнічної системи підприємства потребує впровадження надійної системи оцінювання на основі індикаторного підходу, що охоплює групи ризиків персоналу, системи, проекту та зовнішнього середовища, а також обов'язкової інтеграції стандартів охорони праці ISO 45001, що виступає базовим фундаментом реалізації міжнародної концепції ESG та ключовим критерієм капіталізації та інвестиційної привабливості сучасного суб'єкта господарювання.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Rybalchenko L., Kosychenko A., Klinytskyi I. Ensuring economic security of enterprises taking into account the peculiarities of information security. *Philosophy, Economics and Law Review*, 2022. Vol. 2, no. 1. P. 96–107. DOI: 10.31733/2786-491X-2022-1-96-107.
2. Гріненко А. Ю. Удосконалення механізмів забезпечення економічної безпеки України: теорія, методологія, практика : автореф. дис. … д-ра екон. наук: 21.04.01. Київ, 2021. 37 с. URL: https://niss.gov.ua/sites/default/files/2021-08/avtoreferat_grinenko.pdf.
3. Панченко В. А. Систематизація підходів до трактування поняття «економічна безпека підприємств». *Ефективна економіка*, 2017. № 11. URL: http://www.economy.nayka.com.ua/?op=1&z=6512.

4. Оніщенко М. Л., Сюркало Б. І. Особливості механізму управління економічною безпекою підприємства. *Економіка і суспільство*, 2018. Вип. 16. С. 446–452. URL: https://economyandsociety.in.ua/journals/16_ukr/68.pdf.

5. Мішин О. Ю. Сутність та пріоритетні напрями забезпечення економічної безпеки підприємницької діяльності в умовах воєнного часу. *Ефективна економіка*, 2025. № 10. DOI: http://doi.org/10.32702/2307-2105.2025.10.51.

6. Валіков В. П., Македон В. В. Економічна безпека підприємства в концепті процесного управління. *Нобелівський вісник*, 2017. № 1 (10). DOI: http://doi.org/10.32342/2616-3853-2017-1-10-2.

7. Матусова О., Андрєєва V., Ягодзінський V. Моделі ризик-менеджменту. *Scientia fructuosa*, 2019. Том 128 № 6. С. 75–84. DOI: https://doi.org/10.31617/visnik.knute.2019(128)07.

8. Мельничук Г., Марченко О. Окремі аспекти цифровізація бізнес-процесів підприємства в сучасних умовах. *Збірник наукових праць Державного податкового університету*, 2021. №1. С. 169–185. DOI: https://doi.org/10.33244/2617-5940.1.2021.169-185.

9. Рогоза М. Є., Вівтоніченко Я. В., Максимчук Р. Ю., Шило В. І. Стратегування регіональних інноваційних екосистем: проектний підхід аналізу динаміки економічної безпеки під час війни в контексті потреби інноваційної модернізації. *Вісник економічної науки України*, 2025. № 1 (48). С. 87–94. DOI: https://doi.org/10.37405/1729-7206.2025.1(48).87-94.

10. Lehenchuk S., Valinkevych N., Vyhivska I. Облікові резерви в оптимізації ризиків інноваційної діяльності. *Financial and Credit Activity Problems of Theory and Practice*, 2021. Vol. 2(33). pp. 174–184. DOI: https://doi.org/10.18371/ fcaptp.v2i33.206594.

11. Лоскоріх Г. Л., Грабчук І. Л., Рогаль В. П. Облікове забезпечення управління ризиками діяльності ІТ-підприємств. *Економіка, управління та адміністрування*, 2021. Вип. 4(98). С. 75–80. DOI: https://doi.org/10.26642/ema-2021-4(98)-75-80.

12. Коптєва Г. М. Підходи до оцінки зрілості бізнеспроцесів підприємства з позиції їх економічної безпеки. *Ефективна економіка*, 2020. № 4. DOI: https://doi.org/10.32702/2307-2105-2020.4.69.

13. Малярчук І., Смолинець М. Підвищення ефективності бізнес-процесів через застосування хмарних технологій: безпековий аспект. *Економіка та суспільство*, 2024. № 60. DOI: https://doi.org/10.32782/2524-0072/2024-60-3.

14. Радуш В. В., Лебедєва О. Ю., Кушніренко Н. І., Зоріло В. В. Моделювання організаційних заходів для створення політики безпеки організації з використанням бізнес-процесів. *Інформатика та математичні методи в моделюванні*, 2021. Том 11. № 3. DOI: https://doi.org/10.15276/imms.v11.no3.239.

15. Пустовіт О. Можливості та переваги електронної комерції в підприємницькій діяльності. *Розвиток методів управління та господарювання на транспорті*, 2023. Т. 83. № 2. С. 83–94. DOI: https://doi.org/10.31375/2226-1915-2023-2-83-94.

16. Січко Т. Методи моделювання бізнес-процесів підприємства засобами системного аналізу. *Галицький економічний вісник*. 2016. № 2. С. 190-201. URL: http://nbuv.gov.ua/UJRN/gev_2016_2_27.

17. Salnitri M., Dalpiaz F., Giorgini P. Designing Secure Business Processes with SecBPMN. *Software & Systems Modeling*, 2015. Vol.16. pp. 737–757 (2017). DOI: https://doi.org/10.1007/s10270-015-0499-4.

18. Salnitri M., Dalpiaz F., Giorgini P. Modeling and Verifying Security Policies in Business Processes. In book: *Enterprise, Business-Process and Information Systems Modeling*. (pp.200–214), 2014. DOI: https://doi.org/10.1007/978-3-662-43745-2_14.

REFERENCES:

1. Rybalchenko L., Kosychenko A., Klinytskyi I. (2022). Ensuring economic security of enterprises taking into account the peculiarities of information security. *Philosophy, Economics and Law Review*. vol. 2. no. 1. pp. 96–107. https://doi.org/10.31733/2786-491X-2022-1-96-107.

2. Hrinenko A. Yu. (2021). *Udoskonalennia mekhanizmiv zabezpechennia ekonomichnoi bezpeky Ukrainy: teoriia, metodolohiia, praktyka* [Improvement of mechanisms for ensuring economic security of Ukraine: theory, methodology, practice] (Author's abstract of Doctor's thesis). Kyiv. Available at: https://niss.gov.ua/sites/default/files/2021-08/avtoreferat_grinenko.pdf.

3. Panchenko V. A. (2017). Systematyzatsiia pidkhodiv do traktuvannia poniattia «ekonomichna bezpeka pidpryiemstv» [Systematization of approaches to the interpretation of the concept of economic security of enterprises]. *Efektyvna Ekonomika,* no. 11. Available at: http://www.economy.nayka.com.ua/?op=1&z=6512.

4. Onishchenko M. L., Siurkalo B. I. (2018). Osoblivosti mekhanizmu upravlinnia ekonomichnoiu bezpekoiu pidpryiemstva [Peculiarities of the mechanism of enterprise economic security management]. *Ekonomika i Suspilstvo,* vol. 16. pp. 446–452. Available at: https://economyandsociety.in.ua/journals/16_ukr/68.pdf.

5. Mishyn O. Yu. (2025). Sutnist ta priorytetni napriamy zabezpechennia ekonomichnoi bezpeky pidpryiemnytskoi diialnosti v umovakh voiennoho chasu [The essence and priority directions of ensuring the economic security of entrepreneurial activity in wartime conditions]. *Efektyvna Ekonomika*, no. 10. http://doi.org/10.32702/2307-2105.2025.10.51.

6. Valikov V. P., Makedon V. V. (2017). Ekonomichna bezpeka pidpryiemstva v kontsepti protsesnoho upravlinnia [Economic security of the enterprise in the concept of process management]. *Nobelivskyi Visnyk*, no. 1(10). http://doi.org/10.32342/2616-3853-2017-1-10-2.

7. Matusova O., Andrieieva V., Yahodzinskyi V. (2019). Modeli ryzyk-menedzhmentu [Risk management models]. *Scientia Fructuosa*, vol. 128. no. 6. pp. 75–84. https://doi.org/10.31617/visnik.knute.2019(128)07.

8. Melnychuk H., Marchenko O. (2021). Okremi aspekty tsyfrovizatsiia biznes-protsesiv pidpryiemstva v suchasnykh umovakh [Certain aspects of digitalization of business processes of the enterprise in modern conditions]. *Zbirnyk Naukovykh Prats Derzhavnoho Podatkovoho Universitetu*, no. 1. pp. 169–185. https://doi.org/10.33244/2617-5940.1.2021.169-185.

9. Rohoza M. Ye., Vivtonichenko Ya. V., Maksymchuk R. Yu., Shylo V. I. (2025). Stratehuvannia rehionalnykh innovatsiinykh ekosistem: proektnyi pidkhid analizu dynamiky ekonomichnoi bezpeky pid chas viiny v konteksti potreby innovatsiinoi modernizatsii [Strategizing of regional innovation ecosystems: a project approach to analyzing the dynamics of economic security during the war in the context of the need for innovative modernization]. *Visnyk Ekonomichnoi Nauky Ukrainy*, no. 1(48). pp. 87–94. https://doi.org/10.37405/1729-7206.2025.1(48).87-94.

10. Lehenchuk S., Valinkevych N., Vyhivska I. (2021). Oblikovi rezervy v optymizatsii ryzykiv innovatsiinoi diialnosti [Accounting reserves in risk optimization of innovation activity]. *Financial and Credit Activity Problems of Theory and Practice*, vol. 2(33). pp. 174–184. https://doi.org/10.18371/fcaptp.v2i33.206594.

11. Loskorikh H. L., Hrabchuk I. L., Rohal V. P. (2021). Oblikove zabezpechennia upravlinnia ryzykamy diialnosti IT-pidpryiemstv [Accounting support for risk management of IT enterprises activity]. *Ekonomika, Upravlinnia ta Administruvannia*, vol. 4(98). pp. 75–80. https://doi.org/10.26642/ema-2021-4(98)-75-80.

12. Koptieva H. M. (2020). Pidkhody do otsinky zrilosti biznes-protsesiv pidpryiemstva z pozytsii yikh ekonomichnoi bezpeky [Approaches to assessing the maturity of enterprise business processes from the standpoint of their economic security]. *Efektyvna Ekonomika*, no. 4. https://doi.org/10.32702/2307-2105-2020.4.69.

13. Maliarchuk I., Smolynets M. (2024). Pidvyshchennia efektyvnosti biznes-protsesiv cherez zastosuvannia khmarnykh tekhnolohii: bezpekovyi aspekt [Increasing the efficiency of business processes through the use of cloud technologies: security aspect]. *Ekonomika ta Suspilstvo*, no. 60. https://doi.org/10.32782/2524-0072/2024-60-3.

14. Radush V. V., Lebedieva O. Yu., Kushnirenko N. I., Zorilo V. V. (2021). Modeliuvannia orhanizatsiinykh zakhodiv dlia stvorennia polityky bezpeky orhanizatsii z vykorystanniam biznes-protsesiv [Modeling organizational measures to create an organization security policy using business processes]. *Informatyka ta Matematichni Metody v Modeliuvanni*, vol. 11. no. 3. https://doi.org/10.15276/imms.v11.no3.239.

15. Pustovit O. (2023). Mozhlyvosti ta perevahy elektronnoi komertsii v pidpryiemnytskii diialnosti [Opportunities and advantages of e-commerce in entrepreneurial activity]. *Rozvytok Metodiv Upravlinnia ta Hospodariuvannia na Transporti*, vol. 83, no. 2. pp. 83–94. https://doi.org/10.31375/2226-1915-2023-2-83-94.

16. Sichko T. (2016). Metody modeliuvannia biznes-protsesiv pidpryiemstva zasobamy systemnoho analizu [Methods of modeling enterprise business processes by means of systems analysis]. *Halytskyi Ekonomichnyi Visnyk*, no. 2. pp. 190–201. Available at: http://nbuv.gov.ua/UJRN/gev_2016_2_27.

17. Salnitri M., Dalpiaz F., Giorgini P. (2017). Designing Secure Business Processes with SecBPMN. *Software & Systems Modeling*, vol. 16. pp. 737–757. https://doi.org/10.1007/s10270-015-0499-4.

18. Salnitri M., Dalpiaz F., Giorgini P. (2014). Modeling and Verifying Security Policies in Business Processes. In *Enterprise, Business-Process and Information Systems Modeling* (pp. 200–214). https://doi.org/10.1007/978-3-662-43745-2_14.

Стаття надійшла до редакції:08.04.2026; рецензування: 15.04.2026;
прийнята до публікації 21.04.2026. Автори прочитали и дали згоду рукопису.
The article was submitted on 08.04.2026; revised on 15.04.2026; and accepted for publication on 21.04.2026. The authors read and approved the final version of the manuscript.