УДК 004:519.872 **DOI**: https://doi.org/10.31521/modecon.V39(2023)-08

Касьянова Н. В., доктор економічних наук, професор, завідувач кафедри бізнес-аналітики та цифрової економіки, Національний авіаційний університет, м. Київ, Україна

ORCID: 0000-0001-7729-2011
e-mail: nat_kas@ukr.net

Біличенко М. М., аспірант кафедри бізнес-аналітики та цифрової економіки, Національний авіаційний університет, м. Київ, Україна

ORCID: 0000-0003-4657-1039

Севериненко А. О., здобувач вищої освіти кафедри бізнес-аналітики та цифрової економіки, Національний авіаційний університет, м. Київ, Україна

ORCID: 0009-0001-8393-0101

Моделювання цифрової безпеки підприємства

Анотація. *Метою дослідження є розробки економіко-математичної моделі цифрової безпеки, яка дозволяє оцінити можливості підприємства протистояти цифровим ризикам та мінімізувати ймовірні збитки шляхом формування багаторівневої системи цифрової безпеки підприємства.*

Пропонується цифрову безпеку розглядати у декількох аспектах. На макрорівні, це загальний стан захищеності інформаційно-цифрового середовища країни, який забезпечує її формування, використання та розвиток в інтересах громадян, підприємств та держави. На мікрорівні – стан захищеності цифрової інформації підприємства, який дозволяє забезпечити існування та інноваційний розвиток підприємства незалежно від наявності внутрішніх і зовнішніх цифрових загроз. У роботі визначено основні види цифрових ризиків та загроз у діяльності підприємства. Для зменшення ризикованості цифрового середовища підприємства пропонується використання моделі цифрової безпеки підприємства, яка включає концептуальну, математичну та функціональну моделі. Концептуальна модель спрямована на відображення загальної структури цифрової безпеки. Математична модель описує можливі сценарії цифрових загроз та дозволяє оцінити можливість їх реалізації, дати кількісну оцінку якості функціонування системи захисту, оцінити економічну ефективність застосування засобів захисту та визначити структуру побудови системи захисту цифрового середовища підприємства. Функціональна модель відображає конкретні функції служб захисту цифрового середовища підприємства.

Ключові слова: *цифрова безпека; цифрове середовище підприємства; цифровий ризик; модель цифрової безпеки.*

Kasianova Nataliia, Doctor of Economics, Professor, The Head of the Department of Business Analytics and Digital Economy, National Aviation University, Kyiv, Ukraine

Bilychenko Maksym, graduate student of the Department of Business Analytics and Digital Economy, National Aviation University, Kyiv, Ukraine

Severynenko Artem, applicant for higher education of the Department of Business Analytics and Digital Economy, National Aviation University, Kyiv, Ukraine

Modeling the Digital Security of the Enterprise

Abstract. Introduction*. Digitization of business processes is accompanied by new dangers: malfunctions of automated equipment, cyber-attacks, threats and security breaches in information systems, which hackers and cybercriminals can use to penetrate databases and obtain information from both computer systems and cloud services. Creating a digital security system is one of the unsolved tasks in many companies.*

Purpose *of the study is to develop an economic-mathematical model of digital security, which allows to assess the capabilities of the enterprise to resist digital risks and minimize probable losses by forming a multi-level system of digital security of the enterprise.*

Results. *It is proposed to consider digital security in several aspects. At the macro level, this is the general state of security of the country's information and digital environment, which ensures its formation, use and development in the interests of citizens, enterprises and the state. At the micro level – the state of security of the enterprise's digital information, which allows to ensure the existence and innovative development of the enterprise regardless of the presence of internal and external digital threats. The work defines the main types of digital risks and threats in the company's activities. To reduce the riskiness of the enterprise's digital environment, it is proposed to use the enterprise's digital security model, which includes conceptual, mathematical, and functional models. The conceptual model aims to reflect the overall structure of digital security. The mathematical model describes possible*

[1]**Стаття надійшла до редакції**: 11.05.2023
Received: 11 May 2023

scenarios of digital threats and allows you to assess the possibility of their implementation, to give a quantitative assessment of the quality of the functioning of the protection system, to assess the economic efficiency of the application of protection means and to determine the structure of the construction of the system of protection of the digital environment of the enterprise. The functional model reflects the specific functions of the enterprise's digital environment protection services.

Conclusions. *It is important to have a well-thought-out system of digital security of the enterprise from the point of view of technologies and mechanisms for combating all possible threats to both business operations and technologies. Rapid detection of threats provides information about intruders and other probable events, allowing for proper risk assessment and timely implementation of appropriate measures to protect the enterprise's digital environment.*

Keywords: *digital security; digital enterprise environment; digital risk; digital security model.*

JEL Classification: *A12; C44; D83; E26.*

Постановка проблеми. Цифрова трансформація економіки підштовхнула компанії до цифровізації своїх процесів, використання програмного забезпечення та IT-інструментів для автоматизації процесів, які раніше виконувались вручну. Підприємства отримують низку переваг як від економії коштів, так і від покращення соціально-психологічного клімату, оскільки працівники можуть відмовитися від монотонних завдань і приділяти більше часу творчій роботі. На сьогодні фактично утворюється нове цифрове середовище підприємства, яке за визначенням М. Бєлобородової [1] включає: виробництво та реалізацію продукції на засадах автоматизації бізнес-процесів й електронної комерції, взаємодію з державою шляхом застосування інформаційних систем е-звітність та е-послуги, управління підприємством відповідно до концепції «спільного споживання» та систему забезпечення цифрової безпеки. Цифрове середовище підприємства має нагальну потребу в регламентації поведінки, забезпеченні комунікацій та безпеки всередині цього середовища.

Водночас цифровізація бізнес-процесів супроводжується новими небезпеками: збоями у роботі автоматизованого обладнання, кібератаками, загрозами та порушеннями безпеки в інформаційних системах, якими хакери та кіберзлочинці можуть скористатися для проникнення у бази даних та отримання інформації як з комп'ютерних систем, так і з хмарних сервісів. Створення системи цифрової безпеки є одним із невирішених завдань у багатьох компаніях. Більшість підприємств використовують неякісні методи захисту інформації, що робить їх уразливими до втрати даних. Так, за даними Генеральної прокуратури України за 2022 рік було порушено 3415 кримінальних справ у сфері інформаційних технологій, що на 917 більше порівняно з 2020 роком [2].

У 2020 р. у світі було зафіксовано 1120 масованих витоків інформації та кібератак. У цілому понад 20 млрд записів було зламано. У другому кварталі 2022 р. кількість нападів зловмисників на промислові підприємства зросла у півтора раза щодо попереднього періоду. Атаки в більшості випадків призводили до витоків конфіденційної інформації (55 %) та порушень роботи індустріальних об'єктів (53 %). Більшість кібератак мають фінансову мотивацію. Частка атак із використанням шкідливого програмного забезпечення становила 76 %, а лідерами виявилися програми-вимагачі (61 %) [3].

Економічні витрати від порушень безпеки інформаційних і технологічних активів в світі у 2020 р. становили 4-6 трлн дол., що еквівалентно 4-6% світового ВВП [4]. Україна щорічно втрачає 1-3 млрд дол. прямих іноземних інвестицій внаслідок низького рівня цифрової безпеки. Промисловість входить до трійки галузей, що найчастіше піддаються інформаційним атакам.

Аналіз останніх досліджень та публікацій. Проблеми впливу цифрової трансформації економіки на економічну безпеку суб'єктів господарювання розглядають у своїх роботах Г. Ткачук [5], Ю. Самойленко [6], С. Співаковський [7]. Г. Мельничук та В. Мамалига [8] особливу увагу приділяють взаємозв'язку понять «економічна безпека», «диджиталізація» та «Економіка 4.0» на макроекономічному рівні. В роботі Т. Передерій [9] розглянуто проблему інформаційної безпеки в умовах цифрових трансформацій на рівні держави. Краус К. та Краус Н. у своїй роботі [10] досліджують питання кібербезпеки на мікрорівні.

Однак, попри досить суттєвий науковий доробок протягом останніх років, у напрямі цифрової безпеки, недостатньо розглянутою залишається проблема забезпечення цифрової безпеки окремих суб'єктів господарювання. Особливо гостро ця проблема постає перед підприємствами, адже саме вони є найбільш вразливою ланкою з точки зору цифрових загроз.

Формулювання цілей дослідження. Зважаючи на вищенаведене, метою даної статті є розробка економіко-математичної моделі цифрової безпеки, яка дозволяє оцінити можливості підприємства протистояти цифровим ризикам та мінімізувати ймовірні збитки шляхом формування багаторівневої системи цифрової безпеки підприємства.

Основні результати дослідження. Не зважаючи на наявність гострої проблеми кібершахрайства та захисту економічної інформації підприємств в

умовах цифровізації, саме поняття «цифрової безпеки» досі чітко не визначено. Науковці використовують різні погляди на сутність цифрової безпеки. Так, М. Саврук вважає, що «цифрова безпека – це стан захищеності інформації, яка забезпечує життєво важливі інтереси підприємства та суспільства в цілому» [11]. Т. Ткачук визначає цифрову безпеку як «безпеку об'єкта від інформаційних загроз або негативних впливів, які пов'язані з інформацією, та нерозголошення даних про той чи інший об'єкт, що є комерційною таємницею» [5]. На думку Н. Аванесової цифрова безпека є «основним компонентом інформаційної безпеки та являє собою комплекс заходів, спрямованих на захист конфіденційності, цілісності та доступності інформації від вірусних атак і несанкціонованого втручання» [12].

На наш погляд, цифрову безпеку необхідно розглядати у декількох аспектах. На макрорівні, це загальний стан захищеності інформаційно-цифрового середовища країни, який забезпечує її формування, використання та розвиток в інтересах громадян, підприємств та держави. На мікрорівні, це стан захищеності цифрової інформації підприємства, який дозволяє забезпечити існування та інноваційний розвиток підприємства незалежно від наявності внутрішніх і зовнішніх цифрових загроз. Таким чином, цифрова безпека означає гарантію дотримання трьох основних принципів роботи в цифровому середовищі: конфіденційність (запобігання розкриття інформації стороннім особам); цілісність (захист даних від несанкціонованого доступу чи модифікації); доступність (управління потоком даних та інформаційними процесами).

Забезпечення цифрової безпеки бізнесу в Україні знаходиться на досить низькому рівні. Всупереч тому, що підприємства різних галузей промисловості, включаючи енергетику, продовжують збільшувати бюджети на цифрову безпеку і впроваджувати рішення для захисту інформаційних систем, ситуація в галузі докорінно не змінюється. Аналіз захищеності промислових компаній показує, що майже будь-яке підприємство, незалежно від його масштабу та пулу засобів захисту, може бути зламано лише за кілька кроків. Краще питання цифрової безпеки вирішується у банківському секторі економіки, хоча і тут становище не завжди можна назвати задовільним. Банки наслідують загальносвітові тенденції у розвитку своєї інформаційної діяльності, у секторі роздрібних операцій з банківськими платіжними картками впроваджено світові регламенти функціонування.

Проблема безпеки конфіденційної інформації та комерційної таємниці існувала і раніше. Але в міру розвитку засобів обробки та зберігання даних підвищується ймовірність їх витоку та незаконного копіювання. Якщо раніше для крадіжки креслень нового продукту потрібно було фізично винести їх із заводу, зараз достатньо отримати доступ до сервера через електронні канали зв'язку або записати на карту пам'яті. За даними [13] близько 11 % випадків витоку інформації з обмеженим доступом відбувається через недбалість співробітників компаній, 14 % – через хакерські та вірусні атаки, 31 % – з метою навмисного заподіяння матеріальної шкоди підприємству власними співробітниками. Під час проведення аудиту інформаційного забезпечення діяльності промислових підприємств було визначено, що у кадрових договорах зазвичай передбачено розділ конфіденційності інформації. Але ці розділи не мають під собою регламентної бази, основою якої є класифікація інформації, що циркулює в організації, з урахуванням оцінки її інформаційної критичності для бізнесу. При цьому важливо зберігати простий доступ до інформації тим людям, які на законних підставах користуються базами даних.

Найчастіше крадіжці підлягають такі дані: інформація про реальний фінансовий стан компанії; інноваційні розробки науково-технічних відділів; реєстраційні дані для доступу до захищених серверів; персональні дані працівників тощо. Додатковою складністю є те, що крадіжка інформації може негативно позначитися на компанії не відразу після її вчинення, а через певний час. Крім того, з'являється загроза підміни інформації в базах даних компанії, що може привести до прийняття помилкових управлінських рішень. Найчастіше навмисні кібератаки спрямовані на доступ, зміну або знищення конфіденційної інформації, здирництво грошей у користувачів або порушення безперервності бізнесу. Неважливі, на перший погляд, дані при їх оприлюдненні можуть завдати шкоди репутації компанії та зменшити її ринкову вартість.

Виходячи зі специфіки розповсюдження цифрових технологій на господарську практику промислових підприємств [14] та сфери їх безпосереднього використання доцільно розглядати три критичні поля виникнення цифрових ризиків та загроз: безпека даних; трансформація бізнес-процесів та надійність цифрових систем й інфраструктури. Основні види цифрових ризиків та загроз у діяльності підприємства наведено у таблиці 1.

Таблиця 1 **Цифрові ризики підприємства**

Детермінанти ризику	Загроза втрат	Ключові сфери управління
Технологія	Загроза втрат через технологічні збої або застарілі технології	Масштабованість, сумісність та функціональна точність впровадженої технології
Кіберпростір	Несанкціонований доступ (експлуатація мережі) з подальшим використанням проникнення для зловмисних дій, наприклад, здирництва та перешкоджання нормальному ходу бізнес-процесів	Зміцнення платформи, мережевої архітектури; безпека додатків; управління вразливістю та моніторинг безпеки
Стратегія	Загроза втрат зазвичай пов'язана з цілями та завданнями організації. Ризик може бути зовнішнім стосовно організації та при виникненні викликає зміну стратегічного спрямування її діяльності. Як правило, це впливає на взаємодію з клієнтами, цінність бренду, репутацію та конкурентні переваги на ринку	Розвиток системи моніторингу; досягнення відповідного рівня контролю в операційних процедурах
Дані	Загроза витоку або втрати даних	Забезпечення захисту даних у цифровій екосистемі на різних етапах життєвого циклу; області управління фокусом стосуватимуться класифікації, зберігання, обробки, шифрування даних тощо
Треті особи (споживачі, постачальники)	Включає ризики, що виникають через неналежний контроль з боку постачальників, сторонніх операційних середовищ, їх кібервразливість	Ключові елементи управління стосуватимуться обміну даними, інтеграції технологій, залежності від операцій, стійкості до відмови постачальників тощо
Конфіденційність	Загроза, що виникає через неналежне поводження з особистими та конфіденційними персональними даними клієнта, співробітника	Дотримання принципів конфіденційності: повідомлення, вибору, згоди, точності та інших
Нормативно-правове середовище	Загроза втрат відноситься до будь-яких нових вимог або правил, створюваних державою і які виходять за рамки чинних команд управління та/або ризик-менеджменту. Організація наражається на ризик недотримання нормативних вимог щодо бізнес-операцій, зберігання даних та інших правил ведення бізнесу	Дотримання законодавчих вимог, включаючи закони про технології, галузеві закони та нормативні акти
Стійкість підприємства	Ризик збоїв у роботі або недоступності послуг через високу залежність від тісно пов'язаних технологій	Безперервність бізнесу, аварійне відновлення IT-мереж, кіберстійкість та антикризове управління
Персонал	Низька цифрова грамотність співробітників, плинність персоналу	Розвиток людських ресурсів, навчання та підвищення цифрової грамотності, аутсорсинг персоналу

Джерело: складено авторами на основі [14]

Загальні напрями мінімізації цифрових ризиків на рівні підприємства тісно пов'язані з подальшим прогресом цифрових технологій – штучного інтелекту, Інтернету-речей та «розумних» мереж, блокчейну, інтегрованих системних центрів з обробки великих даних, з розвитком технологій десенсибілізації даних, оцінки та сертифікації відповідності вимогам безпеки, механізмів захисту шифрування та пов'язаних з ними методів технічного моніторингу для збирання та інтеграції масових даних тощо.

Побудова системи цифрової безпеки передбачає обов'язково розгляд таких об'єктивних чинників:

- загрози цифрової безпеки, ймовірність їх виникнення та реалізації;
- вразливостей системи цифрової безпеки;
- ризик та можливі збитки у разі успішної реалізації цифрової загрози, яка знайде відображення у ймовірних прямих чи непрямих фінансових втратах.

При створенні моделі цифрової безпеки будемо розглядати такі об'єкти як: ресурси інформаційної системи; інформаційні системи; цифрові технології; програмні засоби; мережі зв'язку; автоматизовані виробничі системи. Під об'єктом захисту розуміється інформація та інформаційний процес, які необхідно захищати відповідно до мети цифрової безпеки.

Пропонуємо побудову моделі цифрової безпеки підприємства здійснювати на основі системного підходу: концептуальна, математична та функціональна моделі. Концептуальна модель включає перелік взаємопов'язаних понять, їх

властивості, характеристики, класифікацію з урахуванням типів, ситуації, ознак галузі та умови протікання процесу цифровізації. Необхідно розглянути можливі загрози та джерела їх виникнення, способи реалізації, цілі та інші чинники, які здатні погіршити безпекову ситуацію. Створення концептуальної моделі цифрової безпеки підприємства спрямоване на надання відповідей на загальні питання та відображення загальної структури моделі, на основі якої будуть будуватись моделі нижніх рівнів. Концептуальна модель цифрової безпеки, яка є спільною всіх підприємств, представлена на рисунку 1.

Математична модель цифрової безпеки – це опис можливих сценаріїв у вигляді послідовності дій порушників цифрової безпеки та відповідних заходів у відповідь. Такі моделі описують процеси взаємодії порушника із системою захисту та можливі результати дій [15]. У процесі створення математичної моделі цифрової безпеки проводиться експертна оцінка ймовірності загроз з урахуванням їхньої значущості та ступеня фінансових витрат на відновлення нормального функціонування підприємства та збереження даних після атак та витоків інформації.

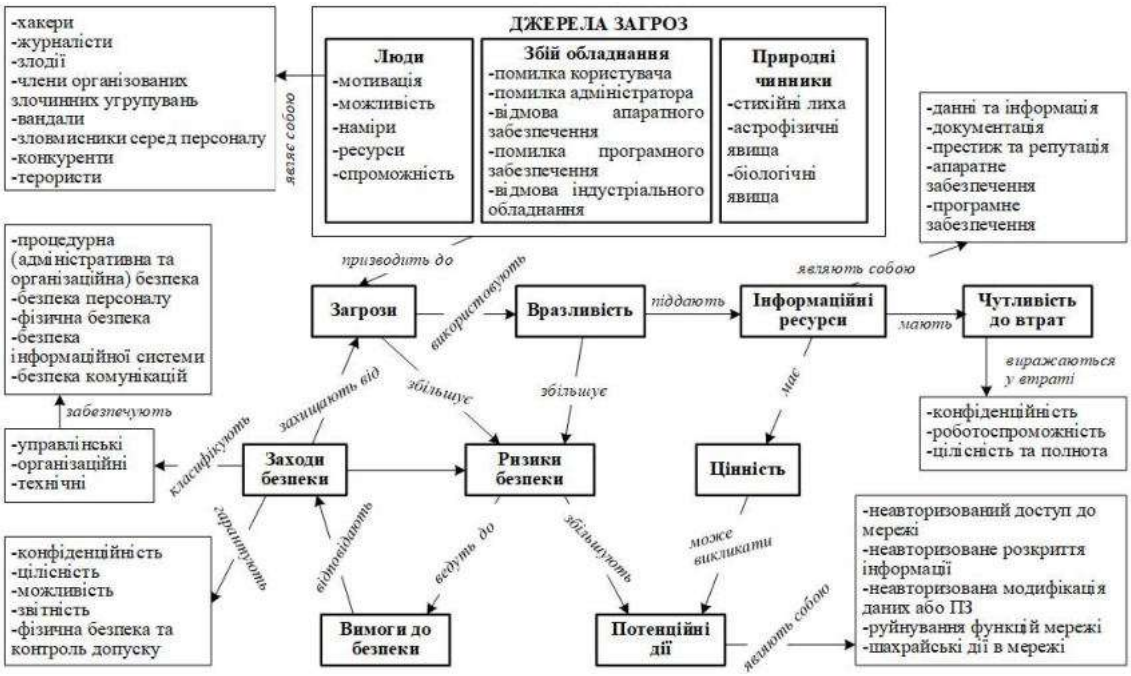

Рисунок 1 – **Концептуальна модель цифрової безпеки підприємства**

Джерело: побудовано авторами

Математична модель цифрової безпеки дозволяє оцінити можливість реалізації різних загроз цифровому середовищу підприємства та проведення атак на нього, дати кількісну оцінку якості функціонування системи захисту, оцінити економічну ефективність застосування засобів захисту та визначити структуру побудови системи захисту цифрового середовища підприємства. Якщо загальні грошові витрати на усунення ризиків менші або рівні максимальному рівню витрат, що виділяються на зниження або усунення сумарних ризиків, систему цифрової безпеки вважають фінансово виправданою.

Розглянемо основні етапи економіко-математичного моделювання системи цифрової безпеки підприємства. Перший етап – визначення об'єкта дослідження (описує конкретні характеристики цифрового середовища підприємства). На другому етапі задаються параметри, що визначають джерела потенційних атак («зловмисників»). За наявністю формальних уявлень про цифрове середовище підприємства, що досліджується, та потенційних загроз переходимо до третього етапу – визначаємо типи атак, яким може піддаватися підприємство, а також пов'язаний із ними ризик. Четвертим етапом є аналіз стійкості цифрового середовища підприємства до атак, які визначено на попередньому етапі. П'ятий етап – використання різних підходів до оцінки економічної ефективності системи цифрової безпеки та заходів протидії атакам.

Таким чином, завдання полягає у розробці математичної моделі цифрової безпеки підприємству, яка дозволяє формалізувати взаємозв'язок між параметрами цифрового середовища підприємства, потенційними «зловмисниками» та можливими атаками. В залежності від галузевої приналежності та особливостей підприємства розробляються багатокритеріальні класифікаційні схеми, які дозволяють ідентифікувати три основні елементи моделі:

1) цифрове середовище підприємства за критеріями: доступність інформації, місце її зберігання, рівень контролю за технологічними процесами, система захисту інформації та тип її реалізації тощо;

2) потенційного «зловмисника» з урахуванням його мотивації, технологічних можливостей та кваліфікації;

3) цифрову атаку з позиції застосування різних інструментів і необхідних для її здійснення ресурсів.

На основі класифікаційних схем будується низка параметричних моделей:

$A \subseteq A_1 * A_2 * \dots * A_n$ – множина параметричних моделей атак, де $A_i (i = \{1, n\})$ – тип атаки відповідно критеріям розробленої класифікації. Фактично, кожна модель $\vec{a} \in A$ є вектором класифікаційних ознак для конкретної атаки.

$\vec{b} \in B$ – параметрична модель «зловмисника», де $B \subseteq B_1 * B_2 * \dots * B_m$ – множина значень *j*-го параметра моделі «зловмисника».

Модель цифрового середовища підприємства описує вектор $\vec{c} \in C$, де $C \subseteq C_1 * C_2 * \dots * C_k$ – множина значень *k* параметрів моделі цифрового середовища.

Зауважимо, що множини значень параметрів моделей є кінцевими.

З кожною атакою пов'язано значення ризику, який обчислюється за загальновідомою формулою на основі двох факторів – ймовірності події та важкості можливих наслідків. Позначимо через $R: A * B * C \to [0; 1]$ функцію, яка задає рівень ризику, пов'язаного з атакою $\vec{a} \in A$ в умовах, коли вона може бути застосована «зловмисником» $\vec{b} \in B$ для злому цифрової системи підприємства $\vec{c} \in C$. Введемо до моделі показники впливу атаки на цифрове середовище підприємства у вигляді можливих втрат від результатів атаки $I: C * A \to [0; 1]$ та ймовірності того, що «зловмисник» здійснить атаку, тобто володіє ресурсами для її здійснення і визнає цю атаку доцільною $P: B * A \to [0; 1]$. Тоді функція ризику буде мати вигляд: $R(\vec{a}, \vec{b}, \vec{c}) = I(\vec{c}, \vec{a}) * P(\vec{b}, \vec{a})$.

Визначимо функцію $I(\vec{c}, \vec{a})$. Функція I_{li} задає рівень взаємовпливу параметрів цифрового середовища підприємства C_l і параметрів атаки A_i:

$I_{li}(c, a) = 0$ – якщо атаку зі значеннями параметру $a \in A_i$ неможливо здійснити до цифрового середовища з параметром $c \in C_l$;

$0 < I_{li}(c, a) < 1$ – якщо значення параметра цифрового середовища $c \in C_l$ зменшує успіх проведення атаки з параметром $a \in A_i$;

$I_{li}(c, a) = 1$ – якщо значення параметра с $\in C_l$ не впливає на реалізацію атаки $a \in A_i$;

$I_{li}(\mathrm{c}, a) > 1$ – якщо значення параметра с $\in C_l$ вказує на те, що проведення атаки $a \in A_i$ буде успішним.

Рівень взаємовпливу параметрів цифрового середовища та атаки визначається за допомогою експертних оцінок (1):

$$\overline{I_{li}}(c, a) = \frac{I_{li}(c,a)}{\sum_{\xi \in C_l} I_{li}(\xi, a)}, \qquad (1)$$

де $I_{li}(\xi, a)$ – оцінка атаки ξ-м експертом.

Тоді рівень втрат від застосування атаки $\vec{a} \in A$ до цифрового середовища підприємства $\vec{c} \in C$ обчислюється за формулою (2):

$$I(\vec{c}, \vec{a}) = \min_i \prod_l \overline{I_{li}}(c_l, a_i), \qquad (2)$$

де атака та цифрове середовище задані векторами $(a_1, a_2, \dots, a_n)$ та $(c_1, c_{k2}, \dots, c_k)$ відповідно. Зауважимо, що рівень впливу цифрового середовища на застосування атаки із заданими значенням *l*-го параметру $(l = \{1, k\})$ визначається за мультиплікативним критерієм $\prod_l \overline{I_{li}}(c_l, a_i)$. Якщо значення хоча б одного параметра цифрового середовища підприємства визначає неможливість проведення атаки, то результат оцінки дорівнюється нулю, що відповідає нульовому рівню втрат від даної атаки.

Залежність між векторами атаки $(a_1, a_2, \dots, a_n)$ та «зловмисника» $(b_1, b_2, \dots, b_m)$, визначається за допомогою аналогічної функції $P(\vec{b}, \vec{a})$. Таким чином, узагальнена формула оцінки рівня ризику, який пов'язаний з атакою $\vec{a} \in A$ на цифрове середовище підприємства $\vec{c} \in C$ «зловмисником» $\vec{b} \in B$, має вигляд (3):

$$R(\vec{a}, \vec{b}, \vec{c}) = \min_i \prod_l \overline{I_{li}}(c_l, a_i) * \min_i \prod_j \overline{P_{jl}}(b_j, a_i) \quad (3)$$

Будемо вважати, що цифрове середовище підприємства $\vec{c} \in C$ схильне до атак $\vec{a} \in A$ з боку «зловмисників» $\vec{b} \in B$, якщо $R(\vec{a}, \vec{b}, \vec{c}) > 0$, тобто рівень ризику перевищує задане порогове значення ϑ, де $\vartheta \in [0;1]$. Припустимий рівень ризику є параметром моделі, який налаштовується.

В описаній математичній моделі зроблено наступні припущення: не враховується залежність параметрів атаки від поєднання параметрів цифрового середовища підприємства, хоча вплив кожного параметра враховується; не враховується можливість спільних дій із боку різних типів «зловмисників», хоча можна задати модель нападу з боку однорідного колективу «зловмисників». Подолання цих припущень є метою подальших досліджень.

Для покращення системи цифрової безпеки підприємства необхідно використовувати інструментальні засоби, які дозволяють протидіяти можливим атакам. А відповідно на основі сформованої математичної моделі необхідно побудувати функціональну модель, яка своєю чергою вимагає особливої уваги, враховуючи розгляд конкретних заходів із захисту цифрового середовища підприємства. Функціональна модель визначає конкретні функції служб захисту протидії, в першу чергу, тим видам атак і тим «зловмисникам», дії яких можуть завдати найбільших втрат підприємству. Формування системи цифрової безпеки підприємства вимагає певних організаційних дій, що здійснюються для перевірки та підтримки безпеки в рамках всього набору компонент кожної цифрової операції: цифрові дані; узагальнену інформацію; IT-мережі та інфраструктуру компанії; співробітників, які керують процесами цифрових знань та навичок. При цьому

потрібно сформувати впорядкований набір функцій, з урахуванням вхідних даних (матеріальних об'єктів), обмежень, виконавців та очікуваного результату.

Функціональна модель захисту цифрового середовища підприємства повинна усувати причини та можливості незаконного доступу до цифрового середовища підприємства, оперативно реагувати на загрози та пропонувати ефективні рішення, до яких відносять:

фізичний захист цифрового середовища підприємства внаслідок обмеження доступу певних осіб до місць зберігання даних, права доступу визначаються за допомогою засобів ідентифікації особистості;

загальні засоби захисту – програми та утиліти, які повинні використовуватися під час роботи в мережі (антивірусні програми, фільтри електронних листів, системи логінів та паролів для доступу у внутрішню мережу тощо);

протидія DDoS-атакам – використання зовнішніх утиліт для виявлення підозрілого трафіку або різкого збільшення запитів на доступ;

резервування інформації шляхом її копіювання на віддалені сховища або «хмару»;

план поновлення роботи після втручання вводиться у дію у разі, якщо підприємство не може функціонувати у стандартному режимі або виявлено стороннє втручання;

передача зашифрованих даних між віддаленими користувачами повинна проводитися тільки з використанням утиліт кінцевого шифрування, що дає можливість переконатися в справжності даних і виключити розшифровку третіми особами, які перехопили повідомлення.

Висновки. Важливо мати добре продуману систему цифрової безпеки підприємства з погляду технологій та механізмів боротьби з усіма можливими загрозами як бізнес-операціям, так і технологіям. Швидке виявлення загроз надає інформацію про зловмисників та інші ймовірні події, дозволяє провести належну оцінку ризиків та своєчасно реалізувати відповідні заходи щодо захисту цифрового середовища підприємства.

Використання інтелектуального аналізу даних дає можливість виявити закономірності у машинних даних. Так, використовуючи Інтернет речей для моніторингу промислових та комерційних середовищ, можна розгорнути системи сигналізації, які можуть виявляти підвищення температури, рівнів потужності або радіації, щоб запобігти групі реагування для вжиття відповідних заходів. Аналогічні системи на засадах штучного інтелекту можуть бути застосовані для моніторингу цифрової безпеки підприємства. І формування подібних систем на основі запропонованого комплексу моделей цифрової безпеки і є завданням подальших досліджень.

Література:

1. Бєлобородова М.В. Економічна безпека суб'єктів підприємництва в умовах переходу до цифрової економіки. *Актуальні аспекти розвитку суб'єктів підприємництва в умовах глобальної економіки*. Дніпро, 2021. С. 349-358.
2. Кіберзлочинність: виклики часу. *Chernivtsi law school*: веб-сайт. URL: https://law.chnu.edu.ua/kiberzlochynnist-vyklyky-chasu (дата звернення: 04.05.2023).
3. The role of cybersecurity and data security in the digital economy. *The UN Capital Development Fund*: веб-сайт. URL: https://static1.squarespace.com/static/5f2d7a54b7f75718fa4d2eef/t/62082f066a25c62651a9ae40/1644703527175/EN-UNCDF-Brief-CyberSecurity-2022.pdf (дата звернення: 04.05.2023).
4. Threat report T1 2022. *Welivesecurity*: веб-сайт. URL: https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf (дата звернення: 04.05.2023).
5. Ткачук Г.О. «Цифрові» трансформації: взаємозв'язок із системою економічної безпеки підприємства. *Економіка харчової промисловості*. 2019. Том 11, № 4. С. 42–50. URL: https://journals.ontu.edu.ua/index.php/fie/article/view/1545/1764 (дата звернення: 07.05.2023).
6. Samoilenko Y., Britchenko I., Levchenko I., Lošonczi P., Bilichenko O., Bodnar O. Economic Security of the Enterprise Within the Conditions of Digital Transformation. *Economic Affairs*. 2022. Vol. 67, № 4. P. 619-629. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/45358/1/Economic%20Security%20of%20the%20Enterprise%20Within%20the%20Conditions%20of%20Digital%20Transformation.pdf (дата звернення: 07.05.2023).
7. Spivakovskyy S., Kochubei O., Shebanina O., Yaroshenko I., Nych T. The impact of digital transformation on the economic security of Ukraine. *Estudios de Economia Aplicada*. 2021. Vol. 39, № . URL: https://fileview.fwdcdn.com/?url=https://mail.ukr.net/api/public/file_view/list%3Ftoken%3DGeacg5rqMKvwX7LOTGCX9ZHUCQGyNMfCQBhIXAh9fs7YJ5MS020FyTne2IFfnE4wr-AqtVLc8dwZVxicp1ZOU6742BiUtJnuflk:cqLU-60WdW5BkY_C%26r%3D1683826491198&default_mode=view&lang=ru#start=1 (дата звернення: 07.05.2023).
8. Мельничук Г., Мамалига В. () Цифровізація економіки: можливості та загрози для ефективного функціонування підприємств. *Приазовський економічний вісник*. 2020. № 2 (19). С. 125–130. URL: http://pev.kpu.zp.ua/journals/2020/2_19_ukr/23.pdf (дата звернення: 07.05.2023).
9. Передерій Т. () Стратегія цифрової безпеки підприємства як драйвер цифрової трансформації економіки України. *Вісник економічної науки України*. 2019. № 2 (37). С. 201–204. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/163994/34-Perederii.pdf?sequence=1http://dspace.nbuv.gov.ua/bitstream/handle/123456789/163994/34-Perederii.pdf?sequence=1 (дата звернення: 07.05.2023).
10. Краус К., Краус Н., Штепа О. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability*. 2022. № 3. С. 26–37. URL: https://ins.vntu.edu.ua/index.php/ins/article/view/60/75 (дата звернення: 09.05.2023).
11. Саврук М.В. Актуальність проблеми забезпечення інформаційної безпеки України та шляхи її розв'язання системи обробки інформації. *Системи обробки інформації*. 2010. № 3 (84). С. 77-79.

12. Аванесова Н.Е., Мордовцев О.С., Колодяжна Т.В. Формування механізму комплексного забезпечення цифрової безпеки промислового підприємства України. *Вісник НТУ «ХПІ» (економічні науки)*. 2020. № 3. С. 9-14. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/d0a9d2dd-a103-4cf3-b641-f36e4f30eb2c/content (дата звернення: 09.05.2023).
13. Сніщенко Р.Г., Гринчуцький В.І. Інформаційна безпека як складова економічної безпеки суб'єктів господарювання. *Економічний аналіз.* 2020. № 30 (1). С. 241-248. URL: https://www.econa.org.ua/index.php/econa/article/view/1787 (дата звернення: 09.05.2023).
14. Касьянова Н.В., Кравчук Н.М., Коваль Ю.Л. Безпека підприємства в умовах цифрової трансформації економіки. *Modern Economics.* 2020. № 20. С. 124-129.
15. Rudnichenko Y., Melnyk S., Havlovska N., Illiashenko O., Nakonechna N. Strategic interaction of state institutions and enterprises with economic security positions in digital economy. *WSEAS Transactions on Business and Economics*. 2021. № 18. С. 218–230. URL: https://www.wseas.org/multimedia/journals/economics/2021/a465107-009(2021).pdf (дата звернення: 09.05.2023).

References:

1. Bieloborodova, M.V. (2021). Economic security of business entities in the conditions of the transition to the digital economy. Current aspects of the development of business entities in the conditions of the global economy. monogr. [in Ukrainian].
2. Cybercrime: challenges of the times. Retrieved from : https://law.chnu.edu.ua/kiberzlochynnist-vyklyky-chasu/ [in Ukrainian].
3. The role of cybersecurity and data security in the digital economy. Retrieved from : https://static1.squarespace.com/static/5f2d7a54b7f75718fa4d2eef/t/62082f066a25c62651a9ae40/1644703527175/EN-UNCDF-Brief-CyberSecurity-2022.pdf
4. Threat report T1 2022. Retrieved from : https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf
5. Tkachuk, H. (2019). "Digital" transformations: relationship with the economic security system of the enterprise. *Economics of the food industry*. 11 (4). 42–50. Retrieved from : https://journals.ontu.edu.ua/index.php/fie/article/view/1545/1764 [in Ukrainian].
6. Samoilenko, Y., Britchenko, I., Levchenko, I., Lošonczi, P., Bilichenko, O. & Bodnar O. (2022). Economic Security of the Enterprise Within the Conditions of Digital Transformation. *Economic Affairs*. 67 (4), 619-629. Retrieved from : https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/45358/1/Economic%20Security%20of%20the%20Enterprise%20Within%20the%20Conditions%20of%20Digital%20Transformation.pdf
7. Spivakovskyy, S., Kochubei, O., Shebanina, O., Yaroshenko, I. & Nych, T. (2021). The impact of digital transformation on the economic security of Ukraine. *Estudios de Economia Aplicada*. 39 (5). Retrieved from : https://fileview.fwdcdn.com/?url=https://mail.ukr.net/api/public/file_view/list%3Ftoken%3DGeacg5rqMKvwX7LOTGCX9ZHUCQGyNMfCQBhIXAh9fs7YJ5MS020FyTne2IFfnE4wr-AqtVLc8dwZVxicp1ZOU6742BiUtJnuflk:cqLU-60WdW5BkY_C%26r%3D1683826491198&default_mode=view&lang=ru#start=1
8. Melnychuk, H. & Mamalyha V. (2020). Digitization of the economy: opportunities and threats for the effective functioning of enterprises. *Pryazovsky Economic Bulletin.* 2 (19). 125–130. Retrieved from : http://pev.kpu.zp.ua/journals/2020/2_19_ukr/23.pdf [in Ukrainian].
9. Perederij, T. (2019). The digital security strategy of the enterprise as a driver of the digital transformation of the economy of Ukraine. *Herald of economic science of Ukraine.* 2 (37). 201–204. Retrieved from : http://dspace.nbuv.gov.ua/bitstream/handle/123456789/163994/34-Perederii.pdf?sequence=1http://dspace.nbuv.gov.ua/bitstream/handle/123456789/163994/34-Perederii.pdf?sequence=1 [in Ukrainian].
10. Kraus, K., Kraus, N. & Shtepa, O. (2022). Digital transformation of cyber security at the micro level in martial law. *Innovation and Sustainability*. 3. 26–37. Retrieved from : https://ins.vntu.edu.ua/index.php/ins/article/view/60/75 [in Ukrainian].
11. Savruk, M.V. (2010). The urgency of the problem of ensuring the information security of Ukraine and ways of solving it in the information processing system. *Information processing systems.* 3 (84).77-79. [in Ukrainian].
12. Avanesova, N.E., Mordovtsev, O.C. & Kolodiazhna, T.V. (2020). Formation of the mechanism of comprehensive provision of digital security of the industrial enterprise of Ukraine. *Bulletin of NTU "KhPI" (economic sciences).* 3. 9-14. Retrieved from : https://repository.kpi.kharkov.ua/server/api/core/bitstreams/d0a9d2dd-a103-4cf3-b641-f36e4f30eb2c/content [in Ukrainian].
13. Snischenko, R.H. & Hrynchuts'kyj, V.I. (2020). Information security as a component of economic security of economic entities. *Economic analysis*. 30 (1). 241-248. Retrieved from : https://www.econa.org.ua/index.php/econa/article/view/1787 [in Ukrainian].
14. Kasianova, N.V., Kravchuk, N.M. & Koval, Yu.L. (2020). Security of the enterprise in the conditions of digital transformation of the economy. *Modern Economics*. 20. 124-129. [in Ukrainian].
15. Rudnichenko, Y., Melnyk, S., Havlovska, N., Illiashenko, O. & Nakonechna, N. (2021). Strategic interaction of state institutions and enterprises with economic security positions in digital economy. *WSEAS Transactions on Business and Economics*. 18. 218–230. Retrieved from : https://www.wseas.org/multimedia/journals/economics/2021/a465107-009(2021).pdf

Ця робота ліцензована Creative Commons Attribution 4.0 International License