Менеджмент
УДК 005.322:004.056:159.9
DOI https://doi.org/10.5281/zenodo.20557789

Лідерство як стратегічний ресурс управління інформаційною безпекою організації: психологічні та безпекові виміри

Ольга Зіновіївна Воронка,
кандидат економічних наук, доцент, доцент кафедри менеджменту та економічної безпеки, Львівський державний університет внутрішніх справ
https://orcid.org/0000-0001-8334-7613

Ольга Ігорівна Пацула,
кандидат економічних наук, доцент, доцент кафедри менеджменту та економічної безпеки, Львівський державний університет внутрішніх справ
https://orcid.org/0000-0002-1815-7554

Прийнято: 16.05.2026 | Опубліковано: 30.05.2026

Анотація. *Актуальність дослідження зумовлена потребою переосмислення моделей захисту даних в умовах цифрової трансформації, зростання витонченості кібератак, високої уразливості людського фактора та наближення організацій до світових стандартів безпекової культури. Метою статті є теоретичне обґрунтування та аналіз ролі лідерства у забезпеченні інформаційної безпеки організацій, з особливим акцентом на психологічних аспектах ідентифікації ризиків та формуванні стійкої системи захисту від внутрішніх і зовнішніх загроз. Методологічну основу становлять системний підхід, синергетичний підхід, поведінковий та інституційний аналіз, порівняльний аналіз і змістовий аналіз джерел. У статті уточнено зміст*

лідерства як стратегічного ресурсу управління інформаційною безпекою; систематизовано емпіричний профіль зовнішніх, внутрішніх та фізичних загроз; сформовано методологічну матрицю інтеграції тріади CIA в систему менеджменту; охарактеризовано трирівневу ієрархічну вертикаль організаційної відповідальності; визначено стратегічні напрями мінімізації інсайдерських ризиків. Запропоновано концептуальну модель лідерства як інтегруючого фактора в системі інформаційної безпеки, яка поєднує технічний, нормативно-організаційний та психологічний компоненти в єдину управлінську архітектуру. Практична цінність результатів полягає у можливості їх використання для вдосконалення корпоративного управління, розробки адаптивних політики безпеки, зниження операційних та репутаційних ризиків, оптимізації інвестицій у кіберзахист та формування стійкої безпекової культури в сучасних організаціях.

Ключові слова: *лідерство, інформаційна безпека, управління ризиками, людський фактор, тріада CIA, психологічна безпека, культура безпеки, кібербезпека.*

Leadership as a strategic resource for managing information security of an organization: psychological and security dimensions

Olga Voronka

PhD, Associate Professor of the Department of Management and Economic Security, Lviv State University of Internal Affairs, Lviv, Ukraine, https://orcid.org/0000-0001-8334-7613

Olga Patsula

PhD, Associate Professor of the Department of Management and Economic Security, Lviv State University of Internal Affairs, Lviv, Ukraine, https://orcid.org/0000-0002-1815-7554

Abstract. *The relevance of the study is due to the need to rethink data protection models in the context of digital transformation, the growth of sophistication of cyberattacks, high vulnerability of the human factor and the approximation of organizations to global standards of security culture. The purpose of the article is to theoretically substantiate and analyze the role of leadership in ensuring information security of organizations, with special emphasis on the psychological aspects of risk identification and the formation of a stable system of protection against internal and external threats. The methodological basis is a systemic approach, a synergistic approach, behavioral and institutional analysis, comparative analysis and content analysis of sources. The article clarifies the content of leadership as a strategic resource for information security management; systematizes the empirical profile of external, internal and physical threats; forms a methodological matrix for integrating the CIA triad into the management system; characterizes the three-level hierarchical vertical of organizational responsibility; identifies strategic directions for minimizing insider risks. A conceptual model of leadership as an integrating factor in the information security system is proposed, which combines technical, regulatory-organizational and psychological components into a single management architecture. The practical value of the results lies in the possibility of their use for improving corporate governance, developing adaptive security policies, reducing operational and reputational risks, optimizing investments in cyber protection and forming a sustainable security culture in modern organizations.*

Keywords: *leadership, information security, risk management, human factor, CIA triad, psychological security, security culture, cybersecurity.*

Постановка проблеми. У сучасному цифровому світі питання інформаційної безпеки набуває стратегічного значення для будь-якої організації. Традиційні технічні засоби захисту (firewalls, шифрування, антивірусне ПЗ) вже не гарантують належного рівня безпеки, адже більшість інцидентів спричинені

«людським фактором». Це висуває на перший план психологічну готовність персоналу та роль керівника, який здатний формувати культуру безпеки в організації. Лідерство перестає бути лише адміністративною функцією й трансформується у стратегічний ресурс управління, що забезпечує цілісність та конфіденційність даних. Саме інтеграція психологічних та безпекових вимірів лідерства визначає стійкість організації до кіберзагроз і робить дослідження цієї проблематики надзвичайно актуальним.

Феномен інформаційної безпеки та побудова систем захисту інформації в сучасному кіберпросторі є об'єктом пильної уваги багатьох науковців. Питання моделювання технічних ризиків, розробки засобів захисту комп'ютерних систем та нормативного формування політик безпеки на основі тріади CIA ґрунтовно дослідили такі вітчизняні вчені, як В. Бурячок, Р. Грищук, Ю. Даник та В. Хорошко [1, 3]. Особливості побудови організаційної структури та ієрархічної вертикалі систем управління інформаційною безпекою (СУІБ) на підприємствах висвітлено у наукових працях В. Домарєва та С. Гордієнка [5], тоді як інтегровані підходи до оцінки та моніторингу динамічних загроз у складних інфраструктурах запропоновано О. Можаєвим [12].

Значну увагу в науковому дискурсі приділено також соціогуманітарним та психологічним аспектам менеджменту. Психологію управління, роль людського фактора у забезпеченні операційної стійкості колективів та специфіку поведінки персоналу в організаційному середовищі детально вивчено у фундаментальних роботах Л. Карамушки [11, с. 234]. Питання трансформації лідерських функцій у сучасних умовах та обґрунтування лідерства як стратегічного управлінського ресурсу відображено у працях Н. Гавкалової та В. Марченко [3]. Серед вагомих зарубіжних напрацювань варто відзначити концепцію психологічної безпеки робочого простору А. Едмондсона [15], а також прикладні дослідження М. Сіпонена, спрямовані на вивчення психологічних чинників дотримання персоналом правил кібергігієни [16].

ISSN: 2786-9431

Попри значну кількість глибоких досліджень у кожній із зазначених сфер, питання безпосередньої синергії сучасних моделей лідерства з практичними інструментами кіберзахисту залишаються маловивченими. Більшість наявних публікацій розглядають лідерську функцію окремо від жорстких технічних правил безпеки, замикаючи ІБ виключно в інженерній площині. Це зумовлює гостру потребу в інтеграційному дослідженні, яке дозволить об'єднати управлінський потенціал лідера, психологічні методи впливу на лояльність людей та технологічні стандарти захисту даних у межах єдиної стратегії менеджменту.

Виділення невирішених раніше частин загальної проблеми Незважаючи на активний розвиток досліджень у сфері кібербезпеки, більшість наукових праць мають суто технічний характер. Вчені переважно вивчають програми захисту, шифрування даних та налаштування мереж. Водночас у теорії менеджменту лідерство розглядають як інструмент підвищення прибутків, але рідко пов'язують його із захистом інформації [13, с. 93].

Поза увагою дослідників залишається роль лідера як головного зв'язуючого елемента між суворими технічними правилами та психологією працівників. Недостатньо вивченим є те, як саме керівник може впливати на поведінку людей, щоб знизити ризики «людського фактора» (наприклад, через створення культури довіри, де люди не бояться повідомляти про помилки). Брак простих і цілісних моделей, які об'єднують технології, правила та психологію навколо лідера, і визначає актуальність цієї статті.

Постановка проблеми. Складність сучасних кібератак, зокрема методів соціальної інженерії, спрямована не на злам програмного коду, а на маніпуляцію психологічними станами співробітників (страхом, цікавістю, поспіхом). Водночас внутрішні загрози, спричинені стресом або низьким рівнем залученості персоналу, створюють приховані уразливості в системі управління організацією. Таким чином, виникає гостра потреба у дослідженні лідерства як

інструменту, що інтегрує технічні протоколи безпеки з психологічними методами управління людьми.

Метою статті є теоретичне обґрунтування та аналіз ролі лідерства у забезпеченні інформаційної безпеки організацій з особливим акцентом на психологічних аспектах ідентифікації ризиків та формуванні стійкої системи захисту від внутрішніх і зовнішніх загроз.

Для досягнення поставленої мети у статті передбачається розв'язання таких **завдань**:

1. Дослідити трансформацію лідерства у стратегічний ресурс інформаційної безпеки (ІБ) в умовах глобальної цифровізації та розвитку кіберзагроз.

2. Розробити концептуальну модель інтегруючої ролі лідера як ядра системи управління інформаційної безпеки, що гармонізує технологічні, нормативні та психологічні компоненти організації.

3. Визначити психологічні та безпекові виміри впливу лідерства на людський фактор, формування свідомої «культури безпеки» персоналу та лояльності стейкхолдерів.

Виклад основного матеріалу дослідження. Інформаційна безпека (ІБ) виступає фундаментом загальної системи безпеки сучасного підприємства, інтегруючи комплекс заходів, спрямованих на всебічний захист інформаційних активів від несанкціонованого втручання, розголошення або знищення [1; 6]. В умовах цифрової трансформації інформація перетворилася на стратегічний актив, що визначає ефективність бізнес-процесів та якість лідерських рішень. Відтак, забезпечення ІБ — це не лише технічне завдання, а пріоритетна функція стратегічного менеджменту.

Сучасна система ІБ покликана забезпечувати надійний захист даних, мережевої інфраструктури та програмного забезпечення від спектру

ISSN: 2786-9431

деструктивних загроз, здатних дестабілізувати діяльність установи [5]. Серед них особливої уваги лідера потребують:

- Кіберзлочинність: високотехнологічна та динамічна загроза, що вимагає від керівництва проактивного мислення, безперервного моніторингу ризиків та готовності до швидкої адаптації стратегій захисту з метою уникнення фінансових і репутаційних втрат [3].
- Промислове шпигунство: критичний ризик несанкціонованого доступу до інтелектуального капіталу інноваційних компаній, що актуалізує роль лідера у формуванні психологічного клімату внутрішньої лояльності та надійного захисту комерційних таємниць [9, с. 123].
- Техногенні та природні чинники: технічні збої, аварії або катастрофи, мінімізація руйнівних наслідків яких безпосередньо залежить від якості розроблених керівництвом планів забезпечення безперервності бізнесу (Business Continuity Planning) [7].

Особливе місце у системі безпеки займає психологічна готовність персоналу протидіяти цим загрозам [8]. Глибоке розуміння лідером того, що інформація є не просто статичним набором даних, а життєво важливим ресурсом розвитку, дозволяє трансформувати політику ІБ із формального переліку адміністративних обмежень у базовий елемент організаційної культури [15]. За такого підходу кожен співробітник стає свідомим суб'єктом безпекового процесу, який чітко усвідомлює власну роль у захисті спільного капіталу організації.

Ризики втрати даних, зумовлені технічними збоями або ненавмисними помилками персоналу, становлять пряму загрозу безперервності бізнес-процесів та фінансовій стабільності сучасної організації. У цьому контексті ефективне управління інформаційною безпекою (ІБ) виступає не лише як локальний технічний інструмент мінімізації ризиків, а як критично важлива лідерська компетенція, спрямована на упередження збитків та підтримання загальної

 ISSN: 2786-9431

операційної стійкості установи. Фундаментом сучасних ділових відносин є довіра зацікавлених сторін до надійності та безпеки інформаційних систем. Здатність лідера гарантувати недоторканність і захищеність цифрових активів стає ключовим фактором довгострокової конкурентоспроможності на ринку.

Реалізація лідерської стратегії у сфері захисту даних базується на фундаментальній тріаді принципів — конфіденційності, цілісності та доступності (CIA) [1]. Проте в межах сучасної парадигми менеджменту ці принципи розглядаються не просто як ізольовані технічні вимоги, а як стратегічні вектори формування адаптивної системи захисту.

Лідер забезпечує конфіденційність через вибудову чіткої ієрархії доступу, гарантує цілісність даних як єдину надійну основу для прийняття управлінських рішень та підтримує безперервну доступність ресурсів [4]. Для системного розуміння взаємозв'язку між стандартами, функціями керівника та аспектами персоналу, основні компоненти захисту структуровано у таблиці 1.

Таблиця 1.

Матриця лідерського управління інформаційною безпекою (ІБ) на засадах тріади CIA

Принцип ІБ	**Технічний аспект (Інструменти)**	**Роль лідера (Управлінський аспект)**	**Психологічний аспект (Людський фактор)**
Конфіденційність	Шифрування, контроль доступу (IAM), двофакторна автентифікація.	Розподіл зон відповідальності, впровадження політик «мінімальних привілеїв».	Виховання етики роботи з даними, формування лояльності для запобігання інсайдерству.
Цілісність	Хешування, цифрові підписи, системи контролю версій.	Встановлення регламентів перевірки даних, аудит бізнес-процесів.	Розвиток уважності та відповідальності співробітників за достовірність звітності.
Доступність	Резервне копіювання (Cloud/Offline), відмовостійкі сервери (HA).	Розробка планів відновлення після збоїв (DRP) та безперервності бізнесу (BCP).	Зниження рівня стресу в команді під час кризових ситуацій (атак/збоїв) для швидкої реакції.

Джерело**:** *розроблено авторами на основі* [1; 4; 6].

ISSN: 2786-9431

Як видно з Таблиці 1, ефективна система інформаційної безпеки не обмежується лише технічним інструментарієм. Вона потребує активного залучення лідера для трансформації технологічних стандартів у організаційні цінності та психологічні установки персоналу. Тільки через поєднання цих трьох рівнів (технічного, лідерського та психологічного) можна досягти справжньої організаційної стійкості.

У системі стратегічного управління сучасною організацією комплексна оцінка ризиків виступає фундаментальним процесом [12]. Вона дозволяє лідеру своєчасно ідентифікувати загрози, що здатні дестабілізувати діяльність підприємства та слугує аналітичним підґрунтям для прийняття управлінських рішень.

Ключовим етапом цього процесу є ідентифікація загроз та вразливостей, що потребує від керівництва глибокого розуміння всіх потенційних джерел небезпеки для інформаційних ресурсів. Ефективна лідерська стратегія передбачає комплексний аналіз середовища функціонування організації, охоплюючи всі аспекти діяльності, що можуть стати об’єктом атаки [6, с. 234].

Традиційно загрози класифікуються на зовнішні та внутрішні, кожна з яких потребує специфічних лідерських та психологічних підходів:

Зовнішні загрози представлені переважно кіберзлочинністю (DDoS-атаки, малваре, фішинг), що спрямована на викрадення фінансових даних або руйнування ділової репутації. У цьому контексті завдання лідера полягає у забезпеченні технологічної готовності та розвитку когнітивної стійкості персоналу до методів соціальної інженерії. Окрему групу становлять форс-мажорні чинники природного характеру, які вимагають наявності чітких протоколів кризового управління.

Внутрішні загрози найбільш тісно пов’язані з психологічними аспектами управління. Вони включають як ненавмисні помилки персоналу (неправильне налаштування систем, випадковий витік даних), так і свідомі дії внутрішніх

ISSN: 2786-9431

зловмисників. Це підкреслює роль лідера у створенні прозорої системи контролю доступу та безперервного навчання співробітників. Формування високої корпоративної відповідальності та лояльності є основним лідерським інструментом мінімізації ризиків, що походять зсередини організації.

Ідентифікація вразливостей у сучасних організаційних системах вимагає від керівництва багатовимірного підходу, що охоплює аналіз технічних, організаційних та людських факторів. Це передбачає не лише виявлення слабких місць у програмному забезпеченні чи мережевій інфраструктурі, а й критичний перегляд систем управління доступом та процесів обробки даних. Лідерська роль у цьому контексті полягає у систематичному аудиті політик безпеки для виявлення прогалин, які можуть бути використані зловмисниками. Використання передових інструментів, таких як сканування вразливостей, тестування на проникнення та моделювання загроз, стає частиною загальної стратегії лідерського контролю за станом захищеності установи.

Ефективне виявлення загроз дозволяє організації розробляти цілеспрямовані заходи безпеки, спрямовані на мінімізацію потенційного впливу на бізнес-процеси. Проактивне управління ризиками, ініційоване вищою ланкою менеджменту, сприяє підтримці високого рівня довіри з боку клієнтів та партнерів. Завдяки безперервному вдосконаленню процесів ідентифікації, організація отримує здатність своєчасно реагувати на нові виклики цифрового середовища, адаптуючи стратегії захисту до динамічних змін кіберпростору. Це гарантує безперебійність фінансових послуг та зміцнює конкурентоспроможність організації [8].

Критично важливим етапом управління є оцінка ймовірності та потенційного впливу ризиків, що дозволяє лідерам ефективно розставляти пріоритети. Після ідентифікації загроз менеджмент організації переходить до детального моделювання сценаріїв: наскільки вірогідною є реалізація конкретної атаки та які наслідки вона матиме для операційної діяльності.

ISSN: 2786-9431

Оцінка ймовірності базується на синтезі історичних даних та прогнозного аналізу поточного ландшафту кіберзагроз. Важливим аспектом лідерського аналізу тут є врахування факторів, що сприяють реалізації загроз: від технологічних недоліків до рівня підготовки персоналу. Такий інтегрований підхід дозволяє трансформувати технічні дані в управлінську стратегію, де безпека стає невід'ємною частиною організаційної культури.

Загрози інформаційній безпеці характеризуються високою динамічністю та здатністю до постійної еволюції паралельно з технологічним прогресом. Для ефективного управління ризиками лідер має розрізняти природу зовнішніх та внутрішніх викликів, оскільки кожен із них потребує специфічних психологічних та організаційних інструментів протидії.

Зовнішні кіберзагрози як виклик стратегічній стійкості. Кіберзлочинність на сучасному етапі трансформувалася у високотехнологічну індустрію, що використовує методи фішингу, розповсюдження шкідливого ПЗ (малваре) та DDoS-атак. Особливу увагу лідер має приділяти фішингу, оскільки цей метод базується на психологічній маніпуляції (соціальній інженерії). Протидія таким атакам лежить не лише в площині IT-фільтрів, а й у площині розвитку критичного мислення команди. Захист від програм-вимагачів та технічних атак на відмову в обслуговуванні (DDoS) вимагає від керівництва інвестицій у відмовустійку інфраструктуру та чітких регламентів кризового менеджменту.

Внутрішні загрози та роль лідера у їх мінімізації. Внутрішні ризики, що походять від персоналу з легальним доступом до даних, часто виявляються складнішими для виявлення, ніж зовнішні атаки. Лідерська стратегія у цьому напрямку має враховувати два аспекти [8] :

1. Психологічна підтримка та навчання**:** мінімізація ненавмисних помилок (ненавмисного розголошення даних) через підвищення кіберграмотності та зниження рівня професійного стресу.

 ISSN: 2786-9431

2. Контроль та етика: запобігання свідомим зловживанням шляхом впровадження прозорих систем моніторингу та формування високої корпоративної етики, де викрадення інформації є неприпустимим на рівні цінностей.

Недостатність лідерської уваги до підготовки кадрів та слабкість процедур контролю створюють «сприятливе» середовище для реалізації внутрішніх загроз. Відтак, завданням сучасного керівника є створення такої архітектури безпеки, де технічні обмеження гармонійно поєднуються з високим рівнем усвідомленості та лояльності працівників.

Окрім кібернетичних викликів, стратегічне управління інформаційною безпекою має враховувати фізичні загрози, здатні спричинити незворотне пошкодження інфраструктури та втрату критичних даних. Пожежі, природні катаклізми, крадіжки обладнання або акти вандалізму вимагають від лідера впровадження надійних бар'єрів: від систем біометричного контролю доступу до відеоспостереження. Проте ключовою функцією лідерства у цьому контексті є розробка та тестування планів безперервності бізнесу (BCP), які гарантують швидке відновлення операційної діяльності після будь-якого фізичного інциденту.

Системний аналіз свідчить, що загрози інформаційній безпеці є багатогранними і вимагають не лише технічної протидії, а й комплексного управлінського підходу. Ефективний захист активів неможливий без активного управління людським фактором. Лідер має виступати ініціатором створення «культури безпеки», де навчання персоналу та психологічна готовність до викликів є безперервним процесом, а не формальною вимогою.

Постійна адаптація стратегій захисту до нових технологічних реалій дозволяє організації випередити еволюцію загроз. У цій парадигмі лідерство трансформується у динамічну функцію, що забезпечує найвищий рівень

ISSN: 2786-9431

захищеності інформаційних активів через синергію технологій, фізичного захисту та людського потенціалу.

Значення інформаційної безпеки для сучасного бізнесу є фундаментальним, оскільки вона визначає рівень захищеності критичних даних та забезпечує безперебійність бізнес-процесів. У парадигмі сучасного менеджменту ефективна ІБ є не просто технічною функцією, а стратегічним активом, що безпосередньо формує репутацію, фінансову стабільність та рівень довіри з боку стейкхолдерів.

Будь-яка сучасна організація оперує значними масивами персональних даних клієнтів, фінансових звітів та комерційних таємниць, які є пріоритетними мішенями для кіберзлочинців. Лідер має усвідомлювати, що компрометація цих систем тягне за собою не лише прямі втрати доходів, а й значні витрати на відновлення інфраструктури, виплати компенсацій та суттєві регуляторні штрафи. Правові наслідки та судові позови від постраждалих сторін можуть стати критичним викликом для життєздатності бізнесу [15].

Репутаційний капітал виступає ще одним виміром, на який критично впливає стан ІБ. Втрата довіри є довготривалим фактором, що важко піддається відновленню у цифрову епоху, де інформація про інциденти миттєво поширюється у медіапросторі. Оскільки споживачі стають все більш обізнаними у питаннях приватності, будь-який витік даних призводить до втрати конкурентних переваг на користь тих гравців ринку, які гарантують вищий рівень захисту.

Відтак, демонстрація високих стандартів безпеки є не лише обов’язком, а й інструментом лояльності. Організації, де лідери приділяють увагу захисту конфіденційності, мають вищі шанси на встановлення довгострокових партнерських відносин, оскільки надійність ІБ мінімізує ризики для всієї екосистеми бізнесу.

ISSN: 2786-9431

Запропонована модель (див. Рис. 1) візуалізує центральну роль лідерства у координації ключових векторів захисту інформації. Психологічний, технічний та безпековий аспекти розглядаються не як ізольовані елементи, а як взаємопов'язані компоненти, що сходяться в єдину стратегію управління. Лідерство у цій системі виступає гарантом того, що технічні інструменти (тріада CIA) будуть підкріплені відповідною організаційною культурою та надійними політиками інформаційної безпеки.

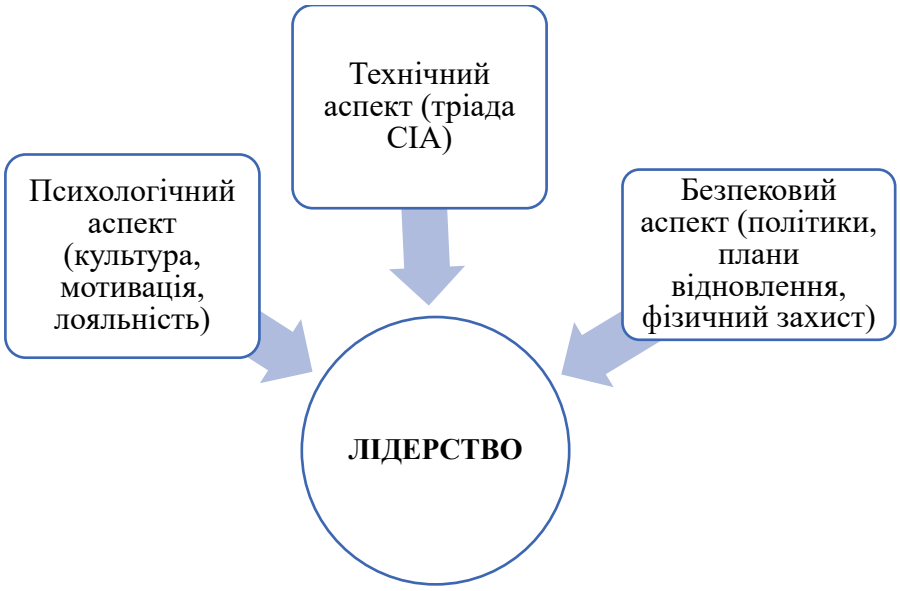

Рис. 1. Концептуальна модель лідерства як інтегруючого фактора в системі інформаційної безпеки

Джерело: розроблено авторами

У контексті глобалізації та стрімкої цифровізації фінансових ринків, забезпечення інформаційної безпеки (ІБ) трансформується у невід'ємну складову стратегічного управління. Інвестиції в ІБ слід розглядати не як витратну частину бюджету, а як стратегічний вклад у зниження операційних ризиків, підвищення ефективності бізнес-процесів та зростання загальної конкурентоспроможності установи. Окрім економічних переваг, такі інвестиції гарантують відповідність нормативним вимогам і міжнародним стандартам, що

ISSN: 2786-9431

дозволяє організації уникати штрафних санкцій та стабільно функціонувати у правовому полі.

Ефективна реалізація системи ІБ є комплексним завданням, яке вимагає від лідера синергії технічних засобів захисту та управління людським фактором. Створення «культури безпеки» через безперервне навчання персоналу дозволяє сформувати багаторівневий захист інформаційних активів, що є запорукою процвітання бізнесу в умовах агресивного цифрового середовища [1].

Важливим вектором лідерської діяльності є правове регулювання інформаційної безпеки. Сучасна стратегія захисту даних повинна базуватися на суворому дотриманні національних та міжнародних нормативно-правових актів, що регламентують зберігання, обробку та передачу інформації. Чітке виконання вимог щодо захисту персональних даних та комерційної таємниці мінімізує юридичні ризики та зміцнює репутацію організації як надійного суб'єкта ринку.

Основою системи управління інформаційною безпекою (СУІБ) у організації є чітко сформовані політики безпеки, які визначають стандарти поведінки та правила захисту активів. З позиції лідерства, ці політики є не просто бюрократичними документами, а стратегічними інструкціями, що регламентують відповідальність кожного співробітника — від рядового персоналу до топменеджменту.

Ключовими компонентами лідерського управління через політики безпеки є:

1. Планування реагування на інциденти: розробка гнучких алгоритмів дій у разі виявлення загроз. Лідер забезпечує координацію між IT-фахівцями та керівництвом для мінімізації наслідків атак і швидкого відновлення бізнес-процесів;

2. Політики контролю доступу: впровадження суворих механізмів автентифікації та авторизації (включаючи двофакторну автентифікацію та

ISSN: 2786-9431

біометрію). Це дозволяє лідеру вибудувати надійну ієрархію доступу до конфіденційної інформації;

3. Криптографічний захист (шифрування): регламентування стандартів шифрування даних під час їх зберігання та передачі. Це є критичним для захисту комерційної таємниці та фінансових записів клієнтів навіть у разі фізичного перехоплення даних зловмисниками;

4. Інтегроване управління ризиками: процеси ідентифікації та оцінки загроз, що дозволяють лідеру ефективно розподіляти ресурси організації для захисту найбільш вразливих ділянок;

Таким чином, політики безпеки трансформують стратегічне бачення лідера у конкретні операційні процедури, що забезпечують комплексну стійкість організації до сучасних викликів.

Ефективність політик безпеки критично залежить від їхньої зрозумілості та доступності для персоналу на всіх ієрархічних рівнях. З позиції лідерства, документування правил — це лише перший крок, справжнім завданням керівника є інтеграція цих норм у загальну бізнес-стратегію. Це перетворює інформаційну безпеку з «додаткового обмеження» на стратегічний пріоритет, що підтримує конкурентоспроможність організації.

Гнучкість та адаптивність СУІБ досягається через регулярне оновлення політик у відповідь на законодавчі зміни та нові технологічні виклики. Постійний контроль через аудити та моніторинг забезпечує відповідність системи стандартам, що, у свою чергу, зміцнює фундамент довіри з боку партнерів та клієнтів.

Для забезпечення життєздатності системи захисту інформації лідер має гарантувати, що політики безпеки є не лише чітко документованими, а й максимально зрозумілими для кожного співробітника. Прозорість і доступність цих регламентів є фундаментом для формування культури безпеки, де виконання правил стає усвідомленою дією на всіх ієрархічних рівнях. Окрім того, динаміка

ISSN: 2786-9431

сучасного кіберсередовища вимагає від лідера забезпечення гнучкості системи: регулярне оновлення політик у відповідь на технологічні інновації та законодавчі зміни дозволяє організації зберігати високу адаптивність до нових загроз.

Ефективність інформаційної безпеки безпосередньо залежить від її інтеграції у загальну бізнес-стратегію. Коли безпека визнається стратегічним пріоритетом, вона стає чинником конкурентоспроможності та довгострокової стійкості. Лідерська роль у цьому процесі полягає у забезпеченні безперервного контролю через регулярні аудити та моніторинг, що гарантує відповідність системи внутрішнім стандартам та зовнішнім регуляторним вимогам. Такий комплексний підхід не лише мінімізує ризики, а й зміцнює фундамент довіри з боку клієнтів та партнерів, перетворюючи безпеку на невід'ємний елемент репутаційного успіху.

Ефективність системи управління інформаційною безпекою (СУІБ) базується на чіткій вертикалі відповідальності, де кожен рівень виконує специфічну роль під егідою стратегічного лідерства. На вершині цієї структури стоїть топменеджмент, чия функція полягає не лише у затвердженні політик та виділенні ресурсів, а й в ініціюванні глибоких культурних змін, що перетворюють безпеку на спільну цінність організації.

Наступна ланка — спеціалізоване управління (зокрема офіцери CISO та IT-підрозділи), виступає транслятором стратегічних цілей у конкретні технічні рішення та механізми комплаєнсу. Завершальним, але не менш важливим елементом є виконавча ланка (рядові співробітники). Саме рівень їхньої дисципліни та дотримання встановлених правил є кінцевим індикатором успішності лідерського впливу та життєздатності всієї системи захисту.

Висновки. У результаті проведеного дослідження обґрунтовано, що в умовах глобальної цифровізації та стрімкого розвитку кіберзагроз, лідерство трансформується у провідний стратегічний ресурс управління інформаційною

 ISSN: 2786-9431

безпекою (ІБ) організації. Традиційний техноцентричний підхід, що базувався виключно на інженерно-технічних інструментах захисту, наразі є недостатнім, оскільки сучасна парадигма менеджменту вимагає від вищого керівництва інтеграції безпекових пріоритетів у загальну бізнес-стратегію через призму психологічних, кадрових та організаційних аспектів. Розроблена в межах дослідження концептуальна модель демонструє, що лідер виступає синергетичним ядром системи управління, який гармонізує технічні заходи тріади CIA, організаційні регламенти СУІБ та корпоративну культуру, перетворюючи розрізнені інструменти захисту на цілісну систему організаційної стійкості.

Особливе місце у цьому процесі належить людському фактору, який визнано найбільш критичною та уразливою ланкою в системі захисту даних. Оскільки більшість сучасних кібератак, зокрема соціальна інженерія та цільовий фішинг, спрямовані на маніпуляцію поведінкою персоналу, стратегічним завданням лідера є проектування «культури безпеки», де кожен співробітник усвідомлює власну відповідальність, володіє навичками кібергігієни та діє на засадах лояльності, що мінімізує як зовнішні загрози, так і внутрішні інсайдерські ризики. Окрім того, аналіз фінансових та правових ризиків довів існування прямого стратегічного зв'язку між станом інформаційної безпеки та репутаційним капіталом установи. Успішне управління на засадах лідерства дозволяє трансформувати витрати на ІБ у високоефективні стратегічні інвестиції, які зміцнюють довіру стейкхолдерів, мінімізують ризики правових позовів чи регуляторних штрафів та забезпечують довгострокові конкурентні переваги на ринку.

Стабільність такої системи захисту забезпечується через принципи адаптивного управління, що передбачають гнучкість внутрішніх політик безпеки та їхню відповідність динамічному правовому й технологічному середовищу. Забезпечення лідером безперервного циклу оцінки ризиків, моніторингу та

 ISSN: 2786-9431

регулярних аудитів дозволяє організації бути проактивною у протидії новим викликам цифрового простору. Підсумовуючи, можна стверджувати, що лідерство у сфері інформаційної безпеки — це здатність керівництва поєднувати високі технологічні стандарти з глибоким розумінням психології управління та етики відповідальності. Тільки такий синергетичний підхід гарантує безперебійність операційних процесів та процвітання організацій у турбулентному кіберпросторі.

Подальший науковий пошук у цьому напрямку доцільно спрямувати на розробку практичного інструментарію (опитувальників та матриць оцінки), який дозволить кількісно вимірювати рівень зрілості безпекової культури в організаціях. Окремого вивчення потребують особливості адаптивного лідерства в умовах масового впровадження інструментів штучного інтелекту та глибокої автоматизації процесів, оскільки поява генеративних нейромереж створює принципово нові психологічні чинники для соціальної інженерії та вимагає трансформації класичних моделей управління людьми.

Список використаних джерел:

1. Архіпова Є. О. Інформаційна безпека: понятійно-методологічний аспект. *Наукові вісті КПІ*. 2016. URL: https://ktpu.kpi.ua/... (дата звернення: 11.04.2026).

2. Бурячок В. Л., Грищук Р. В., Хорошко В. О. Політика інформаційної безпеки : підручник / за заг. ред. В. О. Хорошка. Київ : ПВП «Задруга», 2014. 222 с.

3. Гавкалова Н. Л., Марченко В. О. Проблема лідерства в сучасному менеджменті. *Економіка та суспільство.* 2024. Вип. 63. URL: economyandsociety.in.ua. (дата звернення: 10.04.2026).

4. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки : монографія / за заг. ред. Ю. Г. Даника. Житомир : ЖНАЕУ, 2016. 636 с.

 ISSN: 2786-9431

5. Домарєв В. В., Домарєв Д. В., Гордієнко С. Б. Обґрунтування основних функцій системи управління інформаційною безпекою. *Вісник Державного університету інформаційно-комунікаційних технологій.* 2012. № 10(2). С. 102–104.

6. Домарєв В. В., Климчук Р. В. Безпека інформаційних технологій. Методологія створення систем захисту : монографія. Київ, 2013. 688 с.

7. Завацька Н. Є. Психологічна безпека особистості в сучасному інформаційному просторі. *Технології розвитку інтелекту*. 2022. Т. 6, № 3 (32). URL: psytir.org.ua.

8. Заросило В. О. Інформаційна безпека: сучасні ризики та загрози. *Юридичний бюлетень*. 2022. URL: https://lbku.krok.edu.ua/... (дата звернення: 12.04.2026).

9. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

10. Зоря П. С., Шафранова К. В., Дивинська Ю. А. Теорія лідерства: конспект лекцій. Житомир : ЖУУ, 2025. 148 с.

11. Карамушка Л. М. Психологія управління : підручник. Київ : Фірма «ІНКОС», 2003. 344 с.

12. Можаєв М. О., Можаєв О. О., Гнусов Ю. В. Інтегрована модель управління ризиками інформаційної безпеки в системах критичного застосування. *Сучасний стан наукових досліджень та технологій в промисловості*. 2023. № 1 (23). С. 45–54.

13. Потій О. В., Ленков С. В. Політика інформаційної безпеки в умовах цифрової трансформації. *Політичні студії.* 2024. № 4. С. 92–105.

14. Bass B. M., Avolio B. J. *Improving organizational effectiveness through transformational leadership*. Thousand Oaks : Sage Publications, 1994. 238 p.

 ISSN: 2786-9431

15. Edmondson A. C. The Fearless Organization: Creating Psychological Safety in the Workplace for Learning, Innovation, and Growth. Hoboken : John Wiley & Sons, 2018. 256 p.

16. Honey T. M. An Investigation into Information Security Culture : Executive Doctor of Business Administration Diss. Miami Gardens : St. Thomas University, 2021. 145 p.

ISSN: 2786-9431