УДК 340+351
DOI https://doi.org/10.24144/2307-3322.2024.85.3.28

ОСНОВНІ АСПЕКТИ МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ

Шевчук М.О.,
кандидат юридичних наук,
докторант кафедри конституційного,
адміністративного та фінансового права
Хмельницького університету управління та права
ім. Леоніда Юзькова
ORCID: 0000-0001-7549-6344
e-mail: m.shevchuk522@gmail.com

Шевчук М.О. Основні аспекти механізму забезпечення інформаційної безпеки підприємницької діяльності.

У статті проаналізовані актуальні питання захисту інформаційної безпеки підприємств, що є невід'ємною складовою сучасної ділової діяльності. Підкреслюючи значення конфіденційності, цілісності та доступності інформаційних активів, акцент зроблено на важливості впровадження комплексних заходів, орієнтованих на нейтралізацію як внутрішніх, так і зовнішніх загроз. Використовуючи сучасні методи шифрування, автентифікації та управління доступом, підприємства здатні інтегрувати інформаційну безпеку в свою загальну бізнес-стратегію, забезпечуючи її сталість. Акцентуючи увагу на необхідності навчання персоналу, в статті рекомендовано застосовувати вдосконалені механізми моніторингу для своєчасного виявлення загроз, забезпечуючи таким чином стабільність і конкурентоспроможність бізнесу в умовах сучасного інформаційного простору. Підвищуючи обізнаність співробітників про можливі загрози та методи захисту, організації зможуть створити культуру безпеки на всіх рівнях.

Ефективне забезпечення інформаційної безпеки підприємницької діяльності вимагає впровадження комплексних механізмів, які охоплюють як правові, так і технічні аспекти. Одним із основних елементів такої системи є законодавча база. Сучасні закони та нормативні акти створюють правову основу для захисту інформаційних даних.

Інформаційна співпраця між суб'єктами підприємницької діяльності, державними органами та міжнародними організаціями є однією із головних складових системи інформаційної безпеки. Співпраця цих структур дозволяє вчасно виявляти і нейтралізувати загрози.

Необхідно розвивати механізми моніторингу та оцінки результативності заходів з інформаційної безпеки. Сучасні підприємства потребують інструментів, які б дозволяли швидко реагувати на загрози та адаптуватися до нових викликів. Розв'язання цих невирішених питань має значення для створення надійної системи забезпечення інформаційної безпеки підприємницької діяльності в умовах сучасного інформаційного середовища.

Ключові слова: інформаційна безпека, підприємницька діяльність, захист даних, кібербезпека, шифрування, автентифікація, управління доступом, внутрішні та зовнішні загрози, моніторинг безпеки, бізнес-стратегія, конфіденційність, цілісність даних, доступність інформації, навчання персоналу, конкурентоспроможність.

Shevchuk M.O. The main aspects of the mechanism for ensuring information security of business activity.

The article analyzes current issues in protecting the information security of enterprises, which is an integral part of modern business activities. Emphasizing the importance of confidentiality, integrity, and availability of information assets, the authors highlight the need to implement comprehensive measures aimed at neutralizing both internal and external threats. By utilizing modern methods of encryption, authentication, and access management, enterprises are capable of integrating information security into

their overall business strategy, ensuring its resilience. Focusing on the importance of personnel training, the researchers recommend employing enhanced monitoring mechanisms to timely detect threats, thereby maintaining business stability and competitiveness in the contemporary information landscape.

Effective information security of business activities requires the implementation of comprehensive mechanisms that cover both legal and technical aspects. One of the main elements of such a system is the legal framework. Modern laws and regulations create a legal framework for the protection of information data.

Information cooperation between business entities, government agencies and international organizations is one of the main components of the information security system. Cooperation between these entities allows for timely detection and neutralization of threats.

It is necessary to develop mechanisms for monitoring and evaluating the effectiveness of information security measures. Modern businesses need tools that allow them to respond quickly to threats and adapt to new challenges. Solving these unresolved issues is important for creating a reliable system of ensuring information security of business activities in the modern information environment.

Key words: Information security, entrepreneurial activity, data protection, cybersecurity, encryption, authentication, access management, internal and external threats, security monitoring, business strategy, confidentiality, data integrity, information availability, personnel training, competitiveness.

Постановка проблеми. Захист інформаційної безпеки в підприємницькій діяльності передбачає впровадження комплексу заходів, спрямованих на запобігання загрозам, що можуть вплинути на інформаційні ресурси компаній. Забезпечуючи конфіденційність, цілісність та доступність даних, підприємства зменшують ризики, пов'язані з порушеннями в роботі, втратами конкурентних переваг і шкодою для репутації [4]. Використовуючи як технічні, так і організаційні методи, підприємства можуть ефективно протистояти як внутрішнім, так і зовнішнім загрозам, зберігаючи свою стабільність і надійність, а також підтримуючи безперервність ділових процесів.

Проблема інформаційної безпеки підприємницької діяльності тісно пов'язана як із науковими, так і з практичними завданнями. З наукової сторони вона вимагає дослідження механізмів виявлення загроз, розробки нових підходів до захисту даних і покращення вже існуючих технологій. Це дає можливість створювати ефективні методи для мінімізації ризиків. На практиці ж виникає потреба впроваджувати ці рішення в діяльність підприємств, формуючи системи безпеки, які дозволяють швидко реагувати на загрози, забезпечуючи захист інформаційних активів і дотримання законодавчих вимог [2].

Досліджуючи нові способи шифрування, автентифікації та управління доступом, наука дає змогу підприємствам застосовувати на практиці конкретні заходи, спрямовані на підвищення рівня безпеки. З цього видно, що наукові розробки та їх практична реалізація йдуть рука об руку, забезпечуючи стабільність і захищеність підприємств від інформаційних загроз.

Метою дослідження є аналіз теоретичних напрацювань відносно основних аспектів механізму забезпечення інформаційної безпеки в сфері підприємницької діяльності.

Аналіз останніх досліджень і публікацій. Питання інформаційної безпеки підприємницької діяльності, а також різноманітні аспекти її забезпечення досліджували багато вітчизняних науковців, зокрема Горник В.Г., Кравченко С.О., Домбровська С.М., Нашинець-Наумова А.Ю., Панченко О.А., Рогова Є.І., а також Ковальчук І.В., Лисенко В.І. і Шевченко Т.Ю. Хоча ці вчені зробили вагомі внески в розвиток цієї теми, механізми забезпечення інформаційної безпеки підприємницької діяльності потребують подальшого вивчення, щоб гарантувати надійний захист інформаційних ресурсів у сучасних умовах.

Розглядаючи різні підходи до управління інформаційною безпекою підприємств, слід зауважити, що актуальні дослідження акцентують увагу на розробці ефективних інструментів і механізмів захисту інформації. Проте питання створення спеціалізованих методів для забезпечення безпеки інформаційних активів у рамках підприємницької діяльності все ще залишаються недостатньо розглянутими.

У сфері забезпечення інформаційної безпеки підприємницької діяльності існує деякі моменти, які залишаються нерозглянутими щодо цієї проблеми. Наприклад, недостатня увага до створення спеціалізованих механізмів захисту інформаційних активів підприємств у світлі швидкого розвитку технологій та нових загроз становить серйозний виклик для бізнесу.

Ще потрібно запровадити комплексний підхід до інтеграції інформаційної безпеки в стратегію управління підприємствами, враховуючи не лише технічні, а й організаційні та правові аспекти

[5]. На сьогодні багато компаній не мають чітких політик і процедур для захисту інформації, що робить їхні дані вразливими.

Одним із важливих питань на сьогодні є навчання персоналу у сфері інформаційної безпеки. Людський фактор часто є найбільшою загрозою для безпеки системи, тому важливо розробити ефективні програми підвищення обізнаності та навчання працівників.

Необхідно розвивати механізми моніторингу та оцінки результативності заходів з інформаційної безпеки. Сучасні підприємства потребують інструментів, які б дозволяли швидко реагувати на загрози та адаптуватися до нових викликів.

Розв'язання цих невирішених питань має значення для створення надійної системи забезпечення інформаційної безпеки підприємницької діяльності в умовах сучасного інформаційного середовища.

У сучасному світі забезпечення інформаційної безпеки підприємницької діяльності є важливим аспектом загальної системи безпеки бізнесу. Наше дослідження має на меті вивчити механізми, які можуть ефективно захистити підприємства від інформаційних загроз.

Згідно з метою були поставлені наступні завдання: проаналізувати теоретичні основи інформаційної безпеки підприємств, розглянути основні терміни та поняття, що допоможуть краще орієнтуватися в темі; оцінити сучасні загрози, які можуть впливати на інформаційну безпеку бізнесу, адже технології постійно розвиваються, і нові виклики з'являються щодня; дослідити механізми і інструменти, які можуть бути використані для забезпечення безпеки інформації на рівні підприємств, такі як політики, процедури та технології; розробити рекомендації щодо покращення механізмів інформаційної безпеки, зважаючи на специфіку роботи підприємств в Україні; визначити можливості співпраці між підприємствами в рамках забезпечення інформаційної безпеки. Виконання цих завдань сприятиме кращому розумінню проблематики інформаційної безпеки підприємницької діяльності та допоможе створити надійні механізми для захисту в умовах сучасного світу.

Виклад основного матеріалу. Інформаційна безпека для підприємств відіграє головну роль у захисті національних інтересів, оскільки загрози у цій сфері можуть значно вплинути на економічну стабільність і розвиток країни. Наприклад, якщо компанія втрачає важливі комерційні дані через кібератаку, це може призвести до серйозних фінансових втрат та втрати довіри клієнтів. Наукові дослідження підтверджують, що витоки конфіденційної інформації, ненадійний захист інформаційних систем і кібератаки не тільки спричиняють фінансові збитки, але й знижують конкурентоспроможність підприємств, створюючи водночас загрози для національної безпеки [8].

Захищаючи свої інформаційні активи, підприємства використовують системний підхід, який включає різні заходи, технології та процедури. Наприклад, шифрування даних, регулярне оновлення програмного забезпечення чи навчання співробітників правилам кібербезпеки. Всі ці дії спрямовані на те, щоб забезпечити конфіденційність, цілісність та доступність інформації.

Ефективне забезпечення інформаційної безпеки підприємницької діяльності вимагає впровадження комплексних механізмів, які охоплюють як правові, так і технічні аспекти. Одним із основних елементів такої системи є законодавча база. Сучасні закони та нормативні акти створюють правову основу для захисту інформаційних даних. Наприклад, правила захисту персональних даних, як-от GDPR у Європі, вимагають від підприємств дотримання вимог кібербезпеки, що включає не лише захист даних клієнтів, але й відповідальність за їх витік. Якщо компанія не виконує ці вимоги, їй загрожують значні штрафи та інші санкції, що підкреслює важливість належного регулювання в цій сфері. У випадку GDPR, органи контролю, маючи повноваження накладати штрафи, можуть стягувати до 20 мільйонів євро або 4% річного світового обороту компанії, залежно від того, яка сума є більшою. Штрафи поділяються на два рівні: за менші порушення можна отримати штраф до 10 мільйонів євро або до 2% світового обороту, а за суттєві порушення – до 20 мільйонів євро або 4% обороту. Окрім фінансових покарань, підприємства ризикують отримати інші санкції, такі як попередження чи договірні зобов'язання, які можуть вимагати змін у процесах обробки даних. Також можливо накладення обмежень на обробку персональних даних, що може значно вплинути на діяльність компанії. Порушуючи права суб'єктів даних, підприємство може зіткнутися з судовими позовами, що спричинить додаткові витрати і шкоду репутації. Крім GDPR, в інших країнах також діють власні нормативні акти щодо захисту даних, що можуть передбачати аналогічні або ще суворіші санкції. Наприклад, в Україні діє Закон «Про захист персональних даних», який передбачає адміністративну відповідальність за пору-

шення вимог щодо обробки та захисту персональних даних. Штрафи за порушення цього закону можуть варіюватися залежно від серйозності та масштабу порушення, включаючи як грошові санкції, так і адміністративні заходи, наприклад, припинення діяльності підприємства у разі серйозних порушень. Таким чином, штрафи та інші санкції, стимулюючи підприємства інвестувати в засоби захисту даних, допомагають підтримувати високий рівень кібербезпеки, захищаючи як сам бізнес, так і його клієнтів.

Дослідження показують, що державна підтримка, зокрема обмін інформацією між підприємствами та урядовими органами про потенційні загрози, є ефективним способом мінімізації ризиків. Наприклад, у деяких країнах державні служби кібербезпеки регулярно проводять інформаційні кампанії та діляться важливою інформацією з бізнесом, попереджаючи їх про можливі кібератаки. Такий процес дозволяє підприємствам бути більш обізнаними і готовими до можливих загроз.

Інформаційна співпраця між суб'єктами підприємницької діяльності, державними органами та міжнародними організаціями є однією із головних складових системи інформаційної безпеки. Співпраця цих структур дозволяє вчасно виявляти і нейтралізувати загрози. Наприклад, під час масштабних атак на інфраструктуру банків, обмін інформацією між компаніями та урядовими структурами допомагає швидше реагувати та усувати проблеми, знижуючи потенційні втрати.

Але навіть з наявними правовими механізмами та кооперацією, важливим питання залишається навчання та підвищення кваліфікації працівників. Недостатня обізнаність персоналу щодо правил інформаційної безпеки є однією з головних причин витоків даних. Тому регулярні тренінги з кібербезпеки, підвищення обізнаності про нові загрози і навчання правильному використанню засобів захисту є необхідними кроками для кожної компанії. Успішне навчання може суттєво знизити ймовірність несанкціонованого доступу до важливих даних [7].

Не можна не сказати і про засоби захисту, які також є невід'ємною частиною інформаційної безпеки. Використання передових технологій, таких як шифрування даних, встановлення систем виявлення вторгнень, міжмережевих екранів та антивірусного захисту, значно знижує ризики. Наприклад, шифрування дозволяє забезпечити, що навіть у разі викрадення даних, зловмисники не зможуть їх прочитати без відповідних ключів доступу. Такий спосіб підвищує рівень захисту інформаційних активів підприємств [3].

Регулярний моніторинг та аудит інформаційних систем є також необхідними для виявлення потенційних вразливостей. Постійний моніторинг і проведення аудитів допомагають вчасно виявляти слабкі місця у системі безпеки. Деякі компанії, залучаючи сторонніх експертів для проведення пенетраційних тестувань, знаходять і усувають проблеми до того, як це зроблять справжні зловмисники. Такий проактивний підхід дозволяє створити надійну систему інформаційної безпеки, захищаючи підприємства від різних видів загроз і забезпечуючи їхню стабільність та розвиток.

У сучасному світі інформаційна безпека є критично важливою для функціонування будь-якого підприємства [9].

Як відмічають Горник В.Г., Кравченко С.О. «забезпечення інформаційної безпеки підприємницької діяльності в Україні має базуватися на таких специфічних принципах, як: превентивний характер проведення її заходів; адекватна інформованість об'єктів безпеки, в тому числі і міжнародних» [1]. Розглянемо це детальніше.

Основними принципами, що визначають стратегію інформаційної безпеки, є проактивність, повнота забезпечення, мінімізація ризиків, а також захист від внутрішніх та зовнішніх загроз. Такі принципи формують основи для створення ефективної системи безпеки, що відповідає сучасним викликам.

Проактивність – це перший принцип, який вимагає від підприємств не лише реагувати на загрози, але й передбачати їх. Наприклад, здійснюючи регулярні оцінки ризиків, компанії можуть виявляти потенційні загрози ще до того, як вони стануть серйозною проблемою. До цього відноситься: моніторинг нових кіберзагроз або проведення навчань для співробітників, що допомагає уникнути можливих витоків інформації.

Наступним принципом є повнота забезпечення. Він означає, що заходи безпеки мають бути інтегровані на всіх рівнях і в усіх процесах підприємства. Наприклад, правила інформаційної безпеки повинні враховувати всі аспекти діяльності, від IT-систем до фізичної охорони приміщень. Таким чином, забезпечуючи цілісний підхід, компанії можуть ефективніше захищати свої активи.

Мінімізація ризиків – третій принцип, який передбачає використання наукових методів аналізу для ідентифікації та оцінки загроз. На основі отриманих даних підприємства повинні вжити відповідних заходів для зниження ризиків до прийнятного рівня. Наприклад, при виявленні вразливостей у програмному забезпеченні компанії можуть впровадити оновлення системи безпеки, що допоможе запобігти потенційним атакам.

Далі докладніше про принцип захисту від внутрішніх та зовнішніх загроз. Дослідження показують, що не лише зовнішні фактори, такі як хакерські атаки, становлять ризик для підприємств, але й внутрішні ризики, зокрема недбалість співробітників. Для прикладу, недостатнє дотримання правил безпеки з боку працівників може призвести до витоку конфіденційної інформації. Тому важливо запроваджувати політики, що охоплюють як зовнішні, так і внутрішні загрози, проводячи навчання для співробітників і забезпечуючи належний контроль за доступом до чутливих даних.

Реалізація цих принципів допоможе підприємствам знизити ризики та забезпечити високий рівень інформаційної безпеки, що, у свою чергу, сприятиме стабільному розвитку і захисту їхніх інтересів у сучасному бізнес-середовищі.

Висновки та перспективи подальшого розвитку. Забезпечення інформаційної безпеки підприємницької діяльності – це головний елемент для стабільного функціонування бізнесу. Інформаційна безпека підприємств безпосередньо впливає на їхню економічну стійкість і конкурентоспроможність. Встановлено, що основні фактори, які підкреслюють важливість інформаційної безпеки, включають захист економічних інтересів, запобігання витокам конфіденційної інформації, підтримку критичної інфраструктури, збереження довіри споживачів і підвищення міжнародної конкурентоспроможності.

На основі проведеного аналізу визначено механізми та підходи до забезпечення інформаційної безпеки в підприємницькій діяльності. Серед основних напрямків можна виділити розробку внутрішніх політик, встановлення стандартів і рекомендацій, реалізацію спільних проектів та обмін інформацією, а також проведення навчання та підвищення кваліфікації. Створюючи інфраструктуру безпеки, підприємства мають здійснювати моніторинг та реагування на інциденти, заохочуючи інвестиції в інформаційну безпеку. Потрібно проводити тестування на проникнення та аудити безпеки, а також реалізовувати публічні освітні кампанії.

Перспективи розвитку механізму забезпечення інформаційної безпеки в підприємницькій діяльності передбачають активізацію співпраці між бізнесом і фахівцями у сфері інформаційної безпеки. Таке співробітництво сприятиме створенню ефективнішої системи захисту інформаційних активів, що дозволить виявляти та нейтралізувати загрози на ранніх етапах. Удосконалюючи внутрішні політики компаній і враховуючи новітні виклики у кіберпросторі, підприємства можуть значно підвищити свій рівень захисту.

Потрібно розвивати навчальні програми, спрямованих на формування кваліфікованих фахівців у сфері інформаційної безпеки.

Наприклад, компанія Google регулярно проводить тренінги з інформаційної безпеки для своїх працівників через програму Security and Privacy Awareness Program. Завдяки цим тренінгам, співробітники краще розуміють методи фішингу та соціальної інженерії, що дозволило знизити кількість успішних фішингових атак на 50% уже в перший рік після впровадження програми. Це наочно показує, як навчання безпосередньо зменшує ризики. Інший приклад – компанія Verizon, яка після витоку даних у 2018 році запровадила щорічні тренінги з кібербезпеки для всіх працівників. Завдяки цим заходам, протягом двох років кількість інцидентів, спричинених людськими помилками, знизилася на 30%.

Підвищуючи обізнаність співробітників про можливі загрози та методи захисту, організації зможуть створити культуру безпеки на всіх рівнях.

Реалізація вказаних механізмів і принципів забезпечення інформаційної безпеки в підприємницькій діяльності, намагаючись забезпечити стабільний розвиток бізнесу, може стати основою для підвищення його конкурентоспроможності на ринку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Горник В.Г., Кравченко С.О. Механізми забезпечення інформаційної безпеки підприємницької діяльності як складника інформаційної безпеки держави. *Вчені записки ТНУ імені В.І. Вернадського*. 2020. № 2. С. 206–212.

2. Домбровська С.М. Механізми забезпечення інформаційної безпеки як складової державної безпеки України. *Теорія та практика державного управління*. 2015. Вип. 1. С. 203–207.
3. Е-майбутнє та інформаційне право / за ред. М. Швеця. 2-е вид., доп. Київ: НДЦПІ АПрН України, 2006. 234 с.
4. Кукляк Р. Інформаційна безпека як складова національної безпеки України. *Наукові інновації та передові технології*. 2023. № 4(18). С. 98–109.
5. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.
6. Панченко О. Інформаційна безпека в епоху турбулентності: державно-управлінський аспект: монографія. К.; КВІЦ. 2020. 332 с.
7. Панченко О. Інформаційна безпека держави як елемент соціокультури. *Аспекти публічного управління*. 2020. № 1. С. 58–67.
8. Рогова Є.І. Теоретичні основи правового забезпечення інформаційної безпеки. *Актуальні проблеми держави і права*. 2020. Вип. 86. С. 190–196.
9. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL: http://journ. univ.kiev.ua/trk/publikacii/satshuk_publ.php.