УДК 351:336.7:340.5
DOI: https://doi.org/10.32782/2415-3583/32.38

Крамаренко І.С.
доктор економічних наук, професор,
професор кафедри менеджменту
Національний університет кораблебудування імені адмірала Макарова
ORCID: https://orcid.org/0000-0002-0417-0918

Іртищева І.О.
доктор економічних наук, професор, професор кафедри менеджменту
Національний університет кораблебудування імені адмірала Макарова
ORCID: https://orcid.org/0000-0002-7025-9857

Білоусова С.В.
доктор економічних наук, професор кафедри менеджменту
Інститут міжнародної економіки та інформаційних технологій,
Заклад вищої освіти «Міжнародний університет бізнесу і права»
ORCID: https://orcid.org/0009-0000-6875-750X

Іртищев О.С.
PhD, викладач
Заклад вищої освіти «Міжнародний університет бізнесу і права»
ORCID: https://orcid.org/0000-0002-3910-9607

Гарагуля А.В.
аспірант
Національний університет кораблебудування імені адмірала Макарова
ORCID: https://orcid.org/0000-0001-5829-2112

ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ УКРАЇНИ

В статті розкрито процес формування організаційно-управлінського механізму забезпечення інформаційної безпеки підприємницької діяльності в контексті сталого розвитку. Обґрунтовано, що формування дієвого механізму управління інформаційною безпекою підприємницької є важливим через динамічну та непередбачувану природу сучасного бізнес-середовища. Визначено, що в умовах глобалізації та цифровізації, компанії стикаються з широким спектром загроз, що варіюються від кібератак до фінансових криз, від регуляторних змін до геополітичних нестабільностей. Доведено, що ефективне управління інформаційною безпекою дозволяє бізнесу не лише захистити свої активи та забезпечити стабільність, а й забезпечує стратегічну перевагу, сприяючи адаптації до змін, оптимізації ресурсів та підвищенню конкурентоспроможності. Наголошено, що без ефективного механізму управління, бізнес може зіткнутися з фінансовими втратами, втратою репутації, юридичними санкціями та навіть загрозою банкрутства. На відміну від цього, добре структурований підхід до управління безпекою сприяє створенню стійкої, гнучкої організації, здатної не тільки вистояти перед обличчям негативних подій, але й використовувати виклики як можливості для розвитку та зростання. Здійснено аналіз наукових досліджень щодо формування організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності. Виявлено, що в дослідженнях найбільше використовується організаційно-правовий механізм, механізм забезпечення інформаційної безпеки, що в сучасних умовах господарювання не розкриває основні аспекти управління та можливості швидкої адаптації суб'єктів господарювання до нових викликів та загроз. Запропоновано організаційно-управлінський механізм забезпечення інформаційної безпеки підприємницької діяльності в контексті сталого розвитку, що є комплексною системою організаційних, управлінських, методичних та інструментальних заходів, спрямованих на ідентифікацію, аналіз та мінімізацію внутрішніх та зовнішніх ризиків, що можуть негативно вплинути на стабільність та сталий розвиток підприємства. Цей механізм включає в себе процеси встановлення цілей інформаційної безпеки, вибору стратегій і тактик їх досягнення, розробки та впровадження конкретних заходів з управління ризиками, контролю та аудиту ефективності вжитих заходів.

Ключові слова: *організаційно-управлінські механізми, управлінські системи, інформаційна безпека, підприємницька діяльність, сталий розвиток, управління організаційними трансформаціями, цифрова трансформація економіки, виклики та загрози.*

Постановка проблеми. Формування дієвого механізму управління інформаційною безпекою підприємницької є важливим через динамічну та непередбачувану природу сучасного бізнес-середовища. В умовах глобалізації та цифровізації, компанії стикаються з широким спектром загроз, що варіюються від кібератак до фінансових криз, від регуляторних змін до геополітичних нестабільностей. Ефективне управління інформаційною безпекою дозволяє бізнесу не лише захистити свої активи та забезпечити стабільність, а й забезпечує стратегічну перевагу, сприяючи адаптації до змін, оптимізації ресурсів та підвищенню конкурентоспроможності.

Управління інформаційною безпекою включає розробку політик, стратегій та процедур, що спрямовані на ідентифікацію, оцінку та мінімізацію ризиків, пов'язаних з фінансовою діяльністю та економічними операціями компанії. Це вимагає глибокого розуміння зовнішнього середовища, внутрішніх процесів, а також неперервного моніторингу та аналізу даних для своєчасного реагування на потенційні загрози.

Таким чином, важливість формування дієвого механізму управління інформаційною безпекою визначається не лише необхідністю захисту від потенційних загроз, але й потребою підтримки стабільного розвитку бізнесу, його спроможністю адаптуватися до змін та забезпечувати довгострокову конкурентоспроможність в умовах непевності та швидких змін глобального економічного ландшафту.

Аналіз останніх досліджень і публікацій. Досліджені присвячені механізмам забезпечення інформаційної безпеки підприємницької діяльності відомі серед таких науковців: Бойко Є., Горник В., Мужанова Т., Панченко В., Стегней М., Легомінова С., Чубаєвський В., Якименко Ю., та інших. Без ефективного механізму управління, бізнес може зіткнутися з фінансовими втратами, втратою репутації, юридичними санкціями та навіть загрозою банкрутства. На відміну від цього, добре структурований підхід до управління безпекою сприяє створенню стійкої, гнучкої організації, здатної не тільки вистояти перед обличчям негативних подій, але й використовувати виклики як можливості для розвитку та зростання. Саме, тому процес формування організаційно-управлінського механізму забезпечення інформаційної безпеки підприємницької діяльності є досить актуальним.

Метою написання статті є процес формування організаційно-управлінського механізму забезпечення інформаційної безпеки підприємницької діяльності в умовах цифрової трансформації економіки України.

Виклад основного матеріалу дослідження. Сучасні дослідження в Україні також значною мірою зосереджені на вирішенні актуальних проблем управління інформаційною безпекою підприємницької діяльності. Серед новітніх напрямків досліджень можна виділити розробку комплексних методологій оцінки та управління ризиками, аналіз впливу глобалізаційних процесів на інформаційну безпеку підприємств, вивчення механізмів захисту інтелектуальної власності та боротьби з економічною кіберзлочинністю.

Якименко Ю. М., Мужанова Т. М., Легомінова С. В. визначають, що "Інформаційна безпека являє собою набір інструментів і методів, використовуваних для захисту цифрової та аналогової інформації. Вона охоплює широкий спектр інформаційних технологій, які активно проникають в життя, стаючи необхідною умовою успішного функціонування все більшого числа підприємств. Забезпечення інформаційної безпеки в бізнесі слід розглядати як невід'ємний елемент процесу управління підприємством. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним підприємством, необхідно створювати ефективну систему управління інформаційною безпекою (СУІБ). Оскільки сучасні системи забезпечення інформаційної безпеки підприємства, як досить складні організаційно-технічні системи, функціонують в умовах невизначеності стану зовнішнього і внутрішнього інформаційного середовища, управління такими системами мають ґрунтуватися тільки на результатах застосуванні системного аналізу." [1, с. 37]

Погоджуємось з думкою Чубаєвського В. І., що "Інтенсивна інформатизація всіх сфер життєдіяльності суспільства нині є одним з визначальних глобальних чинників подальшого соціально-економічного, інтелектуального та духовного розвитку людства, а на рівні підприємства інформаційні ресурси розглядають як важливий самостійний елемент виробництва. Розвиток інформаційних технологій, з одного боку, суттєво полегшує процес прийняття рішень та забезпечує їх принципово нову якість (за рахунок відкритості та доступності великих масивів даних, можливості формування та запровадження управлінських систем «у режимі реального часу», використання та швидкого оброблення великих баз даних тощо), а з іншого – створює нові загрози та ризики для функціонування підприємства, рівень та інтенсивність виникнення яких зростає в геометричній прогресії". [2, с. 6].

Дійсно із посиленням ролі цифровізації у всіх сферах суспільного життя буде зростати вплив нових викликів та загроз, що призведе до нестабільності діяльності суб'єктів господарювання. Саме тому, важливим є постійний процес перегляду та формування механізму та інструментів забезпечення інформаційної безпеки підприємницької діяльності в контексті сталого розвитку.

Горник В.Г. та Кравченко С.О. в своєму дослідженні наголошують, що "Серед основних механізмів забезпечення інформаційної безпеки підприємницької діяльності в Україні як складника інформаційної безпеки держави доцільно виділити: інформаційний патронат; інформаційний захист (судовий, адміністративний, автономний); інформаційну кооперацію; формування ефективних систем захисту інформації. Сьогодні ефективне забезпечення безпеки підприємницької діяльності, як і всієї національної економіки, має бути системою заходів за такими взаємопов'язаними напрямами: захист від злочинного світу; захист від порушень закону з тим, щоб самим не потрапити під його санкції; захист від недобросовісної конкуренції; захист від протиправних дій власних співробітників" [3].

Панченко В. визначає "Організаційно-правовий механізм державної політики інформаційної безпеки є впорядкованою сукупністю органів держави, задіяних у процесі формування, забезпечення і провадження політики інформаційної безпеки, а також внутрішні та зовнішні суспільні відносини, які регулюються системою правових норм та принципів у сфері інформації. Встановлено, що загрози інформаційній безпеці поділяються на наявні та потенційно можливі явища і чинники, які можуть створити певну небезпеку інтересам людини, суспільства і держави в інформаційній сфері" [4].

Можемо узагальнити, що в економічних дослідженнях термін «механізм» найчастіше використовується для опису системи методів, принципів і засобів, що забезпечують функціонування і регулювання процесів у суспільстві. Це включає в себе способи, за допомогою яких реалізуються економічні відносини між суб'єктами господарювання, а також меха-

нізми впливу на економічну поведінку індивідів, підприємств та держави з метою досягнення певних макро- та мікроекономічних цілей. Економічний механізм охоплює правові, фінансові, податкові, кредитні та інші інструменти, що дозволяють стимулювати виробництво, розподіл і споживання товарів та послуг, а також впливати на інвестиційну активність, ціноутворення, зайнятість та інші ключові аспекти економічного життя.

"Забезпечення інформаційної безпеки підприємницької діяльності є важливою частиною загальної системи інформаційної безпеки держави. Держави і підприємства можуть взаємодіяти та співпрацювати для забезпечення ефективного захисту важливої інформації. Ось деякі механізми та підходи до забезпечення інформаційної безпеки підприємницької діяльності як складової інформаційної безпеки держави. Ці механізми спільно допомагають забезпечити інформаційну безпеку як окремих підприємств, так і держави в цілому, зменшуючи ризики кібератак і витоку конфіденційної інформації" [6, с. 31].

В сфері управління бізнесом під механізмом найчастіше розуміють сукупність методів, інструментів та процедур, що використовуються для ефективного управління ресурсами, оптимізації виробничих і комерційних процесів, забезпечення фінансової стабільності та досягнення стратегічних цілей підприємства. Це включає системи планування, бюджетування, управління витратами, ціноутворення, фінансовий аналіз, мотивацію та стимулювання персоналу, а також використання фінансових інструментів для підтримки ліквідності і інвестиційної привабливості.

Саме тому, механізм у контексті управління бізнесом орієнтований на вирішення питань оптимального розподілу та використання ресурсів, мінімізацію витрат, збільшення прибутковості та конкурентоспроможності на ринку. Він також передбачає аналіз зовнішнього середовища, адаптацію до його змін, прогнозування економічних тенденцій та формування ефективної стратегії розвитку підприємства.

Отже, здійснений аналіз організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності показав, що найбільше в дослідженнях використовується поняття "організаційно-правовий механізм", "механізм забезпечення інформаційної безпеки". Вважаємо, що в сучасних умовах господарювання використання даних понять не дозволяє в повній мірі розкрити та використати основні аспекти управління з можливістю швидкої адаптації суб'єктів господарювання до нових викликів та загроз інформаційній безпеці.

Таким чином, організаційно-управлінського механізму забезпечення інформаційної безпеки підприємницької діяльності в контексті сталого розвитку – це комплексна система організаційних, методичних та інструментальних заходів, спрямованих на ідентифікацію, аналіз та мінімізацію внутрішніх та зовнішніх ризиків, що можуть негативно вплинути на стабільність та сталий розвиток підприємства. Цей механізм включає в себе процеси встановлення цілей інформаційної безпеки, вибору стратегій і тактик їх досягнення, розробки та впровадження конкретних заходів з управління ризиками, контролю та аудиту ефективності вжитих заходів.

Рис. 1. Організаційно-управлінський механізм забезпечення інформаційної безпеки підприємницької діяльності в контексті сталого розвитку

Джерело: запропоновано авторами

Основною метою такого механізму є забезпечення умов для збереження та ефективного використання ресурсів підприємства, захисту його активів і капіталу від потенційних загроз, забезпечення стійкого фінансового стану, а також створення передумов для сталого розвитку бізнесу. Механізм управління фінансово-економічною безпекою бізнесу передбачає систематичний моніторинг зовнішнього і внутрішнього середовища, виявлення нових можливостей та загроз, а також адаптацію стратегій і дій підприємства з метою оптимізації його фінансових і економічних показників.

Організаційні складові заходи механізму управління інформаційною безпекою бізнесу включають структурну побудову, процеси та процедури, які забезпечують ефективну реалізацію стратегій і політик безпеки на підприємстві. Ці заходи охоплюють:

1. Створення відповідальних структурних підрозділів – формування відділів або служб безпеки, які координують діяльність у сфері захисту активів, інформації, персоналу та інших ресурсів компанії.

2. Розробка політик і процедур безпеки – формулювання чітких правил і норм, що регулюють питання фінансово-економічної безпеки, включаючи заходи протидії шахрайству, корупції, порушенню корпоративної етики.

3. Планування і реалізація заходів з ризик-менеджменту – ідентифікація, аналіз і оцінка ризиків, розробка стратегій мінімізації або уникнення негативних наслідків.

4. Організація системи внутрішнього контролю та аудиту – створення ефективної системи моніторингу за фінансовими та господарськими операціями, перевірка відповідності діяльності підприємства встановленим процедурам і стандартам.

5. Навчання та розвиток персоналу – проведення тренінгів і семінарів для підвищення обізнаності та компетенцій співробітників у питаннях фінансово-економічної безпеки.

6. Забезпечення інформаційної безпеки – впровадження технологічних та програмних засобів для захисту даних, систем управління і комунікацій від несанкціонованого доступу, витоку інформації, втрати даних.

7. Розвиток корпоративної культури – формування у співробітників відповідального ставлення до збереження корпоративних цінностей, активів, забезпечення лояльності та високого рівня корпоративної дисципліни.

Ці заходи дозволяють підприємству створити ефективну, гнучку і відповідну до сучасних викликів систему управління фінансово-економічною безпекою. Організаційні складові механізму управління інформаційною безпекою бізнесу створюють основу для сталого розвитку підприємства, забезпечуючи його стійкість до зовнішніх та внутрішніх загроз.

Щодо системи методичного забезпечення механізму інформаційної безпеки бізнесу, то різні автори виділяють різні методи. Ковальчук А. М. в системі фінансово-економічної безпеки вирізняє методи стимулювання, регулювання, аналізу та прогнозування [8].

Методичне забезпечення організаційно-управлінського механізму забезпечення інформаційної безпеки підприємницької діяльності в контексті сталого розвитку, на нашу думку, має охоплювати аналіз ринків, планування, моніторинг та контроль, внутрішній аудит, фінансове моделювання, корпоративне управління, інформаційно-комунікаційні технології

Методи управління інформаційною безпекою бізнесу включають комплекс заходів та інструментів, що дозволяють підприємству ідентифікувати, оцінювати, мінімізувати та контролювати ризики, пов'язані з його фінансовою та економічною діяльністю. Ці методи сприяють створенню ефективної системи управління, яка захищає активи компанії, підтримує її стабільність та сприяє зростанню:

1. Аналіз ризиків – систематичне виявлення та оцінювання потенційних загроз, що можуть негативно вплинути на діяльність підприємства. Це можуть бути фінансові, ринкові, операційні, правові, технологічні ризики тощо.

2. Планування – розробка стратегій і тактик управління ризиками, включаючи запобігання ризикам, їх мінімізацію або передачу (наприклад, через страхування). Планування включає розробку планів дій на випадок реалізації ризиків.

3. Моніторинг та контроль – регулярне спостереження за станом фінансово-економічної безпеки підприємства, перевірка ефективності заходів управління ризиками та внесення необхідних коректив у стратегії управління.

4. Внутрішній аудит – незалежна оцінка внутрішніх контрольних процесів, систем управління ризиками та корпоративного управління з метою їх удосконалення.

5. Фінансове моделювання – створення математичних моделей для прогнозування фінансових результатів діяльності підприємства в різних умовах, що дозволяє оцінити потенційні ризики та виробити стратегії їх мінімізації.

6. Корпоративне управління – впровадження принципів та практик корпоративного управління, спрямованих на забезпечення прозорості, відповідальності та чесності у веденні бізнесу.

7. Інформаційно-комунікаційні технології – використання сучасних ІКТ для захисту інформації, оптимізації бізнес-процесів та підвищення загальної ефективності управління фінансово-економічною безпекою.

Застосування цих методів дозволяє підприємству адаптуватися до змін у зовнішньому та внутрішньому середовищі, ефективно реагувати на виклики, забезпечувати стале зростання та зміцнювати свої конкурентні переваги.

Важливим в процесі формування організаційно-управлінського механізму є інформаційне забезпечення процесу прийняття управлінських рішень. Колектив авторів наголошує, що "це базовий елемент на всіх етапах процесу прийняття управлінських рішень, що виражається в ідентифікації та наданні різноманітних кількісних та якісних показників інформації про внутрішнє та зовнішнє середовище функціонування підприємства відповідно до потреб суб'єкта управління. Інформаційне забезпечення процесу прийняття рішень охоплює надходження, рух, обробку, зберігання та передачу масиву інформації в рамках визначених управлінських цілей та завдань, вивчення управлінської проблеми, розгляду варіантів

її вирішення, прийняття та доведення управлінського рішення до виконавців, контролю виконання управлінського рішення.” [10, с. 5]

Щодо інструментів механізму інформаційної безпеки бізнесу, то вони є взаємодоповнюючим до методів елементом механізму, оскільки важко провести чітке розмежування між методами та інструментами у даному випадку. Такий взаємозв’язок та взаємодоповнення відслідковується і у працях інших дослідників [8].

На нашу думку, найважливішими інструментами є страхування, хеджування, фінансовий аналіз, інформаційні технології, корпоративне управління, ризик-менеджмент, навчання та розвиток персоналу. В цілому, інструменти механізму управління фінансово-економічною безпекою бізнесу включають комплекс застосувань, методів та засобів, які дозволяють підприємству захистити свої активи, забезпечити стабільність і сприяти зростанню в умовах зовнішніх і внутрішніх загроз. Основні інструменти охоплюють:

1. Страхування – використання страхових продуктів для захисту від фінансових втрат, спричинених ризиками, такими як пожежі, крадіжки, природні катастрофи та інші непередбачувані події.

2. Хеджування – застосування фінансових інструментів, таких як ф’ючерсні та опціонні контракти, для захисту від змін цін на сировину, валютні коливання та інші ринкові ризики.

3. Фінансовий аналіз – регулярний огляд фінансової звітності для виявлення слабких місць в операційній та фінансовій діяльності, оцінка ліквідності, рентабельності та інших ключових показників ефективності.

4. Інформаційні технології – впровадження сучасних ІТ-рішень для захисту інформації, оптимізації управління та підвищення загальної ефективності діяльності.

5. Корпоративне управління – реалізація принципів прозорості, відповідальності та справедливості у веденні бізнесу, що сприяє зміцненню довіри з боку інвесторів, партнерів та клієнтів.

6. Комплаєнс – дотримання законодавчих та регуляторних вимог, включаючи фінансове регулювання, закони про працю, захист даних тощо.

7. Ризик-менеджмент – систематичний підхід до ідентифікації, аналізу, оцінки та контролю ризиків з метою мінімізації потенційних втрат.

8. Навчання та розвиток персоналу – інвестиції в підвищення кваліфікації та розвиток навичок співробітників для підвищення їх обізнаності та здатності виявляти та реагувати на ризики.

Ці інструменти є частиною комплексної стратегії, спрямованої на захист бізнесу від потенційних загроз та на підтримку його стабільного розвитку та конкурентоспроможності.

Інструменти і методи використовуються для досягнення цілей інформаційної безпеки бізнесу, які зосереджені на забезпеченні стабільності та захисті від різних зовнішніх та внутрішніх загроз, які можуть негативно вплинути на фінансове становище та економічну діяльність підприємства. Для досягнення цих цілей використовуються різноманітні стратегії та тактики, які адаптовані під специфіку та потреби конкретного бізнесу.

Цілі інформаційної безпеки: захист активів (забезпечення фізичного та юридичного захисту майна, фінансових ресурсів та інтелектуальної власності від крадіжки, шахрайства, вандалізму тощо), забезпечення ліквідності (підтримка достатнього рівня готівкових коштів та ліквідних активів для забезпечення поточних зобов’язань), мінімізація ризиків (ідентифікація, аналіз та заходи щодо зниження фінансових, операційних, ринкових, правових та інших ризиків), забезпечення прибутковості та дотримання законодавства (планування та виконання дій для забезпечення стабільного зростання доходів та максимізації прибутку й забезпечення відповідності усіх аспектів діяльності підприємства чинному законодавству та регуляторним вимогам).

Вибір стратегій і тактик охоплює стратегії ризик-менеджменту (включає ідентифікацію потенційних ризиків, оцінку їх впливу та розробку планів дій для їх мінімізації або усунення), фінансове планування та аналіз (спрямовані на оцінку фінансового стану підприємства, прогнозування майбутніх потреб у ресурсах та розробку бюджетів), інвестиційну стратегію (має на меті забезпечення оптимального розподілу капіталу між різними активами для досягнення максимальної віддачі при прийнятному рівні ризику), стратегію диверсифікації (передбачає розширення асортименту продукції або послуг, вихід на нові ринки для зниження залежності від одного джерела доходу), кібербезпеку та захист даних (розробка та впровадження заходів для захисту інформаційних систем від несанкціонованого доступу, втрати даних або інших кіберзагроз), корпоративну культуру та навчання (формування серед працівників свідомості про важливість фінансово-економічної безпеки, розвиток навичок та знань у цій сфері).

Реалізація цих стратегій та тактик дозволяє підприємству не лише протистояти поточним викликам, але й адаптуватися до мінливих умов глобального економічного середовища, забезпечуючи стійке зростання та розвиток.

Кінцева мета механізму інформаційної безпеки бізнесу полягає у забезпеченні стійкого розвитку та довгострокового виживання підприємства шляхом мінімізації ризиків і захисту від потенційних загроз. Це включає створення умов для ефективного управління активами, капіталом, інформацією та іншими ресурсами з метою підтримки конкурентоспроможності, оптимізації прибутковості та збереження репутації компанії на ринку.

Забезпечення інформаційної безпеки вимагає від підприємства не тільки реактивних заходів у відповідь на вже виниклі загрози, але й превентивних стратегій, спрямованих на передбачення та запобігання потенційним проблемам. Це охоплює широкий спектр дій, від фінансового моніторингу та контролю до кібербезпеки, правової підтримки та корпоративної культури.

Таким чином, кінцева мета механізму інформаційної безпеки полягає у створенні сильної, гнучкої та адаптивної організації, здатної ефективно протистояти зовнішнім і внутрішнім викликам, забезпечуючи при цьому зростання та процвітання в довгостроковій перспективі.

Висновки. Проведено аналіз організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності. Виявлено, що в дослідженнях найбільше використовується організаційно-правовий механізм, механізм забезпечення інформаційної безпеки, що в сучасних умовах господарювання не розкриває основні аспекти управління та можливості швидкої адаптації суб'єктів господарювання до нових викликів та загроз.

Запропоновано організаційно-управлінський механізм забезпечення інформаційної безпеки підприємницької діяльності в контексті сталого розвитку, що є комплексною системою організаційних, управлінських, методичних та інструментальних заходів, спрямованих на ідентифікацію, аналіз та мінімізацію внутрішніх та зовнішніх ризиків, що можуть негативно вплинути на стабільність та сталий розвиток підприємства. Цей механізм включає в себе процеси встановлення цілей інформаційної безпеки, вибору стратегій і тактик їх досягнення, розробки та впровадження конкретних заходів з управління ризиками, контролю та аудиту ефективності вжитих заходів.

Список використаних джерел:

1. Якименко Ю. М., Мужанова Т. М., Легомінова С. В. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії fireeye. *Кібербезпека: освіта, наука, техніка*. 2021. № 4 (12). С. 36–50. DOI: https://doi.org/10.28925/2663-4023.2021.12.3650

2. Чубаєвський В. І. Корпоративна інформаційна безпека: монографія. Київ: Держ. торг.-екон. ун-т, 2022. 272 с.

3. Горник В. Г., Кравченко С. О. Механізми забезпечення інформаційної безпеки підприємницької діяльності як складника інформаційної безпеки держави. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління.* 2020. Том 31 (70). No 2. С. 206–211.

4. Панченко В. Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти. *Актуальні проблеми правознавства.* 2020. № 1 (21). С. 103–109.

5. Крамаренко І. С., Ляшенко В. М., Антоненко А. А. Впровадження HR-технологій управління персоналом для захисту інформаційного простору та зміцнення економічної безпеки підприємств. *Актуальні проблеми інноваційної економіки та права.* 2024. № 1. С. 117–121. DOI: https://doi.org/10.36887/2524-0455-2024-1-24

6. Васільєва Л. М., Іжболдін М. М. Механізми та підходи щодо забезпечення інформаційної безпеки підприємницької діяльності як елемента інформаційної безпеки держави. *Публічне управління і адміністрування в Україні.* 2023. Вип. 36. С. 28–32. DOI: https://doi.org/10.32782/pma2663-5240-2023.36.5

7. Крамаренко І. С., Надточій І. І., Гришина Н. В. HR-Технології в управлінні персоналом як складова фінансово-економічної безпеки підприємств в умовах цифрової трансформації. *Herald of Khmelnytskyi National University. Economic sciences.* 2024. Том 326. № 1. С. 222–226. DOI: https://doi.org/10.31891/2307-5740-2024-326-36

8. Ковальчук А. М. Фінансово-економічна безпека підприємства в контексті адаптації до викликів цифрового середовища. *Економічний вісник.* 2020. № 3. С. 152–159. DOI: https://doi.org/10.33271/ebdut/71.152

9. Крамаренко І. С., Надточій І. І., Гришина Н. В. Тактичне управління персоналом у системі економічної безпеки суб'єктів е-комерції. *Вчені записки ТНУ імені В. І. Вернадського.* 2024. Том 35 (74). № 1. С. 48–54. DOI: https://doi.org/10.32782/2523-4803/74-1-8

10. Правдюк А. Л., Прутська Т. Ю., Правдюк М. В. Інформаційне забезпечення управління підприємницькою діяльністю на засадах інституціоналізму: монографія. Київ: Центр учбової літератури», 2019. 360 с.

11. Надточій І., Крамаренко І., Гришина Н. Ризик-менеджмент як інструмент управління фінансово-економічною безпекою суб'єктів є-бізнесу в умовах цифрової економіки та суспільства. *Via Economica.* 2024. Вип. 4. С. 212–218. DOI: https://doi.org/10.32782/2786-8559/2024-4-30

References:

1. Yakymenko Yu.M., Muzhanova T.M., Legominova, S. V. (2021). «System analysis of technical systems for ensuring information security of enterprises from the fireeye company». *Kiberbezpeka: osvita, nauka, tekhnika*, no 4 (12), pp. 36–50. DOI: https://doi.org/10.28925/2663-4023.2021.12.3650

2. Chubaevsky, V. I. (2022). Korporatyvna informatsijna bezpeka. [Corporate information security]. Derzh. torh.-ekon. un-t. Kyiv. Ukraine.

3. Gornyk, V. G., and Kravchenko, S. O. (2020). «Mechanisms for ensuring information security of business activity as a component of information security of the state». *Vcheni zapysky TNU imeni V.I. Vernads'koho. Seriia: Derzhavne upravlinnia,* vol. 31 (70), no 2. pp. 206–211.

4. Panchenko, V. (2020). «Management of information security of the state and enterprises: legal and organizational aspects». *Aktual'ni problemy pravoznavstva,* no 1 (21), pp. 103–109.

5. Kramarenko, I. S., Lyashenko, V. M., and Antonenko, A. A. (2024). «Implementation of HR-technologies of personnel management to protect the information space and strengthen the economic security of enterprises». *Aktual'ni problemy innovatsijnoi ekonomiky ta prava,* no 1, pp. 117–121. DOI: https://doi.org/10.36887/2524-0455-2024-1-24

6. Vasilieva, L. M., and Izhboldin, M. M. (2023). «Mechanisms and approaches to ensure information security of business activity as an element of information security of the state». *Publichne upravlinnia i administruvannia v Ukraini,* vol. 36, pp. 28–32. DOI: https://doi.org/10.32782/pma2663-5240-2023.36.5

7. Kramarenko, I. S., Nadtochii, I. I., and Hryshina, N. V. (2024). «NR-Technologies in personnel management as a component of the financial and economic security of enterprises in the conditions of digital transformation». *Herald of Khmelnytskyi National University. Economic sciences,* vol. 326. no 1, pp. 222–226. DOI: https://doi.org/10.31891/2307-5740-2024-326-36

8. Kovalchuk, A. M. (2020). «Financial and economic security of the enterprise in the context of adaptation to the challenges of the digital environment». *Ekonomichnyj visnyk,* no 3, pp. 152–159. DOI: https://doi.org/10.33271/ebdut/71.152

9. Kramarenko, I. S., Nadtochii, I. I., and Hryshina, N. V. (2024). «Tactical personnel management in the system of economic security of e-commerce entities». *Vcheni zapysky TNU imeni V. I. Vernads'koho,* vol. 35 (74), no 1, pp. 48–54. DOI: https://doi.org/10.32782/2523-4803/74-1-8

10. Pravdyuk. A. L., Prutska. T. Yu., and Pravdyuk. M. V. (2019). Informatsijne zabezpechennia upravlinnia pidpryiemnyts'koiu diial'nistiu na zasadakh instytutsionalizmu [Information support for business management on the basis of institutionalism]. Tsentr uchbovoi literatury. Kyiv. Ukraine.

11. Nadtochii, I., Kramarenko, I., and Hryshina, N. (2024). «Risk management as a tool for managing the financial and economic security of e-business subjects in the conditions of the digital economy and society», *Via Economica,* vol. 4, pp. 212–218. DOI: https://doi.org/10.32782/2786-8559/2024-4-30

Kramarenko Iryna, Irtyshcheva Inna
Admiral Makarov National University of Shipbuilding

Bilousova Svitlana
Institute of International Economics and Information Technologies, Higher Education Institution "International University of Business and Law"

Irtyshchev Oleksandr
Higher Education Institution "International University of Business and Law"

Harahulia Arthur
Admiral Makarov National University of Shipbuilding

ORGANIZATIONAL AND MANAGEMENT MECHANISMS FOR ENSURING INFORMATION SECURITY OF BUSINESS ACTIVITIES IN THE CONDITIONS OF DIGITAL TRANSFORMATION OF THE ECONOMY OF UKRAINE

The article describes the process of forming an organizational and management mechanism for ensuring information security of business activity in the context of sustainable development. It is substantiated that the formation of an effective mechanism for managing business information security is important due to the dynamic and unpredictable nature of the modern business environment. It was determined that in the conditions of globalization and digitalization, companies face a wide range of threats, ranging from cyber attacks to financial crises, from regulatory changes to geopolitical instabilities. It has been proven that effective information security management allows a business not only to protect its assets and ensure stability, but also provides a strategic advantage by facilitating adaptation to changes, optimizing resources and increasing competitiveness. It is emphasized that without an effective management mechanism, a business may face financial losses, loss of reputation, legal sanctions and even the threat of bankruptcy. In contrast, a well-structured approach to security management helps create a resilient, flexible organization that can not only withstand adverse events, but also use challenges as opportunities for development and growth. The analysis of scientific research on the formation of organizational and management mechanisms for ensuring the information security of business activities was carried out. It was found that the organizational and legal mechanism, the mechanism for ensuring information security, is the most used in research, which in modern economic conditions does not reveal the main aspects of management and the possibility of rapid adaptation of economic entities to new challenges and threats. An organizational and management mechanism for ensuring the information security of business activity in the context of sustainable development is proposed, which is a complex system of organizational, managerial, methodological and instrumental measures aimed at identifying, analyzing and minimizing internal and external risks that may negatively affect the stability and sustainable development of the enterprise. This mechanism includes the processes of setting information security goals, choosing strategies and tactics for achieving them, developing and implementing specific risk management measures, control and auditing of the effectiveness of the measures taken.

Keywords: *organizational and management mechanisms, management systems, information security, entrepreneurial activity, sustainable development, management of organizational transformations, digital transformation of the economy, challenges and threats.*

JEL classification: M29, Q01