МЕХАНІЗМИ ТА ПІДХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ ЯК ЕЛЕМЕНТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

MECHANISMS AND APPROACHES TO ENSURE INFORMATION SECURITY OF BUSINESS ACTIVITY AS AN ELEMENT OF STATE INFORMATION SECURITY

УДК 340:351
DOI https://doi.org/10.32782/pma2663-5240-2023.36.5

Васільєва Л.М.
д. наук з держ. упр., професор, професор кафедри обліку, оподаткування та управління фінансово-економічною безпекою
Дніпровський державний аграрно-економічний університет

Іжболдін М.М.
магістр управління фінансово-економічною безпекою
Дніпровський державний аграрно-економічний університет

У статті досліджено та узагальнено наукові уявлень щодо механізмів та підходів до забезпечення інформаційної безпеки підприємницької діяльності як елемента інформаційної безпеки держави. Зазначено, що забезпечення інформаційної безпеки підприємницької діяльності є надзвичайно важливою складовою загальної системи інформаційної безпеки держави. Інформаційна безпека підприємств впливає на економічну стійкість та конкурентоспроможність країни, а також на загальний стан її інформаційної інфраструктури та кібербезпеки. Визначено основні причини, чому інформаційна безпека підприємницької діяльності є важливою для держави: захист економічних інтересів; запобігання витокам конфіденційної інформації; підтримка критичної інфраструктури; збереження довіри споживачів; забезпечення національної безпеки; міжнародна конкурентоспроможність. Наголошено, що забезпечення інформаційної безпеки підприємницької діяльності - це процес застосування різних заходів, політик, технологій та практик з метою забезпечення конфіденційності, цілісності та доступності інформації, а також захисту від інших загроз та ризиків. Встановлено, що забезпечення інформаційної безпеки підприємницької діяльності вимагає дотримання таких принципів: проактивність; повне забезпечення; мінімізація ризиків; визначення відповідальності; захист від внутрішніх і загальних загроз; постійна оцінка і покращення; свідомість та навчання; співпраця і обмін інформацією; суворе дотримання законодавства. Визначено механізми та підходи до забезпечення інформаційної безпеки підприємницької діяльності як складової інформаційної безпеки держави: законодавча база; стандарти і рекомендації; спільні проекти та обмін інформацією; навчання і освіта; створення інфраструктури безпеки; моніторинг та відгук на інциденти; співробітництво з міжнародними організаціями; заохочення до інвестицій в інформаційну безпеку; тестування на проникнення та аудит безпеки; публічні освітні кампанії.

Ключові слова: *інформація, інформаційна безпека, державна інформаційна політика, загрози інформаційній безпеці, механізми, підприємницької діяльності.*

The article examines and summarizes scientific ideas about the mechanisms and approaches to ensuring information security of business activity as an element of state information security. It is noted that ensuring the information security of business activities is an extremely important component of the general information security system of the state. Information security of enterprises affects the economic stability and competitiveness of the country, as well as the general state of its information infrastructure and cyber security. The main reasons why information security of business activity is important for the state are identified: protection of economic interests; prevention of leaks of confidential information; support of critical infrastructure; maintaining consumer trust; ensuring national security; international competitiveness. It is emphasized that ensuring information security of business activity is a process of applying various measures, policies, technologies and practices to ensure confidentiality, integrity and availability of information, as well as protection from other threats and risks. It was established that ensuring the information security of entrepreneurial activity requires compliance with the following principles: proactivity; full support; risk minimization; definition of responsibility; protection against internal and general threats; constant evaluation and improvement; consciousness and learning; cooperation and exchange of information; strict compliance with the law. The mechanisms and approaches to ensuring the information security of business activities as a component of the information security of the state are defined: the legislative framework; standards and recommendations; joint projects and information exchange; training and education; creation of security infrastructure; monitoring and response to incidents; cooperation with international organizations; encouragement of investments in information security; penetration testing and security auditing; public education campaigns.

Key words: *information, information security, state information policy, threats to information security, mechanisms, entrepreneurial activity.*

Постановка проблеми. Забезпечення інформаційної безпеки підприємницької діяльності є важливою частиною загальної системи інформаційної безпеки держави. Інформаційна безпека характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих, деструктивних, що уражають державні інтереси і таке інше) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи. Інформаційна безпека підприємства визначається комплексом заходів, політик і процедур, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, а також на захист від інших ризиків, які можуть впливати на інформаційні

активи та операції підприємства. Держави і підприємства можуть взаємодіяти та співпрацювати для забезпечення ефективної захисту важливої інформації.

Аналіз останніх досліджень і публікацій. Проблематику інформаційної безпеки як склад національної безпеки, а також різноманітні аспекти щодо забезпечення інформаційної безпеки підприємницької діяльності як елемента інформаційної безпеки держави розглядали в своїх працях вітчизняні вчені, насамперед, Горник В.Г., Кравченко С.О., Домбровська С.М., Нашинець-Наумова А.Ю., Панченко О.А., Рогова Є.І. та інші. Проте, незважаючи на вагомі напрацювання вчених, питання щодо механізмів забезпечення інформаційної безпеки підприємницької діяльності в системі інформаційної безпеки держави вимагають подальшого вивчення.

Формулювання цілей дослідження – дослідження та узагальнення наукових уявлень щодо механізмів та підходів до забезпечення інформаційної безпеки підприємницької діяльності як елемента інформаційної безпеки держави.

Виклад основного матеріалу. У загальному розумінні, інформаційна безпека означає захист інформації від ризиків, загроз, а також забезпечення її конфіденційності, цілісності і доступності. Іншими словами, це набір заходів і стратегій, спрямованих на забезпечення безпеки інформаційних активів, що можуть бути даними, системами, програмами або будь-якими іншими компонентами інформаційних технологій. Інформаційна безпека є важливою для будь-якого суб'єкта, який має інформаційні активи, включаючи як підприємства, так і держави. Ця безпека допомагає запобігати фінансовим збиткам, порушенню конфіденційності та захищати національні та економічні інтереси.

Підтримуємо думку про те, що «задоволення в будь-якій мірі потреб в інформації призводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави» [3].

Забезпечення інформаційної безпеки підприємницької діяльності є надзвичайно важливою складовою загальної системи інформаційної безпеки держави. Інформаційна безпека підприємств впливає на економічну стійкість та конкурентоспроможність країни, а також на загальний стан її інформаційної інфраструктури та кібербезпеки.

Основні причини, чому інформаційна безпека підприємницької діяльності є важливою для держави, включають:

1. Захист економічних інтересів: Успішна підприємницька діяльність впливає на економічний розвиток держави. Захист від кіберзагроз та інших інцидентів, що можуть завдати фінансових збитків підприємствам, є важливим для забезпечення стабільності економіки країни.

2. Запобігання витокам конфіденційної інформації [1]: Підприємства можуть мати доступ до конфіденційної інформації, такої як технологічні розробки, інтелектуальна власність та клієнтські дані. Захист цієї інформації є критичним для убезпечення національних інтересів.

3. Підтримка критичної інфраструктури: Багато підприємств забезпечують критичну інфраструктуру, таку як енергетичні системи, телекомунікаційні мережі та транспорт. Захист цих систем є важливим для безперебійності функціонування держави.

4. Збереження довіри споживачів: Інформаційні витоки та кібератаки можуть пошкодити репутацію підприємств та викликати втрату довіри споживачів. Захист інформаційної безпеки допомагає зберігати довіру споживачів і інвесторів.

5. Забезпечення національної безпеки: Деякі підприємства можуть бути ключовими для національної безпеки країни, наприклад, у виробництві важливої військової техніки або комунікаційних систем для правоохоронних органів. Захист їхньої інформаційної безпеки має критичне значення для держави.

6. Міжнародна конкурентоспроможність [5]: Країни з високим рівнем інформаційної безпеки мають перевагу в міжнародному бізнесі. Підприємства можуть приваблювати інвесторів і клієнтів, якщо демонструють надійний захист інформації.

З цих причин держави вкладають значні зусилля в розробку і впровадження стратегій та політик інформаційної безпеки, а також у співпрацю з підприємствами для забезпечення належного рівня захисту інформації. Все це сприяє створенню ефективної системи інформаційної безпеки на національному рівні.

Інформаційна безпека підприємства визначається комплексом заходів, політик і процедур, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, а також на захист від інших ризиків, які можуть впливати на інформаційні активи та операції підприємства [7]. Забезпечення інформаційної безпеки підприємницької діяльності - це процес застосування різних заходів, політик, технологій та практик з метою забезпечення конфіденційності, цілісності та доступності інформації, а також захисту від інших загроз та ризиків. Цей процес є важливим для збере-

ження репутації, фінансової стійкості та конкурентоспроможності підприємства. Нижче подані ключові кроки та підходи до забезпечення інформаційної безпеки в підприємницькій діяльності:

- Оцінка ризиків. Проведення оцінки ризиків допомагає ідентифікувати потенційні загрози та визначити, як вони можуть вплинути на підприємство. Це включає в себе аналіз зовнішніх і внутрішніх загроз, таких як кібератаки, втрати даних, невірна поведінка співробітників тощо.

- Розробка політики інформаційної безпеки. Розробка політики, яка визначає правила і стандарти для збереження інформаційної безпеки на підприємстві. Політика повинна включати в себе вимоги до паролів, правила роботи з конфіденційною інформацією, правила доступу до мереж і систем тощо.

- Захист інформаційної інфраструктури. Захист мереж, серверів, комп'ютерів і інших технічних ресурсів від несанкціонованого доступу та кібератак. Включає в себе встановлення вогнепровідних стін, антивірусного програмного забезпечення, систем виявлення вторгнень і регулярне оновлення програм і патчів.

- Захист даних. Забезпечення конфіденційності та цілісності даних. Це включає в себе шифрування даних, створення резервних копій даних, контроль доступу до конфіденційної інформації та інші заходи.

- Аудит і моніторинг [9]. Регулярний аудит і моніторинг інформаційної безпеки для виявлення вразливостей та аномалій. Це допомагає вчасно реагувати на потенційні загрози.

- Навчання і свідомість персоналу: Навчання співробітників з питань інформаційної безпеки та підвищення їх свідомості щодо правил безпеки та їх відповідальності.

- Відповідь на інциденти [6]. Розробка планів відповіді на інциденти та тренування персоналу щодо їх виконання. Це допомагає ефективно реагувати на порушення безпеки і відновлювати нормальну роботу після інциденту.

- Співпраця з іншими суб'єктами. Взаємодія з іншими підприємствами, державними органами та правоохоронними службами для обміну інформацією про загрози та інциденти.

- Законодавство і регулювання: Дотримання відповідного законодавства і нормативів щодо інформаційної безпеки.

- Збереження репутації [4]. Важливий аспект, який включає в себе публічну інформацію та відносини з клієнтами, постачальниками і партнерами.

- Відновлення після інцидентів. Розробка планів відновлення та контингенції в разі інцидентів або втрати доступу до інформації.

- Соціальний чинник. Врахування людського фактору, так як багато загроз пов'язані з соціальним інжинірингом та невідомими діями працівників.

Забезпечення інформаційної безпеки підприємницької діяльності вимагає дотримання таких принципів [8]: проактивність: підприємство повинно передбачати можливі загрози та ризики і приймати заходи для їх попередження, замість чекання, поки вони стануть критичними проблемами; повне забезпечення: інформаційна безпека повинна бути вбудована в усі аспекти діяльності підприємства, включаючи технічні, організаційні та кадрові аспекти; мінімізація ризиків: підприємство повинно визначити і оцінити потенційні загрози та ризики і приймати заходи для їх зниження до прийнятного рівня; визначення відповідальності: ясне визначення відповідальності за інформаційну безпеку на всіх рівнях організації. кожен працівник повинен розуміти свої обов'язки щодо захисту інформації; захист від внутрішніх і загальних загроз: націлювання заходів захисту не лише на зовнішні загрози (наприклад, хакерські атаки), але і на внутрішні фактори ризику, такі як недбале ставлення персоналу до безпеки; постійна оцінка і покращення: постійна моніторинг та оцінка ефективності заходів інформаційної безпеки і внесення змін для поліпшення системи захисту; свідомість та навчання: навчання персоналу щодо загроз та правил безпеки, а також підвищення їх свідомості; співпраця і обмін інформацією: співпраця з іншими підприємствами, органами та групами, які можуть сприяти обміну інформацією про загрози та інциденти безпеки; суворе дотримання законодавства: Дотримання всіх відповідних законів і нормативів щодо інформаційної безпеки. Ці принципи сприяють створенню системи інформаційної безпеки, яка є надійною, ефективною і відповідає потребам і можливостям підприємства. Забезпечення інформаційної безпеки вимагає постійної уваги та дії на всіх рівнях організації.

Забезпечення інформаційної безпеки – це сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства і держави в інформації [2]. Забезпечення інформаційної безпеки підприємницької діяльності є важливою частиною загальної системи інформаційної безпеки держави. Держави і підприємства можуть взаємодіяти та співпрацювати для забезпечення ефективної захисту важливої інформації. Ось деякі механізми та підходи до забезпечення інформаційної безпеки підприємницької діяльності як складової інформаційної безпеки держави (рис. 1).

Рис. 1. 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.

Таким чином, забезпечення інформаційної безпеки підприємницької діяльності є важливим елементом загальної інформаційної безпеки держави, оскільки підприємства є основними джерелами економічної активності та важливими частинами національної інфраструктури.

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]. Ми погоджуємося з даною тезою і відповідно виникає потреба розробки конкретних механізмів реалізації зазначених принципів, що зумовлює перспективи подальших досліджень у цьому напрямі.

Висновки. 1. Зазначено, що забезпечення інформаційної безпеки підприємницької діяльності є надзвичайно важливою складовою загальної системи інформаційної безпеки держави. Інформаційна безпека підприємств впливає на економічну стійкість та конкурентоспроможність країни, а також на загальний стан її інформаційної інфраструктури та кібербезпеки. Визначено основні причини, чому інформаційна безпека підприємницької діяльності є важливою для держави: захист економічних інтересів; запобігання витокам конфіденційної інформації; підтримка критичної інфраструктури; збереження довіри споживачів; забезпечення національної безпеки; міжнародна конкурентоспроможність.

2. Визначено механізми та підходи до забезпечення інформаційної безпеки підприємницької діяльності як складової інформаційної безпеки держави: законодавча база; стандарти і рекомендації; спільні проекти та обмін інформацією; навчання і освіта; створення інфраструктури безпеки; моніторинг та відгук на інциденти; співробітництво з міжнародними організаціями; заохочення до інвестицій в інформаційну безпеку; тестування на проникнення та аудит безпеки; публічні освітні кампанії.

ЛІТЕРАТУРА:

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. 206-2012.

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 безпекиURL: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.