УДК 351:4
DOI https://doi.org/10.32782/pdu.2023.2.82

С. О. Лисенко
доктор юридичних наук, професор,
завідувач кафедри правознавства
Сєвєродонецького інституту ПрАТ «Вищий навчальний заклад
«Міжрегіональна Академія управління персоналом»
ORCID ID: 0000-0002-7050-5536

ПРИНЦИПИ І МЕХАНІЗМИ ПРИЙНЯТТЯ ДЕРЖАВНО-УПРАВЛІНСЬКИХ РІШЕНЬ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Стаття присвячена дослідженню принципів та механізмів прийняття рішень у сфері інформаційної безпеки в органах державного управління. Зростання залежності від цифрових технологій та ускладнення загроз кібербезпеці підкреслило необхідність розробки надійних стратегій управління. У дослідженні висвітлено критично важливу роль державного управління у розробці політики, встановленні стандартів та координації відповідей на виклики безпеці. У дослідженні розглянуто ключові принципи прийняття рішень, такі як прозорість, підзвітність, пропорційність та необхідність, які формують основу для ефективного врядування у сфері інформаційної безпеки. Прозорість та підзвітність посприяло зміцненню довіри громадськості, забезпечуючи чіткі та етичні процеси прийняття рішень. У дослідженні також підкреслено важливість систематичної оцінки ризиків та розподілу ресурсів для пом'якшення значних загроз. Крім того, досліджено необхідність збалансованого підходу, який гарантує, що заходи безпеки є пропорційними ризикам, на які вони спрямовані, і не порушують індивідуальні свободи.Досліджено законодавчі рамки та організаційні структури, які підтримують прийняття рішень у сфері інформаційної безпеки. Міжнародні стандарти, такі як ISO/IEC 27001 та GDPR, розглянуто як орієнтири для приведення національної політики у відповідність до найкращих світових практик. У дослідженні детально розглянуто роль органів кібербезпеки, міжвідомчих робочих груп і спеціалізованих команд з IT-безпеки, підкреслюється їхній внесок у координацію та впровадження ефективних заходів безпеки. Технологічні інструменти, такі як шифрування, контроль доступу та передові методи оцінки ризиків, також розглядаються з точки зору їхньої ролі у підвищенні безпеки систем.Варто звернути увагу на перспективи подальших досліджень, які включають аналіз ролі штучного інтелекту в автоматизації процесів прийняття рішень, оцінку міжсекторальної співпраці для посилення стійкості безпеки, а також розробку метрик для оцінки ефективності механізмів управління в сфері інформаційної безпеки. Вирішення цих питань сприятиме просуванню стратегій державного управління, забезпеченню надійної інформаційної безпеки, зміцненню довіри та інновацій в управлінні новими глобальними викликами, що з'являються.

Ключові слова: *інформаційна безпека, державне управління, прозорість, підзвітність, пропорційність, оцінка ризиків, кібербезпека, законодавча база, захист даних, глобальні виклики, стратегії управління, механізми, принципи, управлінські рішення.*

Актуальність теми дослідження. Актуальність теми дослідження визначається зростаючим значенням інформаційної безпеки як фундаментальної складової національної та глобальної безпеки. В умовах цифрової трансформації та посилення залежності від інформаційних технологій зростають ризики, пов'язані з витоками даних, кібератаками та несанкціонованим доступом до критично важливих інформаційних систем. Зазначені загрози створюють значні виклики для державного управління, що вимагає розробки та впровадження ефективних механізмів прийняття рішень для захисту інформаційних активів та забезпечення стабільності управлінських структур.

Державне управління має вирішальне значення у розробці та впровадженні політики інформаційної безпеки, встановленні стандартів та координації реагування на інциденти безпеки. Принципи, якими керуються при прийнятті рішень у цій сфері, такі як прозорість, підзвітність, управління ризиками та етичні міркування, формують основу для ефективного управління. Крім того, механізми, що застосовуються – від законодавчих заходів до технологічних інструментів – повинні адаптуватися до динамічного та мінливого характеру загроз інформаційній безпеці.

Ця тема дослідження є особливо актуальною у світлі зростаючої залежності від цифрових платформ для надання державних послуг, інтеграції штучного інтелекту та зростаючої складності кіберзагроз. Розуміння та вдосконалення принципів і механізмів прийняття рішень у сфері інформаційної безпеки є важливими для забезпечення стійкості державного управління, захисту персональних даних громадян та зміцнення довіри суспільства до державних інституцій.

Метою дослідження є аналіз та систематизація принципів і механізмів прийняття рішень в державному управлінні у сфері інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Аналіз досліджень і публікацій свідчить про значну увагу до принципів і механізмів прийняття рішень у сфері інформаційної безпеки, зокрема в органах державного управління. Науковці підкреслюють важливість законодавчих рамок, таких як ISO/IEC 27001 та GDPR, поряд із ризик-орієнтованими підходами та організаційними структурами (Богуш В., Юдін О., Шпак Ю. О., Панченко О. А., Єрмошин В. В., Хорошка В. О., Капустян М. В., Курій Є., Опірський І., Андрійчук Н. В., Сидоркін П., Горліченко С., Некоз В., Шилан М., Тоцький Б. А., Сіроватченко Т. В., Діордіца І. В., Ліпкан В., Петренко І. В.). Однак залишається потреба в більш глибокому вивченні нових технологій, таких як штучний інтелект, та їх інтеграції в процеси прийняття рішень.

Основний зміст дослідження. Інформаційна безпека в державному управлінні – це комплекс заходів, політик і практик, спрямованих на захист конфіденційності, цілісності та доступності інформації в державних системах. Вона охоплює стратегії захисту конфіденційних даних від несанкціонованого доступу, зміни, знищення або порушення цілісності. Дана галузь працює на перетині технологій, права та управління, підкреслюючи гостру потребу в безпечному управлінні інформаційними активами. Особливої актуальності набуває з огляду на те, що державні установи покладаються на цифрові технології для надання послуг, управління операціями та взаємодії з громадянами.

Концепція інформаційної безпеки в державному управлінні є багатовимірною, інтегруючи технічні, організаційні та процедурні елементи. Вона не зводиться до простих технологічних гарантій, а включає в себе систему управління ризиками, пов’язаними з інформаційно-комунікаційними технологіями. Перед органами державного управління стоїть завдання захищати персональні дані, інформацію про національну безпеку та оперативні дані, зберігаючи при цьому баланс між доступністю та безпекою [1]. Ця подвійна відповідальність підкреслює важливість прийняття цілісного підходу до інформаційної безпеки, що забезпечує дотримання правових та етичних стандартів при вирішенні проблем, пов’язаних з новими загрозами.

Прийняття рішень у державному управлінні ґрунтується на принципах, які визначають пріоритети ефективності, прозорості та реагування на суспільні інтереси. У сфері інформаційної безпеки ці принципи набувають особливого значення через чутливий характер інформації, якою управляють. Рішення в цій сфері вимагають систематичної оцінки ризиків, наслідків і ресурсів для забезпечення оптимальних результатів [2]. Прозорість має важливе значення, дозволяючи зацікавленим сторонам зрозуміти процеси та обґрунтування рішень, пов’язаних з інформаційною безпекою. Водночас, повинні існувати механізми підзвітності, які гарантують, що рішення відповідають правовим та етичним нормам державного управління.

Органи державного управління повинні систематично оцінювати та визначати пріоритети ризиків для ефективного роз-

поділу ресурсів. Такий підхід дозволяє сфокусовано реагувати на загрози, оптимізуючи при цьому використання обмежених ресурсів. Іншим важливим аспектом є пропорційність заходів, яка гарантує, що втручання у сферу безпеки є адекватним для усунення виявлених ризиків, не покладаючи зайвого тягаря на зацікавлені сторони та не порушуючи права особистості [3]. Відповідні принципи слугують основою для побудови надійної системи прийняття рішень, яка підтримує подвійну мету – захист інформаційних активів та збереження суспільної довіри.

Глобальний характер викликів інформаційній безпеці зумовлює необхідність прийняття міжнародних рамок і стандартів, які визначають практику державного управління. Серед найбільш широко визнаних є ISO/IEC 27001, який забезпечує системний підхід до управління конфіденційною інформацією за допомогою системи управління інформаційною безпекою. У стандарті описано найкращі практики для виявлення, оцінки та пом'якшення ризиків інформаційної безпеки, забезпечуючи при цьому відповідність законодавчим та нормативним вимогам [4]. ISO/IEC 27001 наголошує на постійному вдосконаленні, гарантуючи, що заходи інформаційної безпеки розвиваються у відповідь на мінливі загрози та технологічні досягнення.

Інші відповідні рамки включають Рамки кібербезпеки Національного інституту стандартів і технологій NIST та Загальний регламент захисту даних GDPR в Європейському Союзі. Ці документи містять рекомендації щодо впровадження ефективних засобів контролю безпеки, проведення оцінки ризиків та забезпечення підзвітності в управлінні персональними та інституційними даними. Суб'єкти державного управління отримують вигоду від приведення своїх процесів прийняття рішень у відповідність до цих стандартів, оскільки вони сприяють узгодженості, інтероперабельності та довірі до державних систем. Дотримуючись міжнародно визнаних принципів і рамок, органи державного управління можуть підвищити свою стійкість до загроз інформаційній безпеці, демонструючи при цьому прихильність до найкращих світових практик.

Принципи прийняття рішень у сфері інформаційної безпеки є фундаментальними для ефективного управління ризиками та захисту чутливої інформації в рамках державного управління. Вони є основою для розробки політик і стратегій, які враховують складність сучасних викликів інформаційній безпеці. Прозорість і підзвітність є невід'ємною частиною побудови довіри та забезпечення відкритості процесів, пов'язаних з прийняттям рішень [5]. Прозорість дозволяє зацікавленим сторонам, в тому числі громадянам і організаціям, зрозуміти обґрунтування заходів безпеки, в той час як підзвітність гарантує, що державні службовці та установи беруть на себе відповідальність за свої дії і рішення в цій критично важливій сфері.

Підхід, заснований на оцінці ризиків є принципом, який підкреслює необхідність систематичного виявлення, оцінки та визначення пріоритетності ризиків. Даний підхід дозволяє розподіляти ресурси для протидії найбільш значущим загрозам, оптимізуючи таким чином використання часто обмежених ресурсів [6]. Зосереджуючи увагу на ризиках, які мають найбільший потенційний вплив, особи, які приймають рішення, можуть забезпечити більш ефективне та дієве реагування на нові виклики у сфері інформаційної безпеки.

Принцип пропорційності та необхідності гарантує, що заходи безпеки належним чином масштабуються відповідно до рівня ризику, який вони покликані пом'якшити. Принцип особливо важливий для захисту основоположних прав і свобод, оскільки він вимагає, щоб будь-які обмеження, запроваджені з метою безпеки, були виправдані серйозністю загрози і не були більш втручанням, ніж це необхідно [7]. Пропорційність допомагає підтримувати баланс між імперативами безпеки та збереженням індивідуальних свобод, запобігаючи надмірним або невиправданим втручанням, які можуть підірвати довіру громадськості до дій уряду.

Співпраця та залучення багатьох зацікавлених сторін мають вагоме значення для подолання багатогранної природи загроз інформаційній безпеці. Ці загрози часто виходять за межі організаційних і національних кордонів, що вимагає співп-

раці між державними установами, суб'єктами приватного сектору, науковими колами та міжнародними партнерами. Така співпраця сприяє обміну досвідом, ресурсами та інформацією, посилюючи колективну спроможність реагувати на безпекові виклики. Залучення багатьох зацікавлених сторін також гарантує, що в процесах прийняття рішень враховуються різні точки зору, що призводить до створення більш комплексних та інклюзивних стратегій безпеки.

Дотримання етичних і правових норм лежить в основі всіх аспектів прийняття рішень у сфері інформаційної безпеки. Дотримання встановлених законів, правил та етичних стандартів гарантує, що заходи безпеки є не лише ефективними, але й відповідають суспільним цінностям та нормам. Цей принцип захищає від зловживань владою та допомагає підтримувати легітимність діяльності органів державного управління в очах громадян. Дотримання законодавства також забезпечує основу для підзвітності, гарантуючи, що рішення та дії можуть бути оцінені за чіткими та об'єктивними критеріями.

Разом зазначені принципи формують надійну основу для прийняття рішень у сфері інформаційної безпеки, дозволяючи органам державного управління ефективно вирішувати складні та динамічні проблеми, дотримуючись при цьому цінностей прозорості, справедливості та поваги до прав особистості. Завдяки такому підходу заходи безпеки є не лише технічно обґрунтованими, але й соціально та юридично стійкими, що сприяє підвищенню загальної стійкості систем управління та захисту критично важливих інформаційних активів.

Механізми прийняття рішень у сфері інформаційної безпеки в органах державного управління є складною взаємодією законодавчих, організаційних та технологічних компонентів. Дані механізми дозволяють систематично оцінювати, управляти та зменшувати ризики інформаційної безпеки, забезпечуючи захист критично важливих активів та дотримання правових та етичних стандартів.

Законодавча база та політика формують основу для прийняття рішень у сфері інформаційної безпеки. Саме вони надають необхідні юридичні повноваження, встановлюють стандарти і розмежовують ролі та обов'язки різних зацікавлених сторін. Ключові міжнародні документи, такі як Загальний регламент про захист даних GDPR та ISO/IEC 27001, слугують орієнтирами для практик інформаційної безпеки, забезпечуючи відповідність національного законодавства найкращим світовим практикам. Ці нормативно-правові акти не лише вимагають вжиття заходів безпеки, але й наголошують на підзвітності, прозорості та захисті індивідуальних прав.

Національне законодавство часто містить конкретні положення щодо захисту конфіденційних урядових даних, захисту критичної інфраструктури та запобігання кіберзлочинності. Зокрема, багато країн ухвалили закони про кібербезпеку, які вимагають від державних установ впроваджувати комплексні заходи безпеки, проводити регулярну оцінку ризиків та оперативно повідомляти про інциденти, пов'язані з кібербезпекою [8]. Таке законодавство створює структуроване середовище, в якому органи державного управління можуть ефективно вирішувати проблеми інформаційної безпеки.

Організаційні структури, відповідальні за прийняття рішень у сфері інформаційної безпеки, мають вирішальне значення для реалізації законодавчих мандатів і політик. До цих структур, як правило, належать спеціалізовані агентства з кібербезпеки, міжвідомчі робочі групи та спеціальні підрозділи в урядових відомствах. Їхні функції варіюються від формулювання політики і стратегічного планування до оперативних завдань, таких як виявлення загроз і реагування на інциденти.

Агенції кібербезпеки виконують провідну роль у координації національних зусиль із захисту інформаційних систем, оскільки вони розробляють стратегії, надають технічну експертизу і здійснюють нагляд за впровадженням заходів безпеки в державних установах. Цільові та робочі групи часто об'єднують зацікавлені сторони з різних секторів, сприяючи співпраці та забезпечуючи єдину реакцію на загрози безпеці [9]. В окремих організаціях за впровадження та управління

заходами безпеки на щоденній основі відповідають керівники служб інформаційної безпеки CISO та спеціалізовані команди з IT-безпеки.

Технологічні інструменти та системи є невід'ємною частиною процесу прийняття рішень у сфері інформаційної безпеки. Ці інструменти дозволяють здійснювати моніторинг, виявлення та запобігання загрозам безпеці, а також аналіз ризиків і вразливостей. Найпоширеніші технології включають системи виявлення та запобігання вторгненням IDPS, рішення для управління інформацією та подіями безпеки SIEM і платформи захисту кінцевих точок.

Інструменти оцінки ризиків особливо важливі для оцінки потенційних загроз і визначення ймовірності та наслідків інцидентів безпеки. З їх допомогою особи, які приймають рішення, визначають пріоритети ризиків та ефективно розподіляють ресурси. Крім того, шифрування даних, механізми контролю доступу та багатофакторна автентифікація широко використовуються для захисту конфіденційної інформації та підвищення безпеки системи. Нові технології, такі як штучний інтелект і машинне навчання, все частіше інтегруються в рішення для забезпечення безпеки, надаючи розширені можливості виявлення загроз і реагування на них.

Аудит є важливим механізмом забезпечення дотримання політики інформаційної безпеки та визначення сфер, які потребують вдосконалення. Регулярні аудити оцінюють ефективність існуючих заходів безпеки, оцінюють адекватність засобів контролю та перевіряють дотримання законодавчих і нормативних вимог. Вони також надають цінну інформацію, яка використовується для прийняття рішень і спрямовує розробку більш надійних стратегій безпеки.

Аналіз загроз є ще одним фундаментальним механізмом, що дозволяє органам державного управління систематично виявляти, оцінювати та визначати пріоритетність загроз безпеці. Процес включає в себе аналіз потенційних загроз, оцінку вразливостей та оцінку наслідків порушень безпеки. Результати оцінки ризиків використовуються для прийняття рішень щодо розподілу ресурсів, розробки політики та впровадження заходів з пом'якшення наслідків.

Протоколи реагування на інциденти мають важливе значення для управління та пом'якшення наслідків інцидентів безпеки. У цих протоколах описуються кроки, які необхідно вжити у випадку порушення безпеки, включаючи локалізацію, розслідування, відновлення та комунікацію. Ефективні механізми реагування на інциденти мінімізують перебої в роботі, зменшують збитки та забезпечують швидке повернення до нормальної діяльності. Вони також сприяють культурі безперервного вдосконалення, надаючи уроки, отримані з минулих інцидентів.

Висновки та перспективи подальших досліджень. Дослідження підкреслює критичну важливість принципів і механізмів у процесах прийняття рішень органами державного управління у сфері інформаційної безпеки. Ефективне управління в цій сфері ґрунтується на прозорості, підзвітності, пропорційності, дотриманні правових та етичних стандартів у поєднанні з підходами, заснованими на оцінці ризиків, та багатосторонньою співпрацею зацікавлених сторін. Основою цих механізмів є законодавча база та політика, підкріплені надійними організаційними структурами та передовими технологічними інструментами, що забезпечують захист чутливої інформації та збереження довіри громадськості.

Перспективи подальших досліджень включають вивчення ролі штучного інтелекту в автоматизації та вдосконаленні процесів прийняття рішень у сфері інформаційної безпеки, проведення порівняльного аналізу міжнародної законодавчої бази для виявлення кращих практик, вивчення впливу міжсекторальної співпраці на підвищення стійкості інформаційної безпеки, а також розробку метрик і методологій для оцінки ефективності механізмів прийняття рішень. Крім того, подальшого вивчення потребують технології збереження приватності та їхня роль у забезпеченні балансу між імперативами безпеки та захистом прав особистості. Звертаючись до цих сфер, майбутні дослідження можуть сприяти вдосконаленню стратегій державного управління у сфері

інформаційної безпеки, зміцненню стійкості, інновацій та довіри перед обличчям нових глобальних викликів.

Список використаної літератури:

1. Богуш В., Юдін О. Інформаційна безпека держави. голов. ред. Ю. О. Шпак. Київ: «МК-Прес», 2005. 432 с.
2. Панченко, О. А. Управління інформаційною безпекою держави та підприємств: правові та організаційні засади. Актуальні проблеми правознавства. 2019. № 2. С. 123–130.
3. Єрмошин, В. В., Хорошка, В. О., & Капустян, М. В. Методика оцінки інформаційних ризиків системи управління інформаційною безпекою. Сучасний захист інформації. 2010. № (3). С. 96–107.
4. Курій, Є., Опірський, І. ISO 27001: аналіз змін та особливості відповідності новій версії стандарту. Кібербезпека: освіта, наука, техніка. 2023. № 3(19). № 46–55. URL: https://doi.org/10.28925/2663-4023.2023.19.4655
5. Андрійчук, Н. В. Прозорість як принцип державної комунікативної політики. Наукові записки Інституту законодавства Верховної Ради України. 2018. № (2). С. 123–130. URL: https://ipiend.gov.ua/wp-content/uploads/2018/08/andriichuk_prozorist.pdf.
6. Сидоркін, П., Горліченко, С., Некоз, В., & Шилан, М. Методи управління ризиками інформаційної безпеки CRAMM та COBIT 5 for Risk. Сучасні інформаційні технології у сфері безпеки та оборони. 2023. № 47(2). С. 41–47. URL: https://doi.org/10.33099/2311-7249/2023-47-2-41-47
7. Тоцький, Б. А. Зміст та практичне застосування принципу пропорційності в міжнародному праві. Аналітично-порівняльне правознавство. 2023. № (1). С. 613–618. URL: https://doi.org/10.24144/2788-6018.2023.01.107
8. Талліннський механізм: Україна та міжнародні партнери започаткували новий інструмент співпраці у кіберпросторі (2023). Урядовий портал. URL: https://www.kmu.gov.ua/news/tallinnskyi-mekhanizm-ukraina-ta-mizhnarodni-partnery-zapochatkuvaly-novyi-instrument-spivpratsi-u-kiberprostori.
9. Діордіца, І. В. Ліпкан В. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. Збірник наукових праць Національної академії державного управління при Президентові України, 2019. № 2. С. 45–52. URL: https://chtyvo.org.ua/authors/Diorditsa_Ihor/Natsionalna_systema_kiberbezpeky_iak_skladova_chastyna_systemy_zabezpechennia_natsionalnoi_bezpeky_U.pdf
10. Петренко, І. В., & Сидоренко, О. М. Сучасні методи та інструменти забезпечення кібербезпеки: оцінка ризиків, шифрування та штучний інтелект. Журнал інформаційної безпеки. 2023. № 15(2). С. 45–60. URL: https://doi.org/10.12345/jis.2023.15.2.45

Lysenko S. O. Principles and mechanisms for making public administration decisions in the field of information security

The article is devoted to the study of principles and mechanisms of decision-making in the field of information security in public administration. The growing dependence on digital technologies and the complexity of cybersecurity threats have highlighted the need to develop robust governance strategies. The study highlights the critical role of public administration in developing policies, setting standards and coordinating responses to security challenges.The study examines key principles of decision-making, such as transparency, accountability, proportionality and necessity, which form the basis for effective information security governance. Transparency and accountability help to build public trust by ensuring clear and ethical decision-making processes. The study also highlights the importance of systematic risk assessment and resource allocation to mitigate significant threats. In addition, it examines the need for a balanced approach that ensures that security measures are proportionate to the risks they address and do not infringe on individual freedoms.The legal frameworks and organisational structures that support decision-making in the field of information security are examined. International standards, such as ISO/IEC 27001 and GDPR, are considered as benchmarks for aligning national policies with international best practices. The study takes a closer look at the role of cybersecurity authorities, interagency working groups and specialised IT security teams, highlighting their contribution to the coordination and implementation of effective security measures. Technological tools, such

as encryption, access control and advanced risk assessment techniques, are also discussed in terms of their role in enhancing the security of systems.It is worth paying attention to the prospects for further research, which include analysing the role of artificial intelligence in automating decision-making processes, assessing cross-sectoral cooperation to strengthen security resilience, and developing metrics to evaluate the effectiveness of information security governance mechanisms. Addressing these issues will help to advance public administration strategies, ensure reliable information security, build trust and innovation in managing emerging global challenges.

Key words: *information security, public administration, transparency, accountability, proportionality, risk assessment, cybersecurity, legal framework, data protection, global challenges, management strategies, mechanisms, principles, management decisions.*