УДК 004.056.8
DOI https://doi.org/10.32782/2663-5941/2024.6.2/28

Прокопович-Ткаченко Д.І.
Університет митної справи та фінансів

Саричев В.І.
Університет митної справи та фінансів

Звєрєв В.П.
Державний торговельно-економічний університет

Бушков В.Г.
Державний торговельно-економічний університет

Хрушков Б.С.
Університет митної справи та фінансів

МОДЕЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ ЯК СКЛАДНОЇ ТЕХНОГЕННОЇ СИСТЕМИ: СТРАТЕГІЧНИЙ ПІДХІД ДО УПРАВЛІННЯ РИЗИКАМИ

У статті розглянуто проблеми забезпечення інформаційної безпеки держави, яка є складною техногенною системою, що поєднує технічні, організаційні, інформаційні та людські компоненти, функціонуючи в умовах динамічного середовища та ризиків високих рівнів. Представлено системний підхід до моделювання інформаційної безпеки, який враховує її складну структуру, динамічність, адаптивність та багатофакторність. Розроблено концептуальну модель, що відображає основні ризики та шляхи їх мінімізації за допомогою стратегічного планування та управління. Модель базується на принципах системної динаміки, інтегрованого аналізу ризиків та адаптивного управління, що забезпечує її ефективність у сучасних умовах.

Особливу увагу приділено впливу людського фактору на функціонування системи інформаційної безпеки та необхідності врахування його ролі у досягненні кінцевих результатів. Запропоновані підходи спрямовані на оптимізацію управлінських процесів у різних сферах соціального та економічного життя, забезпечення надійності та стійкості системи, а також її здатності до адаптації відносно змін зовнішнього середовища. Використання розробленої моделі дозволяє державним установам та організаціям, бізнес-структурам зокрема вдосконалювати процеси прийняття рішень у сфері інформаційної безпеки, знижувати ризики та підвищувати ефективність заходів безпеки.

Провідними науковими методами моделювання, які доцільно використовувати для аналізу інформаційної безпеки, визначено: системну динаміку – що дозволяє вивчати взаємозв'язки між компонентами системи та моделювати їхню поведінку у відповідь на зміни зовнішнього середовища; а також мітаційне моделювання – яке використовується для оцінки ефективності різних сценаріїв реагування на загрози та оптимізації управлінських рішень.

Результати дослідження є вагомим внеском у розвиток теоретичних та практичних аспектів інформаційної безпеки, що є критично важливим для забезпечення сталого розвитку держави в умовах сучасних викликів, воєнного часу та наступного відновлювального періоду тощо.

Ключові слова: *інформаційна безпека, техногенні системи, системна динаміка, управління ризиками, стратегічне планування, адаптивність, моделювання.*

Постановка проблеми. Інформаційна безпека держави є фундаментальною складовою національної безпеки, забезпечуючи стабільне функціонування державних інституцій, національної економіки, захист критично важливих даних, інфраструктурних об'єктів та інформаційних систем. В умовах глобалізації, цифровізації суспільства та зростання масштабів кібератак традиційні підходи до забезпечення інформаційної безпеки виявляють обмежену ефективність.

Це зумовлює необхідність наукового переосмислення безпекових проблем, враховуючи їх багатовимірний, динамічний та технологічно залежний характер. Закони України «Про основи

національної безпеки України» та «Про захист інформації в інформаційно-телекомунікаційних системах», наголошують на важливості системного підходу до забезпечення інформаційної безпеки та управління інформаційними ресурсами [1, с. 3–5; 2, с. 12].

Сучасні стратегії, зокрема Стратегія кібербезпеки України на 2021–2025 роки, визначають кібератаки та інформаційні загрози як ключові ризики для національної безпеки [3, с. 7]. Стратегія акцентує увагу на необхідності інтегрованого підходу до захисту інформаційного простору через використання наукових методів моделювання, системного аналізу ризиків та прогнозування. Ці положення створюють належне підґрунтя для розгляду інформаційної безпеки держави як складної динамічної системи, яка функціонує в умовах взаємодії технічних, організаційних, інформаційних та людських компонентів.

Запропонований системний підхід до моделювання інформаційної безпеки держави дозволяє врахувати вплив ключових компонентів, їх взаємозалежність, адаптивність до змін та динамічність наявних, а також прогнозованих у майбутньому ризиків. Зокрема, модель має інтегрувати аналіз взаємодії технічних та організаційних складових із соціальними факторами, включаючи вплив людського фактору.

Результати моделювання можуть використовуватися для оцінювання стану інформаційної безпеки, прогнозування можливих загроз та формування стратегій їх мінімізації у різних сферах суспільного життя. Науковий аналіз моделей інформаційної безпеки забезпечує стратегічну основу для впровадження інноваційних підходів до управління ризиками та підвищення ефективності управлінських рішень.

Аналіз останніх досліджень і публікацій. Серед сучасних наукових досліджень, які розкривають сутність складних динамічних систем, слід відзначити роботу Доусона М. П. (2020). У книзі «Мислення в системах та ментальні моделі» підкреслено важливість системного підходу для вирішення складних проблем та прийняття рішень у багатокомпонентних системах. Ця робота є фундаментальною для розуміння системної інтеграції в управлінні інформаційною безпекою [4, с. 27].

Турнер С., Ганель Р., Клімек П. як співавтори у праці «Вступ до теорії складних систем» (2018) наголошують на важливості нелінійної динаміки та адаптивності у складних технічних і соціальних системах. Вони пропонують методології для аналізу взаємодій між компонентами системи, які можуть бути корисними для розробки стратегій інформаційної безпеки держави [5, с. 45, 68].

Ауянг С. Ю. у книзі «Основи теорій складних систем: У економіці, еволюційній біології та статистичній фізиці» (1999) розглядає міждисциплінарний підхід до дослідження складних систем. Її висновки застосовані для інтеграції підходів до управління інформаційною безпекою через аналіз складних технічних систем [6, с. 89, 120].

Маккі З. у праці «Мислення в системах: Теорія та практика стратегічного планування» (2018) пропонує прості інструменти для стратегічного управління, які можуть стати корисними у контексті інформаційної безпеки, дозволяючи уникнути типових помилок при моделюванні складних технічних систем [7, с. 18, 52].

Беттенкурт Л. М. у книзі «Вступ до науки про міста» (2021) акцентує увагу на містах як складних системах із багатошаровою взаємодією компонентів. Цей підхід може бути адаптований для аналізу критичної інфраструктури держави, яка також функціонує за принципами складних систем [8, с. 5, 33].

Гуастелло С. Дж., Купманс М., Пінкус Д. у праці «Хаос і складність у психології: Теорія нелінійних динамічних систем» (2009) пропонують інструменти для вивчення нелінійної поведінки систем, що є важливим для аналізу людського фактора у питаннях інформаційної безпеки [9, с. 14, 50].

Поряд з цим, Іванцевич В. Г. і Рід Д. Дж. у книзі «Складність і управління: До строгої поведінкової теорії складних динамічних систем» (2014) пропонують методи моделювання та управління складними технічними системами, що безпосередньо пов’язано з управлінням інформаційною безпекою держави [10, с. 8, 42].

Кіль Л. Д. і Елліот Е. В. у праці «Складні системи в соціальних і поведінкових науках» (2021) аналізують взаємодію компонентів у соціальних системах. Цей підхід може бути корисним для розуміння системної адаптивності у контексті інформаційної безпеки [11, с. 20, 55].

Берхаут Е., Фійтенман Р., Хендрікс Л., де Бур М. та Бутейн Б. у книзі «Аудит цифрових систем: Теорія і практика аудиту складних інформаційних систем і технологій» (2022) розглядають методології аудиту складних інформаційних систем. Їхній підхід дозволяє ефективно оцінювати ризики та вразливості, що є ключовим для забезпечення безпеки державних систем [12, с. 17, 35].

Раш В. та Вулф К. у праці «Спостереження за складністю: Теорія систем і постмодерн»

(2000) розкривають концептуальні основи складних систем і взаємодій. Цей теоретичний підхід може допомогти у розробці наукових підходів до захисту інформаційних систем [13, с. 6, 45].

Беннет А. та Беннет Д. у книзі «Організаційне виживання в новому світі» (2003) досліджують адаптивність складних систем і методи їхнього стійкого функціонування. Це дозволяє впроваджувати ефективні моделі управління у сфері інформаційної безпеки [14, с. 11, 28].

Отже, активний науковий інтерес безперечно свідчить про актуальність досліджуваної теми. Проте, невирішеними аспектами визначеної проблеми залишається реалізація системного підходу в аналізі інформаційної безпеки держави, яку доцільно розглядати як складну динамічну техногенну систему, а інтеграцію системного мислення, міждисциплінарних підходів та адаптивного управління, на цьому тлі, – ключем до підвищення захисту критичних інформаційних ресурсів.

Постановка завдання. Метою статті є визначення провідних чинників розв'язання проблем моделювання інформаційної безпеки України як складної динамічної системи, що дозволить визначити найвпливовіші фактори ризику, які впливають на її стійкість та ефективність, а головне завдання полягає у формуванні та вдосконаленні техногенних стратегій, спрямованих на забезпечення адаптивності, стійкості та надійності системи інформаційної безпеки у сучасних умовах глобальних викликів.

Поряд з цим, важливими завданнями дослідження, по-перше, є розробка концептуальної моделі інформаційної безпеки держави, яка враховує взаємодію технічних, організаційних, інформаційних та людських компонентів, а також ідентифікація ключових факторів ризику, які впливають на стійкість системи інформаційної безпеки, та оцінка їх впливу на динаміку системи.

По-друге, важливим завданням дослідження стала розробка техногенних стратегій управління ризиками, що забезпечують інтегровану стійкість системи до зовнішніх і внутрішніх загроз та визначення підходів до оптимізації управлінських рішень на рівні технологій та персоналу, спрямованих на мінімізацію ризиків, а також надання практичних рекомендацій для державних установ щодо впровадження інноваційних рішень у сфері інформаційної безпеки, які враховують динамічні та багатофакторні характеристики системи.

Для реалізації зазначених завдань передбачено проведення системного аналізу складових інформаційної безпеки, включаючи технічну інфраструктуру, організаційні процеси, інформаційні ресурси та людський фактор, а також використання методів системної динаміки для моделювання взаємодії ключових компонентів системи та прогнозування можливих сценаріїв розвитку ризиків.

До цього ж, зауважимо, що розробка інтегрованих підходів до управління ризиками передбачає застосування технологічних інновацій, налаштування адаптивного управління та створення дієвих алгоритмів вдосконалення навичок персоналу.

На такій основі стає можливим формування обґрунтованих рекомендацій для оптимізації процесів прийняття рішень у сфері інформаційної безпеки з урахуванням специфіки функціонування державних установ, суб'єктів господарювання всіх рівнів тощо. При цьому, очікувані результати дослідження передбачають створення ефективних інструментів для підвищення стійкості інформаційної безпеки України, що враховують складність і динамічність сучасного інформаційного простору.

Виклад основного матеріалу. Інформаційна безпека держави є складною динамічною технічною системою, яка включає в себе багаторівневу інтеграцію технічних, інформаційних, організаційних та людських компонентів для забезпечення захисту державного інформаційного простору від зовнішніх і внутрішніх загроз. Як і будь-яка складна техногенна система, інформаційна безпека має визначальні риси, що суттєво впливають на її ефективність і стійкість.

Однією з ключових рис є нелінійність, яка полягає у тому, що взаємодія між компонентами системи може створювати ефекти, які важко передбачити. Наприклад, вплив людського фактору в управлінні технічними засобами може призвести до появи нових ризиків. Це підтверджується дослідженнями, які підкреслюють важливість системного підходу до аналізу взаємозв'язків між компонентами [4, с. 12, 27].

Наступною важливою рисою є адаптивність, що проявляється у здатності системи до налаштування під впливом змін у зовнішньому середовищі. Дослідники наголошують, що адаптивність є ключовою умовою для стійкості систем в умовах невизначеності та зростаючих ризиків [7, с. 18, 52]. Цей підхід до адаптивного управління є особливо цінним для інформаційної безпеки, яка потребує постійного вдосконалення в умовах динамічної трансформації технологічного середовища.

Інформаційна безпека також є динамічною системою, що означає постійні зміни у її структурі та функціонуванні. Динамічні системи вима-

гають швидкої реакції на зміни, що є важливим для протидії новим кіберзагрозам та оптимізації управління інформаційними процесами.

Ще однією характерною рисою системи інформаційної безпеки є стохастичність, тобто наявність випадкових впливів, які ускладнюють прогнозування результатів і функціонування системи. Дослідження підкреслюють, що системи з високим рівнем стохастичності потребують ретельного управління ризиками та використання нелінійних моделей для оцінки можливих сценаріїв розвитку [9, с. 14, 50].

Для забезпечення ефективності інформаційної безпеки як складної техногенної системи важливо також враховувати суттєвий вплив людського фактору. Дослідники відзначають важливість інтеграції людських і технічних компонентів у процесах адаптивного управління ризиками, що є особливо актуальним у сфері інформаційної безпеки, де якість управлінських рішень залежить не лише від технологій, а й від компетентності персоналу, його соціально-психологічного стану, стресостійкості та конфліктності тощо [10, с. 8, 42].

Виходячи з цього, можна стверджувати, що система інформаційної безпеки держави повністю відповідає характеристикам складної динамічної технічної системи. Вона інтегрує технічні, організаційні, інформаційні та людські компоненти, взаємодія яких визначає її ефективність і стійкість. Висновки, зроблені на основі аналізу наукових робіт, підтверджують необхідність системного підходу до моделювання та управління інформаційною безпекою [6, с. 89, 120; 8, с. 5, 33; 13, с. 6, 45].

Загалом інформаційна безпека держави, будучи складною системою, потребує інтеграції системного мислення, адаптивного управління і багатофакторного аналізу, що дозволить забезпечити її надійність і стійкість у сучасному динамічному середовищі.

Інноваційні методи моделювання складних техногенних систем включаючи системи інформаційної безпеки відкривають нові можливості для ефективного управління їхньою динамікою, стійкістю та адаптивністю. Ці методи базуються на інтеграції сучасних технологій математичного моделювання та людського досвіду, що дозволяє враховувати багатофакторний характер таких систем.

Серед найбільш перспективних інноваційних підходів слід відзначити використання цифрових двійників. Цей метод передбачає створення інтегрованих цифрових моделей, які імітують функціонування реальних об'єктів. Цифрові двійники дозволяють тестувати сценарії розвитку подій, оцінювати ризики та знаходити оптимальні рішення без ризику для реальних систем.

Наприклад, такі моделі можуть бути використані для перевірки ефективності нових засобів захисту або виявлення вразливостей у державних інформаційних системах. Їх застосування є ключовим для підвищення стійкості та надійності системи в умовах динамічних загроз.

Поряд з цим, інтелектуальні алгоритми на основі штучного інтелекту та машинного навчання стають ще одним потужним інструментом моделювання складних систем. Вони дозволяють автоматизувати аналіз ризиків, виявляти патерни аномальної поведінки та пропонувати адаптивні стратегії реагування на загрози. Ці алгоритми мають особливу цінність для прогнозування та раннього виявлення кіберзагроз, що дозволяє оперативно реагувати на нові виклики.

Ще одним продуктивним підходом є експертні оцінки які використовуються для визначення слабких місць у системі. Хоча цей метод є менш автоматизованим, він залишається актуальним завдяки можливості врахування досвіду фахівців, які мають глибокі знання про специфіку функціонування техногенних систем. Залучення експертів дозволяє комбінувати інтуїтивне розуміння системних процесів із точністю математичних моделей.

Використання цих інноваційних методів дозволяє створювати гібридні моделі, які поєднують математичний аналіз, імітаційне моделювання та експертний підхід. Такий підхід забезпечує системний аналіз складних техногенних систем, включаючи інформаційну безпеку держави і дозволяє враховувати як технічні так і організаційні аспекти.

Інтеграція цифрових двійників штучного інтелекту та експертних оцінок сприяє підвищенню якості управлінських рішень адаптивності системи до змін зовнішнього середовища та ефективності заходів безпеки. Отже, впровадження інноваційних методів моделювання складних систем є важливим напрямом розвитку інформаційної безпеки, який дозволяє одночасно підвищувати її надійність стійкість та здатність до адаптації у відповідь на сучасні виклики.

Методи математичного та інноваційного моделювання, які можуть бути ефективно використані для аналізу інформаційної безпеки також застосовуються для моделювання інших складних техногенних систем держави. Їх використання дозволяє оцінювати функціонування цих систем, визначати ключові ризики, а також розробляти стратегії їхнього вдосконалення та підвищення стійкості.

Наприклад, у системі управління енергетичною безпекою застосування методів системної динаміки дозволяє моделювати взаємозв'язки між компонентами енергетичної системи, такими як: постачання, споживання, зберігання та резервування енергії.

Разом з цим, використання цифрових двійників допомагає прогнозувати наслідки технічних збоїв або атак на критичну інфраструктуру енергомережі, а інтелектуальні алгоритми забезпечують оптимізацію енергоспоживання та управління ризиками. Також цифрові двійники допомагають тестувати стратегії без реального ризику, а інтелектуальні алгоритми забезпечують автоматизацію прийняття рішень.

У системі забезпечення кібербезпеки критичної інфраструктури держави, яка включає транспортні мережі, водопостачання, зв'язок та фінансові установи, імітаційне моделювання використовується для тестування сценаріїв атак оцінки їхнього впливу на функціонування системи та перевірки ефективності заходів безпеки.

Паралельно значного функціонального значення набувають також методи мережевого аналізу, що допомагають визначити критичні вузли, які потребують посилення захисту. У системі реагування на надзвичайні ситуації, яка включає природні катастрофи, техногенні аварії та ін. кризи, використання таких методів як агентне моделювання дозволяє імітувати поведінку системи в умовах кризи, оцінювати можливі сценарії розвитку подій і розробляти оптимальні стратегії реагування.

У системі управління екологічною безпекою моделювання взаємодії між екологічними, технічними та соціальними компонентами є важливим для забезпечення стійкості екосистем та зменшення впливу техногенних факторів. Методи системної динаміки дозволяють прогнозувати наслідки забруднення зміни клімату чи інших екологічних загроз, а імітаційні моделі допомагають визначити ефективність заходів з мінімізації шкоди.

У системі охорони здоров'я в умовах пандемії можуть застосовуватися інтелектуальні алгоритми для прогнозування поширення захворювань, оцінки ефективності карантинних заходів і оптимізації розподілу медичних ресурсів. Імітаційні моделі допомагають оцінити можливі сценарії розвитку епідемії, а експертні оцінки доповнюють математичні розрахунки знаннями фахівців.

Таким чином методи моделювання складних техногенних систем є універсальними інструментами, які можуть бути адаптовані для аналізу та оптимізації функціонування різноманітних систем держави. Їх застосування забезпечує можливість не лише оцінювати поточний стан систем, але й прогнозувати їхню поведінку за різних умов, розробляти ефективні стратегії управління та мінімізувати ризики у сучасному мінливому середовищі.

Для аналізу інформаційної безпеки держави як складної технічної системи у дослідженні обрано системно-динамічну модель на основі методу наукового аналізу. Цей метод дозволяє всебічно оцінити взаємодію численних факторів, що впливають на інформаційну безпеку, враховуючи її динаміку, нелінійність, зворотні зв'язки та еволюцію у часі. Вибір цієї моделі був обґрунтований через її здатність формалізувати комплексні процеси, інтегрувати різнорідні аспекти, а також прогнозувати сценарії розвитку ситуацій.

При цьому, перш за все зауважимо, що саме нормативна база України вимагає врахування багатовимірності інформаційної безпеки. Закон України «Про основи національної безпеки України» [1, с. 351] визначає забезпечення інформаційної безпеки як один із пріоритетів державної політики. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [2, с. 286] підкреслює важливість технічного і організаційного захисту інформаційних систем, що передбачає моделювання їхньої роботи як складних систем. Крім того, у Стратегії кібербезпеки України на 2021–2025 роки [3, с. 7–16] акцентується увага на важливості комплексного підходу до аналізу ризиків і прогнозування загроз, що підтверджує доцільність застосування системного підходу.

З теоретичної точки зору, системно-динамічна модель дозволяє враховувати складну взаємодію між елементами системи і зовнішніми факторами. Як зазначає, приміром, Доусон М. П. [4, с. 11], системне мислення допомагає розуміти нелінійні динамічні процеси та ухвалювати стратегічні рішення. Турнер С. та його співавтори [5, с. 18] підкреслюють, що складні системи, зокрема інформаційні, потребують моделювання із врахуванням емерджентних властивостей, а Ауянг С. Ю. [6, с. 22] акцентує увагу на необхідності адаптивного управління такими системами.

Крім того, системно-динамічний підхід дозволяє формалізувати взаємозв'язки між компонентами інформаційної безпеки та здійснювати кількісний аналіз. Маккі З. [7, с. 9] зазначає, що саме системно-динамічні моделі є найкращими для стратегічного планування та вирішення проблем,

що виникають у складних адаптивних системах. Це підтверджує і Беттенкурт Л. М. А., який досліджував складність урбаністичних систем, подібних за структурою до інформаційних [8, с. 14].

Отже, порівнюючи системно-динамічну модель з іншими підходами, варто зазначити, що агентно-орієнтовані моделі [9, с. 12] ефективні для аналізу окремих суб'єктів системи, але не враховують загальну динаміку. Моделі ризик-менеджменту, як стверджує Іванцевич В. Г. [10, с. 8], фокусуються на оцінці ризиків, проте ігнорують складні взаємозв'язки між ними. Натомість системно-динамічні моделі, за словами Кіля Л. Д. [11, с. 5], є більш універсальними і здатні враховувати всі аспекти поведінки складної системи.

Інформаційна безпека держави є складною багатокомпонентною системою, яка охоплює технічну інфраструктуру, організаційні процеси, інформаційні ресурси, людський фактор та взаємодію із зовнішніми загрозами. Схема демонструє модель інформаційної безпеки держави як складної динамічної системи, розробленої на основі системно-динамічного підходу. Метою такої моделі є виявлення ключових компонентів системи, аналіз їх взаємодії та оцінка впливу зовнішніх і внутрішніх факторів на її стійкість. Система побудована так, щоб забезпечувати адаптивність, інтегрованість і здатність до ефективного реагування на загрози.

Таким чином, на основі аналізу нормативної бази, теоретичних досліджень та порівняння з іншими підходами, ми дійшли висновку, що системно-динамічна модель є найбільш ефективною для аналізу інформаційної безпеки держави. Вона дозволяє враховувати складність, адаптивність і взаємозалежність компонентів системи, що забезпечує надійність у прогнозуванні і прийнятті рішень (рис. 1). Представлена візуалізація є не лише інструментом аналізу поточного стану інформаційної безпеки, але й методологічною основою для розробки стратегій управління ризиками та вдосконалення управлінських процесів.

Система інформаційної безпеки держави складається з кількох ключових компонентів, кожен із яких виконує важливу роль у забезпеченні її стійкості та ефективності.

По-перше, технічна інфраструктура включає сервери, мережі зв'язку, системи захисту та

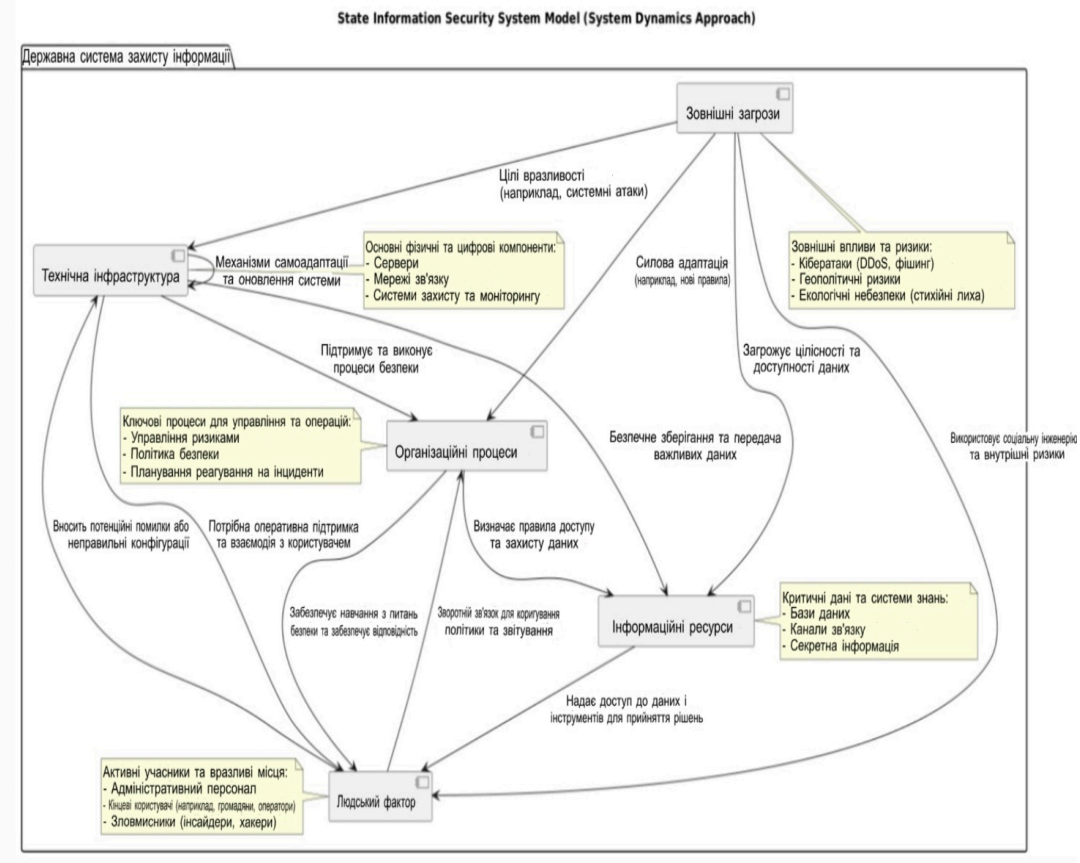

Рис. 1. Взаємозв'язок провідних складових системно-динамічної моделі аналізу інформаційної безпеки держави

Джерело: складено авторами.

моніторингу, які забезпечують стабільну роботу інформаційних процесів. Вона виконує основну функцію захисту даних та систем, а також має вбудовані механізми самодіагностики та оновлення, що дозволяють оперативно реагувати на зміни у технологічному середовищі або нові загрози.

По-друге, організаційні процеси пов'язані з стратегічним управлінням, яке охоплює ризик-менеджмент, формування політик та планування реагування на інциденти. Вони забезпечують інтеграцію технічної інфраструктури та людського фактору через навчання персоналу, контроль дотримання правил безпеки та вдосконалення процедур.

По-третє, інформаційні ресурси є критично важливими даними, які включають бази даних, канали зв'язку та інформацію з обмеженим доступом. Вони потребують забезпечення належного рівня доступу, безпечного зберігання та захисту від несанкціонованого втручання.

По-четверте, людський фактор відіграє ключову роль у функціонуванні системи, включаючи діяльність персоналу, поведінку кінцевих користувачів та наміри потенційних зловмисників. Він може бути джерелом ризиків, таких як помилкові дії, недотримання вимог внутрішньо-організаційних політик або атаки через соціальну інженерію, але також є важливим елементом управління системою.

Та, по-п'яте, зовнішні загрози, включаючи кібератаки, геополітичні ризики різної спрямованості чи екологічні небезпеки, створюють постійний тиск на систему, змушуючи її адаптуватися до нових умов.

При цьому, усі компоненти системи взаємопов'язані. Технічна інфраструктура підтримує організаційні процеси та інформаційні ресурси, забезпечуючи їхню функціональність. Організаційні процеси формують політики доступу до даних, стандарти взаємодії персоналу із системою та управляють ризиками. Людський фактор взаємодіє з усіма компонентами, забезпечуючи їхню роботу, виконання політик та реагування на загрози. Зовнішні загрози впливають на всі рівні системи, зокрема через технічні атаки, соціальну інженерію та організаційний вплив.

Отже, система має кілька унікальних рис, які роблять її ефективною у сучасних умовах. Вона є адаптивною, тобто здатною динамічно реагувати на зовнішні впливи та внутрішні зміни. Системна інтеграція забезпечує комплексну взаємодію між усіма її компонентами.

Проактивність дозволяє системі прогнозувати загрози та заздалегідь планувати дії для мінімізації ризиків. Усе це робить її стійкою та надійною в умовах сучасних викликів. Ця модель надає чітке уявлення про структуру, взаємозв'язки та механізми функціонування державної системи інформаційної безпеки. Вона є основою для подальшого впровадження стратегічних рішень, що підвищують стійкість державних інформаційних систем до сучасних викликів.

Висновки. Інформаційну безпеку держави слід розглядати як складну динамічну технічну систему, що об'єднує технічні, інформаційні, організаційні та людські компоненти для забезпечення захисту інформаційного простору від зовнішніх і внутрішніх загроз.

Її функціонування визначається такими характеристиками, як нелінійність, адаптивність, динамічність і стохастичність, що створює передумови для використання наукового математичного моделювання для її подальшого аналізу та вдосконалення.

Нелінійність системи відображає складність взаємодії між її компонентами, які можуть призводити до непередбачуваних наслідків. Це вимагає застосування системного підходу для вивчення її структури та поведінки. Адаптивність забезпечує здатність системи реагувати на нові виклики, що є особливо важливим в умовах динамічних кіберзагроз. Динамічність вказує на постійні зміни у системі, пов'язані із впровадженням нових технологій та появою нових загроз, а стохастичність підкреслює важливість врахування випадкових факторів і сценаріїв.

Наукові методи моделювання, які доцільно використовувати для аналізу інформаційної безпеки, включають:

1. Системну динаміку – метод, що дозволяє вивчати взаємозв'язки між компонентами системи та моделювати їхню поведінку у відповідь на зміни зовнішнього середовища.

2. Імітаційне моделювання, яке використовується для оцінки ефективності різних сценаріїв реагування на загрози та оптимізації управлінських рішень.

3. Методи мережевого аналізу, які дозволяють оцінити критичні вузли системи, їхній вплив на загальну стійкість та ефективність функціонування.

4. Цифрові двійники – інтегровані моделі, що імітують реальні системи, дають змогу проводити експерименти з метою тестування ефективності стратегій управління ризиками.

5. Інтелектуальні алгоритми, які базуються на штучному інтелекті, дозволяють аналізувати

ризики, прогнозувати загрози та автоматизувати управління.

6. Експертні оцінки – метод, що доповнює математичні моделі досвідом фахівців для визначення слабких місць системи.

Завдяки цим методам можна створювати багатофакторні моделі, які враховують технічні, організаційні та соціальні аспекти системи. Це дозволяє не лише досліджувати її функціонування, але й формувати ефективні стратегії для підвищення її стійкості. Інтеграція цифрових двійників, інтелектуальних алгоритмів та методів системної динаміки забезпечує поєднання теоретичного аналізу та практичних заходів.

У подальшому наукове математичне моделювання інформаційної безпеки держави стає не лише можливим, але й необхідним для її постійного вдосконалення. Застосування оновлених інноваційних методів моделювання відкриває можливості для визначення пріоритетних стратегій її підвищення, зокрема шляхом впровадження сучасних технологій, адаптивного управління ризиками та розвитку системного підходу до управління. Це у перспективі буде здатне забезпечити надійність, адаптивність і стійкість системи інформаційної безпеки в умовах як сучасних, так і майбутніх викликів.

Список літератури:

1. Закон України «Про основи національної безпеки України» від 19 червня 2003 року № 964-IV // *Відомості Верховної Ради України.* 2003. № 39. С. 351.

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР // *Відомості Верховної Ради України.* 1994. № 31. С. 286.

3. Стратегія кібербезпеки України на 2021–2025 роки, затверджена рішенням РНБО України від 14 травня 2021 року, введена в дію Указом Президента України від 26 серпня 2021 року № 447/2021 // *Офіційний вісник Президента України.* 2021. № 20. С. 7–16.

4. Доусон М. П. Мислення в системах та ментальні моделі: Як мислити як супер-мислитель. Керівництво з мистецтва ухвалення рішень і вирішення складних проблем. Теорія хаосу, наука про мислення для соціальних змін / М. П. Доусон. 2020. 184 с.

5. Турнер С., Ганель Р., Клімек П. Вступ до теорії складних систем / С. Турнер, Р. Ганель, П. Клімек. Оксфордське університетське видавництво, США, 2018. 240 с.

6. Ауянг С. Ю. Основи теорій складних систем: У економіці, еволюційній біології та статистичній фізиці / С. Ю. Ауянг. – Кембриджське університетське видавництво, 1999. 320 с.

7. Маккі З. Мислення в системах: Теорія та практика стратегічного планування, вирішення проблем та створення тривалих результатів – простота складності / З. Маккі. *CreateSpace Independent Publishing Platform,* 2018. URL: https://vcf.vn.ua/sposib-piznannya-rozvinuti-logichne-mislennya/ (дата звернення: 10.12.2024).

8. Беттенкурт Л. М. А. Вступ до науки про міста: Докази та теорія міст як складних систем / Л. М. А. Беттенкурт. MIT Press, 2021. URL: https://ela.kpi.ua/bitstream/123456789/50988/1/Metody_modeliuvannia.pdf (дата звернення: 10.12.2024).

9. Гуастелло С. Дж., Купманс М., Пінкус Д. Хаос і складність у психології: Теорія нелінійних динамічних систем / С. Дж. Гуастелло, М. Купманс, Д. Пінкус. Кембриджське університетське видавництво, 2009. URL: https://www.yakaboo.ua/ua/mistectvo-misliti-sistemno-rozv-jazannja-problem-vid-osobistogo-do-globalnogo-masshtabu.html (дата звернення: 10.12.2024).

10. Іванцевич В. Г., Рід Д. Дж. Складність і управління: До строгої поведінкової теорії складних динамічних систем / В. Г. Іванцевич, Д. Дж. Рід. – World Scientific Publishing Co., 2014. URL: https://khai.edu/assets/files/ robochi-programi/124/sistemnij-analiz/rp_b_124_modelyuvannya-skladnih-sistem-z-kr.pdf (дата звернення: 10.12.2024).

11. Кіль Л. Д., Елліот Е. В. Складні системи в соціальних і поведінкових науках: Теорія, метод і застосування / Л. Д. Кіль, Е. В. Елліот. Мічиганське університетське видавництво, 2021. URL: https://hub.kyivstar.ua/ reviews/mistecztvo-sistemnogo-mislennya (дата звернення: 10.12.2024).

12. Берхаут Е., Фійтенман Р., Хендрікс Л., де Бур М., Бутейн Б. Аудит цифрових систем: Теорія і практика аудиту складних інформаційних систем і технологій / Е. Берхаут, Р. Фійтенман, Л. Хендрікс, М. де Бур, Б. Бутейн. Springer, 2022. URL: https://link.springer.com/book/10.1007/978-3-030-57530-3 (дата звернення: 10.12.2024).

13. Раш В., Вулф К. Спостереження за складністю: Теорія систем і постмодерн / В. Раш, К. Вулф. Видавництво Університету Міннесоти, 2000. URL: https://www.upress.umn.edu/book-division/books/observing-complexity (дата звернення: 10.12.2024).

14. Беннет А., Беннет Д. Організаційне виживання в новому світі: Розумна складно-адаптивна система / А. Беннет, Д. Беннет. Butterworth-Heinemann, 2003. URL: https://www.elsevier.com/books/ organizationalsurvival-in-the-new-world/bennett/9780750677121 (дата звернення: 10.12.2024).

Prokopovych-Tkachenko D.I., Sarychev V.I., Zvieriev V.P., Khruskov B.S., Bushkov V.G.

MODELING STATE INFORMATION SECURITY AS A COMPLEX TECHNOLOGICAL SYSTEM: A STRATEGIC APPROACH TO RISK MANAGEMENT

The article addresses the issues of ensuring the information security of the state, which is a complex technogenic system combining technical, organizational, informational, and human components, operating in a dynamic environment and under high-level risks. A systematic approach to modeling information security is presented, taking into account its complex structure, dynamism, adaptability, and multifactorial nature. A conceptual model has been developed, reflecting the main risks and ways to minimize them through strategic planning and management. The model is based on the principles of system dynamics, integrated risk analysis, and adaptive management, ensuring its effectiveness under modern conditions.

Special attention is given to the influence of the human factor on the functioning of the information security system and the need to consider its role in achieving final results. The proposed approaches aim to optimize management processes in various spheres of social and economic life, ensure the reliability and resilience of the system, and its ability to adapt to changes in the external environment. The application of the developed model allows state institutions and organizations, including business structures, to improve decision-making processes in the field of information security, reduce risks, and enhance the effectiveness of security measures.

The leading scientific modeling methods that are appropriate for analyzing information security include: system dynamics, which enables the study of interconnections between system components and modeling their behavior in response to changes in the external environment; and scenario-based modeling, used to assess the effectiveness of different threat response scenarios and optimize managerial decisions.

The research results make a significant contribution to the development of theoretical and practical aspects of information security, which is critically important for ensuring the sustainable development of the state in the context of modern challenges, wartime, and the subsequent recovery period, among others.

Key words: *information security, technogenic systems, system dynamics, risk management, strategic planning, adaptability, modeling.*