УДК 004.056.5
DOI https://doi.org/10.32782/2521-6643-2024-2-68.10

Прокопович-Ткаченко Д. І., кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки та інформаційних технологій
Університету митної справи та фінансів
ORCID: 0000-0002-6590-3898

ЕМЕРДЖЕНТНО-АДАПТИВНИЙ МЕТОД ОЦІНКИ ВПЛИВУ ПОСТКВАНТОВОГО СЕРЕДОВИЩА НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ДЕРЖАВИ

У статті запропоновано емерджентно-адаптивний метод для оцінки впливу постквантового середовища на інформаційну безпеку держави, що ґрунтується на принципах самоорганізації та синергії. Метод спрямований на забезпечення ефективного реагування на загрози, пов'язані з розвитком квантових обчислень, які можуть порушити існуючі криптографічні протоколи, такі як RSA та ECC. Розглянуто ключову роль штучного інтелекту в аналізі, прогнозуванні та динамічній адаптації захисних систем.

При моделюванні атак проводяться симуляції впливу квантових обчислень на криптографічні системи, зокрема оцінюється стійкість ключових протоколів до атак алгоритмів Шора та Ґровера. На етапі адаптації впроваджуються квантово стійкі криптографічні рішення, такі як решіткові алгоритми, кодові схеми та геш-функції, а також проводиться моніторинг їхньої ефективності.

Далі виконується аналіз загроз, який фокусується на дослідженні можливостей квантових обчислень, здатних порушити сучасні криптографічні системи. Наступним кроком є оцінка вразливостей, під час якої ідентифікуються використовувані криптографічні алгоритми, такі як RSA та ECC, і аналізується їхня стійкість до атак квантовими алгоритмами.

Після цього виконується аналіз критичних точок і протоколів зв'язку, що охоплює оцінку стійкості таких протоколів, як TLS/SSL, IPsec, VPN, до можливих квантових атак. Наступним етапом є симуляція атак, яка передбачає моделювання квантових атак для оцінки ймовірності їхнього успіху. Завершальним етапом є розробка рішень постквантової безпеки, що включає вибір та впровадження нових криптографічних алгоритмів, стійких до квантових атак, та їхню інтеграцію в існуючі системи. Усі етапи взаємопов'язані та забезпечують динамічну адаптацію системи до нових викликів.

Доведено, що запропонований підхід забезпечує підвищену стійкість інформаційних систем до нових загроз завдяки інтеграції класичних та постквантових протоколів. Особливу увагу приділено синергії різних компонентів безпеки, що дозволяє створювати адаптивні та самоорганізовані системи. Перспективи подальших досліджень включають розробку моделей емерджентності, інтеграцію постквантових рішень у державні інформаційні системи та впровадження міждисциплінарного підходу до забезпечення кібербезпеки.

Ключові слова: *постквантове середовище, емерджентність, кібербезпека, квантові обчислення, адаптація.*

Prokopovych-Tkachenko D. I. Emergent-adaptive method of assessing the impact of the post-quantum environment on the information security of the state

The article proposes an emergent-adaptive method for assessing the impact of the post-quantum environment on the state's information security, based on the principles of self-organization and synergy. The method aims to ensure effective responses to threats associated with the development of quantum computing, which may compromise existing cryptographic protocols such as RSA and ECC. The critical role of artificial intelligence in analyzing, forecasting, and dynamically adapting defensive systems is highlighted.

During attack modeling, simulations are conducted to evaluate the impact of quantum computing on cryptographic systems, specifically assessing the resilience of key protocols against attacks by Shor's and Grover's algorithms. At the adaptation stage, quantum-resistant cryptographic solutions such as lattice-based algorithms, code-based schemes, and hash functions are implemented, and their effectiveness is monitored.

This is followed by a threat analysis that focuses on exploring the capabilities of quantum computing to break current cryptographic systems. The next step is a vulnerability assessment that identifies the cryptographic algorithms used, such as RSA and ECC, and analyzes their resistance to quantum attacks.

This is followed by an analysis of critical points and communication protocols, which includes assessing the resistance of protocols such as TLS/SSL, IPsec, VPN to possible quantum attacks. The next stage is attack simulation, which involves modeling quantum attacks to assess the likelihood of their success. The final stage is the development of post-quantum security solutions, which includes the selection and implementation of new cryptographic algorithms that are resistant to quantum attacks and their integration into existing systems. All stages are interconnected and ensure the dynamic adaptation of the system to new challenges.

It has been proven that the proposed approach enhances the resilience of information systems to new threats by integrating classical and post-quantum protocols. Particular attention is given to the synergy of various security components, enabling the creation of adaptive and self-organized systems. Prospects for further research include the development of emergent models, the integration of post-quantum solutions into state information systems, and the adoption of an interdisciplinary approach to cybersecurity.

Key words: *post-quantum environment, emergence, cybersecurity, quantum computing, adaptation.*

Вступ. Розвиток квантових обчислень створює нові виклики для сучасних систем інформаційної безпеки, що вимагає перегляду підходів до їх побудови та адаптації. Постквантове середовище характеризується взаємодією двох складних систем – квантових технологій та державної системи інформаційної безпеки. Ці системи мають різну природу, структуру і динаміку, що ускладнює їх інтеграцію та потребує розробки нових адаптивних методів.

Квантові технології відкривають нові можливості, такі як створення стійких до зламів каналів зв'язку, однак одночасно створюють і ризики, пов'язані зі зростанням потужності квантових алгоритмів для аналізу та компроментації даних. Інформаційна безпека держави, у свою чергу, має забезпечувати стійкість національної інфраструктури, включаючи урядові комунікації, управління критично важливими ресурсами та захист конфіденційної інформації.

Для цього необхідно впроваджувати інноваційні рішення, які дозволяють гнучко адаптуватися до динамічних змін у технологічному ландшафті. Особливу увагу слід приділити адаптації складних систем інформаційної безпеки до викликів, які супроводжують впровадження квантових технологій. Цей процес потребує розробки методів, що враховують складність обох систем, їхню взаємозалежність та необхідність функціонування в умовах невизначеності. Йдеться про створення моделей, які забезпечать ефективний перехід до квантово-стійкої архітектури з урахуванням сучасних загроз.

Зокрема, перспективним напрямом є розробка багаторівневих адаптивних систем, які поєднують квантові та традиційні підходи, забезпечуючи їх гнучкість, стійкість і надійність. Це включає механізми прогнозування загроз за допомогою штучного інтелекту, автоматизацію процесів оцінки ризиків та інтеграцію технологій, здатних працювати у складному динамічному середовищі. Такий підхід дозволить адаптувати державні системи інформаційної безпеки до нових умов, забезпечуючи їхню стійкість і ефективність у постквантовому технологічному середовищі.

Аналіз останніх досліджень і публікацій. Розвиток квантових обчислень створює нові загрози для сучасних систем інформаційної безпеки, що викликає потребу у впровадженні квантово-стійких рішень. Квантові алгоритми, такі як алгоритм Шора, мають здатність порушувати основи криптографічних протоколів, зокрема RSA та ECC, що підкреслює необхідність впровадження нових стандартів безпеки. Cyriac et al. (2024) наголошують на важливості поєднання класичних і квантових протоколів, таких як квантовий розподіл ключів (QKD), для створення захищених каналів зв'язку.

Однією з ключових проблем є вплив квантових обчислень на системи Інтернету речей (IoT). Alomari і Kumar (2024) відзначають, що хоча квантові обчислення сприяють прискоренню обробки даних, вони також створюють нові загрози для безпеки IoT-систем. У відповідь на це запропоновано підходи, які інтегрують емерджентні властивості для забезпечення стійкості таких систем.

Anantraj et al. (2023) пропонують системний підхід до інформаційної безпеки, який базується на принципах емерджентності. Цей підхід дозволяє створювати адаптивні моделі аналізу ризиків та захисту даних, які здатні до самоорганізації. Особливу увагу приділено інтеграції адаптивних технологій у постквантове середовище для побудови саморегульованих систем захисту.

Принципи емерджентності стають важливими в контексті квантової криптографії. Cyriac et al. (2024) підкреслюють, що взаємодія різних компонентів, таких як поєднання класичних і квантових підходів, сприяє утворенню властивостей, що перевищують можливості окремих елементів. Lara-Nino et al. (2022) акцентують увагу на необхідності впровадження квантово-стійких алгоритмів, які базуються на ґратках і геш-функціях, як надійного механізму захисту в державному секторі.

Крім того, синергія між різними методами захисту підсилює емерджентні властивості систем. Alomari і Kumar (2024) розглядають комбіноване використання шифрування і багаторівневого контролю доступу як приклад такого підходу. Це забезпечує більш стійкий захист в умовах динамічного середовища загроз. Висновки Anantraj et al. (2023) підкреслюють важливість дослідів цих методів. Інтеграція таких підходів з активним моніторингом та адаптивними технологіями стає ключовим напрямом для майбутнього інформаційної безпеки.

Постановка проблеми. Постквантові обчислення створюють нові виклики для забезпечення інформаційної безпеки, особливо в контексті державних інформаційних систем та критично важливих інфраструктур. Зі зростанням потужності квантових технологій існуючі підходи до забезпечення захисту даних стають дедалі менш ефективними. Вразливість сучасних криптографічних систем потребує не лише впровадження нових квантово-стійких алгоритмів, але й переосмислення методології виявлення загроз і побудови адаптивних систем безпеки.

Ключовою проблемою є те, що традиційні моделі кіберзахисту базуються на статичних методах виявлення загроз, які не відповідають динамічному та швидко змінюваному ландшафту сучасних атак. Постквантове середовище вимагає інноваційних підходів, які враховують можливості квантових обчислень для аналізу, прогнозування та нейтралізації ризиків у реальному часі. Це стосується не лише розробки нових технологій, але й створення самонавчальних систем, здатних адаптуватися до нових типів загроз без втручання людини.

У державному контексті це питання набуває критичного значення, оскільки від інформаційної безпеки залежить збереження конфіденційності, цілісності й доступності даних, які підтримують функціонування урядових структур, національної безпеки та критичних секторів економіки. Загрози постквантового середовища охоплюють не лише прямий компроміс даних, а й нові, складні вектори атак, які можуть залишатися непоміченими в рамках існуючих систем моніторингу.

Необхідно розробити нові підходи до виявлення загроз, які ґрунтуються на принципах адаптивності та емерджентності. Адаптивність дозволяє системам реагувати на непередбачувані ризики, тоді як емерджентність створює нові властивості через взаємодію компонентів системи. Інтеграція цих підходів забезпечить можливість саморегулювання, активного моніторингу та швидкого реагування на невідомі загрози. Таким чином, постквантове середовище вимагає трансформації підходів до інформаційної безпеки шляхом впровадження інноваційних методів аналізу ризиків, адаптивних моделей захисту та системного управління загрозами, здатних забезпечити стійкість у новій технологічній реальності.

Мета дослідження. Оцінка впливу постквантового середовища на інформаційну безпеку держави на підставі запропонованого емерджентно-адаптивний методу, що ґрунтується на принципах самоорганізації та синергії.

Виклад основного матеріалу дослідження. Під час реалізації запропонованого методу передбачається наступна поетапність:

1. ***Ідентифікація загроз**:* на цьому етапі проводиться аналіз векторів атак, які базуються на можливостях постквантових технологій. Особливу увагу приділяють вразливостям сучасних криптографічних протоколів (RSA, ECC, DSA) до алгоритмів Шора чи Гровера.

2. ***Моделювання атак**:* створюються симуляції квантових атак, що дають змогу оцінити ймовірність успіху зловмисника, а також розробити можливі. сценарії атак. Це включає аналіз потенційного впливу компрометації на ключові системи державної інфраструктур

3. ***Адаптація безпекових політик**:* впроваджуються постквантові алгоритми (наприклад, решіткові схеми, кодові алгоритми або геш-функції). Після інтеграції алгоритмів проводиться тестування оновлених систем, моніторинг ефективності захисту та постійна адаптація політик до нових загроз, також відповідну сегментацію поетапності (див. рис. 1).

Рис. 1. Оцінка постквантової безпеки

Схема, зображена на рисунку 1, відображає багатоступеневий алгоритм оцінки впливу постквантового середовища на інформаційну безпеку. На першому етапі здійснюється ініціалізація аналізу безпеки, що передбачає проведення систематичного огляду існуючих механізмів захисту для формування бази подальшого аналізу.

Далі виконується аналіз загроз, який фокусується на дослідженні можливостей квантових обчислень, здатних порушити сучасні криптографічні системи. Наступним кроком є оцінка вразливостей, під час якої ідентифікуються використовувані криптографічні алгоритми, такі як RSA та ECC, і аналізується їхня стійкість до атак квантовими алгоритмами.

Після цього виконується аналіз критичних точок і протоколів зв'язку, що охоплює оцінку стійкості таких протоколів, як TLS/SSL, IPsec, VPN, до можливих квантових атак. Наступним етапом є симуляція атак, яка передбачає моделювання квантових атак для оцінки ймовірності їхнього успіху. Завершальним етапом є розробка рішень постквантової безпеки, що включає вибір та впровадження нових криптографічних алгоритмів, стійких до квантових атак, та їхню інтеграцію в існуючі системи. Усі етапи взаємопов'язані та забезпечують динамічну адаптацію системи до нових викликів. Використовуючи поетапність сформуємо спрощений алгоритм у вигляди схеми (див. рис. 2), яка візуалізує процеси та взаємозв'язки, що реалізує запропонований метод.

Рис. 2. Відображення схеми у вигляді алгоритму реалізації емерджентно-адаптивного методу

Розглянемо питания адаптивності, що пов'язано з використанням штучного інтелекту у забезпеченні функції алхдаптивності цього методу.

Штучний інтелект (ШІ) викормтовується у адаптивному процесі емерджентно-адаптивного методу, оскільки він забезпечує динамічну інтеграцію аналізу, прогнозування та адаптації складних систем у відповідь на загрози або зміни середовища. ШІ здатний виявляти емерджентні властивості системи, які виникають із взаємодії її елементів, і використовувати ці властивості для підвищення ефективності управління ризиками.

У цьому контексті важливу роль відіграють нейронні мережі, які є ключовим компонентом ШІ для обробки великих обсягів даних, аналізу складних закономірностей та забезпечення адаптивності. Глибокі нейронні мережі (Deep Neural Networks, DNN) забезпечують здатність системи розпізнавати складні та нелінійні залежності між різними параметрами в умовах динамічного середовища.

Наприклад, у кібербезпеці нейронні мережі використовуються для аналізу великих масивів даних, таких як трафік мережі або поведінка користувачів, для виявлення аномалій, які можуть свідчити про потенційні загрози. Глибокі нейронні мережі також можуть прогнозувати ймовірність успішних атак, адаптуючи систему захисту до нових умов ще до виникнення проблеми. Нейронні мережі дозволяють створювати автономні адаптивні системи, які самостійно вивчають динаміку середовища. Наприклад, рекурентні нейронні мережі (RNN) особливо ефективні для аналізу часових послідовностей даних, що дозволяє прогнозувати майбутні події, засновані на історичній інформації, від поведінки зловмисника до розвитку загрози.

Конволюційні нейронні мережі (CNN), у свою чергу, можуть бути корисними для аналізу структурованих даних, таких як пакети мережевого трафіку, виявляючи характерні патерни або відхилення від норми. Завдяки цим властивостям нейронні мережі стають основою для створення адаптивних систем, які можуть виявляти раніше невідомі загрози, створювати нові механізми захисту та забезпечувати проактивне управління ризиками.

Водночас вони підвищують рівень інтеграції між різними компонентами системи, такими як шифрування, аналіз аномалій і управління доступом, сприяючи створенню єдиного адаптивного механізму захисту. Таким чином, використання нейронних мереж у рамках емерджентно-адаптивного методу забезпечує не лише підвищення стійкості систем до динамічних змін, але й їхню здатність самостійно еволюціонувати для реагування на нові виклики.

ШІ є фундаментальною частиною емерджентно-адаптивного підходу, оскільки він забезпечує динамічну інтеграцію аналізу, прогнозування та адаптації складних систем до нових загроз. ШІ дозволяє автоматизувати процеси виявлення вразливостей, моделювання атак і розробки захисних механізмів. Завдяки можливостям нейронних мереж, таких як глибокі нейронні мережі (DNN) і рекурентні нейронні мережі (RNN), ШІ здатний аналізувати великі обсяги даних, виявляючи складні закономірності та нелінійні залежності.

Застосування нейронних мереж у кібербезпеці включає аналіз аномалій, де ШІ здатний виявляти аномалії в мережевому трафіку, що можуть вказувати на потенційні загрози, аналізуючи мільйони пакетів даних у реальному часі. Прогнозування атак здійснюється за допомогою використання історичних даних для моделювання поведінки зловмисників та прогнозування нових сценаріїв атак.

Автоматична адаптація дозволяє системам самостійно коригувати політики безпеки залежно від змін у середовищі, наприклад, активуючи нові алгоритми шифрування або обмежуючи доступ до критичних ресурсів. Самонавчання забезпечує вдосконалення систем завдяки використанню технологій глибокого навчання, підвищуючи їхню стійкість до загроз, навіть тих, які раніше не існували.

Емерджентно-адаптивний метод базується на моделюванні загроз, створенні агентно-орієнтованих моделей для оцінки можливих впливів квантових атак на інформаційні системи. Оцінка вразливостей зосереджується на аналізі слабких місць у криптографічних системах, особливо тих, які базуються на класичних алгоритмах шифрування. Динамічна адаптація передбачає розробку механізмів реального часу для перемикання між класичними і постквантовими криптографічними протоколами.

Емерджентний аналіз ризиків вивчає каскадні ефекти компрометації однієї частини системи на всю інфраструктуру. Прогнозування майбутніх викликів включає форсайт-аналіз із використанням штучного інтелекту для передбачення нових загроз та довгострокового планування безпеки. Інтеграція синергії поєднує існуючі технології безпеки з новітніми постквантовими рішеннями для підвищення ефективності захисту.

Приклад можливого використання методу – найбільш вразлива у постквантовому середовищі система з високим ступенем емерджентності, як фінансова система (див. рис. 3). У фінансовій системі емерджентно-адаптивний метод може бути застосований для моделювання атак квантового комп'ютера, аналізу сценаріїв компрометації цифрових підписів у транзакціях, оцінки стійкості протоколів до атак квантовими алгоритмами, впровадження гібридного захисту через інтеграцію класичних і постквантових криптографічних рішень.

Також він дозволяє аналізувати ризики, вивчаючи вплив компрометації одного компонента на всю систему, і здійснювати довгострокове прогнозування, оцінюючи вплив квантових технологій через 5–10 років на фінансові транзакції та безпеку даних.

Рис. 3. Схема процесу застосування емерджентно-адаптивного методу в контексті фінансової системи для забезпечення інформаційної безпеки в умовах квантових загроз

Схема, представлена на рисунку 3, відображає процес застосування емерджентно-адаптивного методу в контексті фінансової системи для забезпечення інформаційної безпеки в умовах квантових загроз. Вона структурована у п’ять ключових компонентів, які послідовно та взаємопов’язано реалізують завдання оцінки ризиків, моделювання сценаріїв атак, впровадження криптографічних рішень та довгострокового прогнозування.

Перший елемент – моделювання атак з використанням квантових складних систем – охоплює аналіз можливих сценаріїв компрометації цифрових підписів у транзакціях. На цьому етапі створюються симуляції для оцінки потенційної загрози квантових обчислень на криптографічні механізми, які використовуються у фінансових системах.

Другий елемент, оцінка стійкості протоколів, передбачає тестування існуючих протоколів безпеки на предмет їхньої вразливості до атак з використанням квантових алгоритмів. Цей етап дозволяє визначити слабкі місця в системі шифрування та комунікацій.

Третій компонент, впровадження гібридного захисту, зосереджений на інтеграції класичних та постквантових криптографічних рішень. Він передбачає використання інноваційних схем шифрування, таких як решіткові алгоритми або кодові конструкції, для підвищення стійкості системи до новітніх загроз.

Четвертий елемент, аналіз ризиків, спрямований на вивчення впливу компрометації одного компонента на загальну інфраструктуру системи. Тут враховуються каскадні ефекти та розробляються механізми для зменшення можливого негативного впливу на ключові процеси.

П’ятий компонент – довгострокове прогнозування – забезпечує оцінку впливу квантових технологій на фінансову безпеку протягом 5–10 років. Цей етап включає форсайт-аналіз і розробку стратегій, які дозволяють адаптувати систему до майбутніх викликів.

Логічні зв’язки між компонентами схеми демонструють їхню взаємозалежність. Моделювання атак формує основу для оцінки стійкості протоколів, результати якої стають основою для інтеграції гібридного захисту. Гібридні рішення сприяють мінімізації ризиків, що, у свою чергу, інформує довгострокове прогнозування. Прогнозування ж генерує нові сценарії загроз, які знову враховуються при моделюванні.

Таким чином, представлена схема є інтегрованою структурою, яка забезпечує адаптивний підхід до захисту фінансової системи, дозволяючи не лише протистояти сучасним загрозам, але й передбачати виклики, спричинені еволюцією квантових технологій.

Математичне представлення схеми з урахуванням оцінки постквантового впливу на інформаційну безпеку фінансової системи можна застосувати для відображення взаємозв'язку між етапами моделювання, оцінки ризиків, впровадження криптографічних рішень та довгострокового прогнозування.

Позначимо основні компоненти схеми як змінні:

$M(t)$ – функція моделювання атак квантового комп'ютера на момент часу t. Вона враховує сценарії компрометації цифрових підписів.

$R(t)$ – функція оцінки стійкості протоколів, яка залежить від результатів моделювання та відображає поточну вразливість системи.

$H(t)$ – функція гібридного захисту, яка відображає ефективність інтеграції класичних і постквантових криптографічних рішень.

$V(t)$ – функція аналізу ризиків, що враховує можливі каскадні ефекти компрометації компонентів системи.

$F(t)$ – функція довгострокового прогнозування, яка оцінює вплив квантових технологій у перспективі.

Кожна функція залежить від попередніх етапів, що формує систему динамічних взаємозв'язків. Математична модель може бути представлена таким чином:

$M(t) = f_1(D, P, K)$, (1)

де D – дані про існуючі протоколи;

P – поточні параметри криптографії,

K – обчислювальна потужність квантових алгоритмів.

$R(t) = f_2(M(t), S)$, (2)

де S – набір специфічних параметрів, що характеризують криптографічну стійкість системи.

$H(t) = f_3(R(t), C)$, (3)

де C – набір криптографічних рішень, що включає класичні та постквантові методи.

$V(t) = f_4(H(t), L)$, (4)

де L – ймовірність каскадних збоїв у системі.

$F(t) = f_5(V(t), Q)$, (5)

де Q – прогнозований розвиток квантових обчислень у майбутньому.

Для оцінки загальної користі (U) від впровадження постквантового підходу враховується покращення всіх компонентів:

$$U = \int_{t_0}^{t_f} \left[\alpha_1 M(t) + \alpha_2 R(t) + \alpha_3 H(t) + \alpha_4 V(t) + \alpha_5 F(t) \right] dt, \quad (6)$$

де $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$ – вагові коефіцієнти, що визначають значущість кожного етапу в загальному контексті інформаційної безпеки.

Ця модель дозволяє оцінювати вплив кожного етапу процесу на загальну стійкість фінансової системи до постквантових загроз. Інтеграція показує сукупний ефект від застосування емерджентно-адаптивного методу у визначений проміжок часу. Вагові коефіцієнти можуть коригуватися залежно від пріоритетів захисту та специфіки середовища.

Майбутній розвиток емерджентно-адаптивного підходу включає створення формалізованих моделей емерджентності для прогнозування нових властивостей систем у квантовому середовищі, використання штучного інтелекту для форсайт-аналізу і довгострокового планування безпеки, інтеграцію квантових і класичних систем для забезпечення максимальної стійкості інформаційних систем. Передбачаються міждисциплінарні дослідження, які об’єднують криптографію, системний аналіз, квантові обчислення і кібербезпеку.

Емерджентно-адаптивний метод є перспективним інструментом для забезпечення інформаційної безпеки в умовах зростаючих викликів, спричинених розвитком квантових технологій. Він базується на принципах взаємодії складних систем, нових властивостях, що виникають завдяки їхній взаємодії, і здатності систем до адаптації та еволюції в умовах динамічних змін. Цей метод пропонує не лише виявляти і нейтралізувати існуючі загрози, а й прогнозувати нові сценарії атак, враховуючи непередбачувані наслідки впровадження квантових обчислень. Інтеграція постквантових технологій, динамічна адаптація до змін і активне використання штучного інтелекту для аналізу загроз роблять цей метод принципово новим у контексті державної інформаційної безпеки.

Основні результати. Основні результати роботи демонструють інноваційний підхід до формування політики інформаційної безпеки держави в умовах переходу на квантові технології. Розроблено алгоритм, що забезпечує багатоступеневий аналіз вразливостей, включаючи оцінку ризиків у реальному часі та впровадження новітніх рішень для підвищення стійкості інформаційних систем. Запропоновано використання емерджентних властивостей систем для створення самоадаптивних механізмів захисту, які здатні реагувати на нові загрози без необхідності зовнішнього втручання.

Особливу увагу приділено виявленню ефекту від інтеграції класичних і постквантових криптографічних протоколів, що дозволяє посилити захист даних за рахунок поєднання переваг обох підходів. Таким чином, впровадження запропонованого методу забезпечує динамічне та адаптивне реагування на виклики постквантового середовища, що є критично важливим для підтримки національної безпеки та захисту критичних інформаційних систем у сучасних умовах.

Емерджентний підхід, інтегрований у методики забезпечення інформаційної безпеки, відкриває нові перспективи для підвищення стійкості державних інформаційних систем в умовах переходу до квантових технологій. Його унікальність полягає у врахуванні складної взаємодії між компонентами системи, що дозволяє утворювати нові властивості для адаптації до непередбачуваних загроз. Застосування ШІ, зокрема нейронних мереж, не тільки підвищує здатність до аналізу великих обсягів даних, але й забезпечує автоматизоване прогнозування та динамічну адаптацію систем безпеки в режимі реального часу.

Новітні напрями розвитку цієї методики включають інтеграцію квантових обчислень для оптимізації механізмів виявлення загроз. Наприклад, квантові алгоритми здатні прискорити процеси ідентифікації аномалій у мережевому трафіку або виявлення складних моделей атак, які можуть залишатися невидимими для традиційних систем моніторингу. Перспективним є також поєднання емерджентних властивостей із гібридними моделями безпеки, де класичні, квантові та постквантові підходи синергетично працюють для створення багатоетапних бар'єрів проти атак.

Додатково перспективним напрямом є використання децентралізованих архітектур, таких як блокчейн, для забезпечення довіри у постквантових середовищах. Емерджентний підхід у цьому контексті може допомогти побудувати системи, де автономні елементи співпрацюють, забезпечуючи високу стійкість до спроб порушення цілісності даних.

Інший важливий вектор розвитку – впровадження емерджентних моделей в системи раннього попередження. Використовуючи штучний інтелект для моделювання потенційних сценаріїв атак, системи можуть прогнозувати нові типи загроз, базуючись на взаємодії різних компонентів кіберсередовища. Це дозволить розробляти не лише реактивні, а й проактивні стратегії захисту.

Подальше вдосконалення методики може включати інтеграцію з концепціями «цифрових двійників», які дозволяють симулювати функціонування системи в реальному часі, відстежуючи та прогнозуючи її вразливості. Це забезпечує ще більш високу адаптивність і здатність до самоорганізації, що є ключовим для кіберзахисту в умовах невизначеності.

Таким чином, запропонована методика має широкий спектр перспективних напрямів розвитку, що робить її одним із найбільш інноваційних підходів до забезпечення інформаційної безпеки в епоху квантових технологій.

Висновки та перспективи подальших досліджень. Основною перевагою методу є здатність з його допомогою прогнозувати майбутні ризики, що досягається через використання моделювання сценаріїв атак у постквантовому середовищі, а також можливість динамічної адаптації до нових викликів. Це дозволяє забезпечити не лише захист від відомих атак, але й створення системи, здатної до самонавчання і формування нових механізмів захисту.

На першому етапі проводиться аналіз потенційних векторів атак і вразливостей у державних інформаційних системах, зокрема оцінюється стійкість існуючих комунікаційних протоколів до квантових атак.

На другому етапі моделювання атак включає використання симуляцій квантових обчислень для оцінки ймовірності компрометації ключових компонентів системи.

Третій етап передбачає впровадження постквантових криптографічних рішень, таких як решіткові схеми, кодові алгоритми або багатоваріантні функції, з подальшим тестуванням і адаптацією до нових загроз.

Емерджентність у цьому підході проявляється у створенні нових властивостей системи, які неможливо звести до суми її компонентів, наприклад, формування самоорганізованих механізмів захисту. Адаптивність забезпечує динамічну перебудову систем залежно від змін у середовищі, включаючи активацію нових захисних алгоритмів або обмеження доступу до критично важливих ресурсів.

Інноваційність емерджентно-адаптивного методу полягає у використанні міждисциплінарного підходу, який об'єднує знання з квантових обчислень, кібербезпеки та системного аналізу. Він пропонує не лише технологічні, але й організаційні рішення, які включають створення стандартів постквантової безпеки, розробку довгострокових стратегій захисту та підготовку фахівців у цій галузі.

Майбутній розвиток цього методу передбачає створення формалізованих моделей емерджентності, які дозволять точніше оцінювати взаємодію компонентів системи і прогнозувати нові загрози. Використання штучного інтелекту для форсайт-аналізу і довгострокового планування також стане ключовим напрямом досліджень. Інтеграція постквантових криптографічних рішень у сучасні мережі, хмарні сервіси, IoT та VPN забезпечить ефективний захист критичних інформаційних систем.

Емерджентно-адаптивний підхід формує нову парадигму інформаційної безпеки, яка забезпечує довгострокову стійкість до викликів квантової епохи, зберігаючи цілісність, конфіденційність і доступність інформації в умовах постійних технологічних змін. Він відкриває нові можливості для міждисциплінарних досліджень і міжнародного співробітництва, створюючи фундамент для інтеграції новітніх технологій у державні системи захисту.

Список використаних джерел:

1. Allgyer, W., White, T., & Youssef, T. A. Securing the Future: A Comprehensive Review of Post-Quantum Cryptography and Emerging Algorithms. *Proceedings of IEEE SoutheastCon*. 2024. DOI: 10.1109/southeastcon52093.2024.10500031. URL: https://ircommons.uwf.edu/esploro/outputs/presentation/Securing-the-Future-A-Comprehensive-Review/99380555884006600

2. Alomari, A., & Kumar, S. Securing IoT systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions. *Internet of Things*. DOI: 10.1016/j.iot.2024.101132. 2024. URL: https://www.sciencedirect.com/science/article/abs/pii/S254266052400074X

3. Anantraj, I., Umarani, B., Karpagavalli, C., Usharani, C., & Lakshmi, S. J. Quantum Computing's Double-Edged Sword: Unravelling the Vulnerabilities in Quantum Key Distribution for Enhanced Network Security. *Proceedings of IEEE NELEX*. 2023. DOI: 10.1109/nelex59773.2023.10420896. URL: https://www.researchgate.net/publication/378277590_Quantum_Computing's_Double-Edged_Sword_Unravelling_the_Vulnerabilities_in_Quantum_Key_Distribution_for_Enhanced_Network_Security

4. Cyriac, R., Eswaran, S., & Selvarajan, S. Quantum Computing in Cryptographic Systems. *Journal ResearchGate Article*. 2024. DOI: 10.69942/1920184/20240101/03. URL: https://www.researchgate.net/publication/382165513_Quantum_Computing_in_Cryptographic_Systems

5. Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. Post-Quantum Cryptography for Embedded Systems. *Mexican International Conference on Computer Science*. 2022. DOI: 10.1109/ENC56672.2022.9882904. URL: https://ieeexplore.ieee.org/abstract/document/9882904

References:

1. Allgyer, W., White, T., & Youssef, T. A. (2024). Securing the Future: A Comprehensive Review of Post-Quantum Cryptography and Emerging Algorithms. Proceedings of IEEE SoutheastCon. DOI: 10.1109/southeastcon52093.2024.10500031

2. Alomari, A., & Kumar, S. (2024). Securing IoT systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions. Internet of Things. DOI: 10.1016/j.iot.2024.101132

3. Anantraj, I., Umarani, B., Karpagavalli, C., Usharani, C., & Lakshmi, S. J. (2023). Quantum Computing's Double-Edged Sword: Unravelling the Vulnerabilities in Quantum Key Distribution for Enhanced Network Security. Proceedings of IEEE NELEX. DOI: 10.1109/nelex59773.2023.10420896

4. Cyriac, R., Eswaran, S., & Selvarajan, S. (2024). Quantum Computing in Cryptographic Systems. Journal Article. DOI: 10.69942/1920184/20240101/03

5. Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2022). Post-Quantum Cryptography for Embedded Systems. Mexican International Conference on Computer Science. DOI: 10.1109/ENC56672.2022.9882904