DOI: https://doi.org/10.35681/1560-9189.2026.28.1.358608

УДК 004.2+004.7+519.8

О. Г. Додонов, М. Г. Кузнєцова, О. С. Горбачик
Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна

Інформаційні системи критичної інфраструктури в умовах сучасних загроз: підтримка функціональної стійкості

Розглянуто особливості інформаційних систем, що включені до критичної інфраструктури (КІ). Обґрунтовано залежність резильєнтності критичної інфраструктури від рівня функціональної стійкості та кібербезпеки інформаційних систем (ІС). Сформульовано завдання підтримки функціональної стійкості ІС КІ в умовах реалізації загроз і виникнення надзвичайної ситуації. Зроблено формалізований опис задачі забезпечення функціональної стійкості ІС КІ. Сформульовано та формалізовано задачу оцінювання функціональної стійкості інформаційної інфраструктури в умовах кібератак. Окрему увагу приділено інтелектуалізованим підходам до забезпечення функціональної стійкості ІС, зокрема протидії кібератакам із використанням сучасних методів організації, управління, зберігання та захисту даних, а також застосуванню технологій штучного інтелекту для підтримки функціональної стійкості ІС КІ.

Ключові слова: *критична інфраструктура, функціональна стійкість інформаційних систем, кібератака.*

Вступ

Критичні інфраструктури (КІ) є складно структурованими об’єктами, які характеризуються ієрархією, розподілом функцій і ресурсів, великою кількістю взаємодіючих елементів, блоків, підсистем і складною системою управління [1], до того ж їм притаманна взаємозалежність і взаємопроникнення.

Інформаційні системи (ІС) є компонентами будь-якої КІ. Інструменти ІС збирають, обробляють, передають, зберігають, відображають, документують і відтворюють інформацію для забезпечення функцій управління, підтримки стійкості, відновлення та розвитку КІ. ІС КІ повинні мати високу готовність, стабільність, мобільність, необхідну пропускну здатність мережі зв’язку, доступність, безпеку, керованість і забезпечувати дотримання вимог щодо своєчасності, надійності та безпеки обміну інформацією [2], оскільки вимоги до резильєнтності КІ стають дедалі більш

жорсткими на тлі зростаючої кількості складних гібридних загроз і пов'язаних з ними ризиків безпеки. Так, за статистикою щодня відбувається понад 2300 унікальних кібератак [3]. За прогнозами, до 2029 року збитки бізнесу від кіберзлочинності можуть сягнути 15,63 трлн доларів США [3].

В Україні фіксується близько 15 кібератак щодня. У 2025 році фахівці Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA опрацювали майже 6000 кібератак на державну та критичну інфраструктури, що на 37 % більше, ніж роком раніше, і вдвічі більше, ніж у 2022 році. [4]. Інциденти, що пов'язані з негативним впливом на ІС КІ, призводять до знищення інформаційних ресурсів, порушення регламентів процесу взаємодії, збоїв у стандартних інформаційних процедурах, зупинки виробництва на об'єктах КІ, порушення логістичних ланцюгів, спотворення управлінських рішень, тобто створюють загрозу стабільності функціонування КІ в цілому. Їх важко передбачити, вони зазвичай трапляються несподівано. Ймовірність ризику, пов'язаного з фізичними явищами, наприклад, відмову обладнання, можна визначити на основі накопичених статистичних даних, тоді як прогнозування реалізації кіберзагроз в ІС набагато складніше. Кібератаки різноманітні, відбуваються в різні періоди часу, на різні компоненти ІС та з різною періодичністю. Згідно з останнім звітом IBM «Вартість витоку даних», який обраховується як середній час, який необхідний для виявлення та стримування кібератаки, становить понад 200 днів, що ускладнює своєчасне реагування та мінімізацію збитків.

Забезпечення функціональної стійкості ІС КІ — основного інформаційно-комунікаційного активу КІ — є одним із шляхів підвищення резильєнтності КІ, прискорення реагування та відновлення функціонування КІ, скорочення тривалості перерв у обслуговуванні та мінімізації часу відновлення КІ після кібератак.

Особливості інформаційних систем критичної інфраструктури

ІС КІ являють собою складні системи з розподіленою багаторівневою структурою, що перебувають у постійній взаємодії одна з одною та із зовнішнім середовищем. Функціональність, надійність і безпека критично важливих об'єктів та інфраструктур залежать від якості функціонування ІС. КІ включають ІС операційного рівня об'єктів КІ, ІС рівня знань, ІС рівня управління та інформаційно-аналітичні системи стратегічного рівня.

ІС операційного рівня забезпечують оперативну обробку даних та управління виробничими процесами на об'єктах КІ. Системи рівня знань і управління (ІС середнього рівня, керівні ІС) орієнтовані на моніторинг стану КІ та окремих об'єктів КІ, контроль, розробку та прийняття управлінських рішень, адміністрування тощо. Інструменти цих ІС дозволяють відстежувати та порівнювати поточні показники ефективності інфраструктури з минулими, архівувати та надавати доступ до архівної інформації, створювати звіти за певний період часу тощо. ІС стратегічного рівня задіяні в довгостроковому плануванні, аналізі та прогнозуванні змін у середовищі функціонування об'єктів КІ, визначенні ресурсів для змін у функціонуванні КІ.

Функціональна стійкість ІС визначається як її здатність підтримувати свою структуру управління та продовжувати виконувати свої основні функції за призначенням, незважаючи на вплив потоків відмов, несправностей і збоїв [5]. Функціональна стійкість передбачає, що ІС має певний рівень надійності, відмовостійкості,

живучості та безпеки, і характеризує здатність системи протистояти змінам і бути стабільною. Функціонально стійка ІС гарантовано виконує основні функції за своїм призначенням, не має негативного впливу на навколишнє середовище та не становить загрози для його існування.

Результатом функціонування ІС КІ є складна система керуючих впливів різноманітної фізичної природи, прямої та опосередкованої дії, різної інтенсивності, тривалості та періодичності, на об'єкти управління. У разі появи негативних впливів засоби ІС КІ забезпечують:

1) моніторинг — безперервну обробку даних у режимі реального часу від об'єктів КІ та генерування сповіщень, коли певні параметри перевищують допустимі межі;

2) діагностику, спрямовану на виявлення та локалізацію зон несправності або помилки;

3) прогнозування потенційних наслідків подій або явищ на основі аналізу даних з різних джерел;

4) планування дій і розподілу ресурсів для запобігання інцидентам і зменшення загроз;

5) коригування управлінських рішень при виявленні інцидентів, помилок або збоїв;

6) контроль об'єктів КІ та КІ в цілому, включаючи встановлення відповідного режиму функціонування самої ІС;

7) інформаційну взаємодію в КІ.

В умовах реалізації загроз, виникнення надзвичайної ситуації (НС) у КІ та у функціонуванні ІС виникають проблеми, що пов'язані з високою швидкістю змін стану об'єктів КІ, непередбачуваністю подій, залежністю інформаційних потоків від ситуації, змінами розподілу функцій, розширенням або звуженням сфери дій тощо. Ситуація ще більше ускладнюється тим, що реакція об'єкта управління (критичної інфраструктури) на зовнішні керуючі впливи й інші зовнішні та внутрішні збудження, враховуючи здатність КІ, як системи, до самоорганізації, є апріорі відомою та передбачуваною лише певною мірою.

Зазначені особливості ІС КІ та КІ призводять до того, що стан цих систем у будь-який момент часу та перелік їхніх характеристик, що його відображають, і повнота такого відображення, є значною мірою невизначеними. Отже, для ІС КІ і в цілому КІ характерним є висока ступінь невизначеності щодо вхідних зовнішніх впливів, керуючих впливів, стану системи управління, стану об'єктів управління, і це робить малопродуктивними спроби точного визначення повного вектора їхнього стану та функціонального опису взаємодії як між ними, так і із зовнішнім середовищем. Водночас, забезпечення функціональної стійкості ІС вимагає розробки структури (моделі) можливих станів ІС, які є критично важливими для підтримки функціональної стійкості, тобто формування кінцевого переліку загроз функціональній стійкості ІС та опису кожної з них. Зрозуміло, що перелік загроз не може бути сталим у часі. Він потребує періодичного перегляду, що може призводити як до збільшення, так і зменшення їхньої кількості. Загрози можуть бути незалежними або мати причинно-наслідкові зв'язки. Зазвичай побудова моделей загроз у більшості випадків є процесом формування їхнього переліку із зазначенням джерел кожної загрози, способів її реалізації, об'єктів впливу та деструктивних властивостей,

а також проведення оцінок її небезпечності для конкретної системи. На практиці для формування таких переліків загроз найчастіше використовуються експерт-ні методи. Перегляд (або повторна оцінка) переліку загроз повинна проводитися принаймні у таких випадках:

— виявлення нових уразливостей системи (внутрішні причини);

— виявлення (поява) нових можливостей для «порушників» або факторів навколишнього середовища (зовнішні причини);

— поглиблення знань про систему (накопичення досвіду експлуатації) або її зовнішнє середовище.

Формуючи перелік загроз функціональній стійкості ІС і виконуючи їхній опис (фактично, створення моделей), необхідно визначити параметри та характеристики ІС, що призводять до виникнення тієї чи іншої загрози. Моніторинг цих параметрів (їхніх показників) дозволить визначити можливість виникнення, подальшого розвитку або послаблення загрози. Звичайно, до переліку таких параметрів доцільно включати лише ті, які можна виміряти (визначити) тим чи іншим способом (прямим чи непрямим). Логічно припустити, що однакові параметри, але (у загальному випадку) з різними значеннями, відповідатимуть різним загрозам.

Як показують дослідження, загальною особливістю параметрів і факторів (впливів зовнішнього середовища), що визначають стан, умови функціонування та загрози функціональній стійкості ІС КІ є притаманна їм різного роду невизначеність, яка стосується:

— форми їхнього існування (вираження);

— різнорідності даних, що потребують спільної обробки;

— відповідності значень показників дійсним характеристикам ІС і КІ;

— спроможності показників у сукупності відображати стан ІС КІ;

— можливості одночасного надходження різних значень одних і тих самих показників від різних джерел.

Завдання підтримки функціональної стійкості інформаційних систем критичних інфраструктур

Розглянемо деяку інформаційну систему Ω у складі КІ, функціональна стійкість якої має бути забезпечена. Здійснимо декомпозицію ІС Ω за функціональною ознакою. Результатом декомпозиції буде певна сукупність, відносно самостійних функціональних підсистем $\Omega = \{\Theta_i\}, i = \overline{1,n}$, що мають мінімальну кількість зв'язків між собою. Кожна підсистема Θ_i виконує деяку унікальну в рамках системи Ω функцію.

Можлива подальша декомпозиція підсистем Θ_i з метою визначення переліку «стандартних» функцій і типових технічних та інших ресурсів для їхньої реалізації. Серед Θ_i є підсистеми Θ_j^*, що виконують певну цілісну функцію, подальша декомпозиція якої недоцільна для дослідження системи Ω. Виокремлення цих підсистем є важливим щодо питань моніторингу показників, які характеризують процес функціонування системи Ω. Зазвичай підсистеми Θ_j^* виконують забезпечувальні функції, що не входять до цільової функції системи. Моніторинг показників ефектив-

ності таких підсистем виконується для розуміння «руху» підсистеми в бік «старіння» та припинення функціонування.

Для усіх інших функціональних підсистем $\{\Theta_i\}\backslash\{\Theta_j^*\}$, доцільно здійснювати подальшу декомпозицію з метою виявлення груп однорідних та унікальних елементів у кожній підсистемі. Під однорідними елементами підсистеми будемо розуміти близькі (подібні) за змістом «елементарні функції», а також типові технічні засоби та персонал одного рівня кваліфікації. У межах однорідних груп перерозподіл функціональності виконується просто, без суттєвих втрат в ефективності системи Ω в цілому. Наявність резервних елементів у цих групах дозволяє здійснювати перерозподіл практично «непомітно» для функціонування системи Ω. Стосовно персоналу замість резервних елементів доречно говорити про додаткові трудові ресурси, які можна «накопичити» не лише за рахунок залучення додаткових працівників, а й завдяки переходу наявного персоналу на більш інтенсивний режим роботи.

Слід зазначити, що однорідні елементи не обов'язково знаходяться лише в межах однієї підсистеми. Такі елементи можуть міститися одночасно і різних підсистемах. І у цьому випадку «вільні» елементи деяких функціональних підсистем можуть бути передані «для використання» підсистемам, які зазнали втрат. Контроль за працездатністю однорідних елементів у найпростішому випадку можна звести до визначення факту їхньої працездатності в певні моменти (або інтервали) часу: «працездатний» або «непрацездатний». Такий показник у більшості випадків можна виміряти технічними засобами. Стосовно персоналу показник працездатності також можна «виміряти» технічними засобами, наприклад, системами контролю прибуття та/або присутності на робочому місці.

Унікальні елементи підсистем реалізують унікальну (специфічну) «елементарну функцію», передача їхньої функції іншим елементам практично неможлива, і тому для забезпечення функціональної стійкості системи Ω необхідно мати резервні унікальні елементи. За умови наявності резервних елементів, моніторинг показників унікальних елементів системи також може зводитися до визначення факту їхньої працездатності в певні моменти часу.

До особливого типу унікальних елементів системи можна віднести експертні, аналітичні або діагностичні підсистеми, функціонування яких необхідно для підтримки працездатності ІС та КІ в цілому. Результатом їхньої роботи є формування певною мірою суб'єктивних узагальнених показників. Ці системні показники, що перебувають у певному взаємозв'язку, створюють основу для моніторингу стану системи Ω і виявлення існуючих загроз стабільності її функціонування.

Після втрати резервних ресурсів підсистем система втрачає функціональну стійкість, і її подальша адаптація до поточних умов експлуатації може здійснюватися шляхом відмови від деяких «елементарних функцій», відсутність виконання яких мінімально впливає на цільову функцію системи Ω або відкладає такий вплив на деякий час. Однак, слід зазначити, що можлива ситуація, коли якась «елементарна функція» однієї з підсистем, яка мало впливає на її функції, може суттєво впливати на функції іншої підсистеми, з якою вона взаємодіє. Тому бажано, щоб деградація функціональності окремих підсистем здійснювалася під певним «контролем зверху», перш за все, для уникнення так званого ефекту «доміно», коли втрата функції окремої підсистеми може призвести до каскаду виведення з робочого стану

великої кількості інших елементів або навіть підсистем КІ. Доцільно мати заздалегідь розроблені сценарії як такої функціональної деградації ІС чи інших складових КІ, так і різних ситуацій дефіциту ресурсів.

Необхідно також вести моніторинг факторів впливу зовнішнього середовища, оскільки це дозволить заздалегідь виявити групу/групи елементів системи (або зв'язків між ними), які вразливі і можуть зазнати руйнівного впливу зовнішнього фактора, та своєчасно відреагувати. Це також спростить завдання визначення переліку можливих факторів, що призвели до цього, та виявлення конкретного фактора руйнівного впливу, який потрібно нейтралізувати.

Складові КІ можуть мати власні засоби впливу на зовнішнє середовище для покращення умов функціонування КІ. Такі засоби є важливим, а іноді й засадничим елементом забезпечення функціональної стійкості складових КІ та в цілому резильєнтності КІ.

Завдання формування моделей виявлення загроз функціональній стійкості ІС КІ можна розглядати як задачу розпізнавання. У процесі моніторингу стану ІС КІ визначається ступінь відповідності поточного стану ІС опису певної загрози її функціональної стійкості. Моделі загроз мають бути сформовані та описані заздалегідь, а набір показників функціонування ІС КІ слід розглядати на відповідність виявленим ознакам загрози. Методи розпізнавання забезпечують якісні результати, коли об'єкти розпізнавання значно «рознесені» в просторі ознак. Коли простір ознак загроз перекривається, тобто образи загроз схожі, складність правильного розв'язання задачі розпізнавання зростає.

Складність формалізації залежностей між окремими показниками функціонування ІС КІ та можливістю виникнення певних загроз призводить до того, що для ідентифікації загроз найбільш доцільно проводити процедуру нечіткого розпізнавання. Крім того, неповнота інформації про загрози та даних про їхні характеристики породжує різного роду інформаційні невизначеності як щодо самої загрози, об'єкта розпізнавання, так і «образу» об'єкта, отриманого системою моніторингу стану функціонування ІС КІ. Тому, в строгому сенсі, задача розпізнавання стає нечіткою за визначенням.

Завдання розпізнавання загроз для ІС КІ загалом включає два етапи: І етап — формування шаблонів загроз, ІІ етап — ідентифікації («розпізнавання») загрозливих щодо функціональної стійкості станів ІС КІ.

На І етапі необхідно визначити множину можливих (передбачуваних) загроз Z. Загрози з цієї множини можуть перебувати в різних ієрархічних зв'язках, проте визначення цих зв'язків не є важливим для формування шаблонів, але є важливим для вирішення задачі залучення та розподілу ресурсів для нейтралізації загроз.

Для кожної загрози $z_t \in Z$ має бути визначена вичерпна множина ознак M_t, що характеризує її та є підмножиною множини ознак, доступних для спостереження підсистемою моніторингу. Після цього множину загроз Z розділяємо на підмножини так, щоб загрози з різних підмножин не перетиналися за переліком ознак, що їх визначають, або перетиналися таким чином, щоби перелік ознак загроз однієї підмножини не був підмножиною переліку ознак загроз іншої. Усі загрози однієї підмножини вважатимуться однотипними. Для однотипних загроз можна розробити типові рішення щодо реагування та нейтралізації. Для кожної підмножини загроз $Z_j \subset Z$ можна визначити ступінь небезпеки для функціонування ІС КІ.

Повний список ознак $\mathcal{M}_j$ для підмножини загроз Z_j , де $j \in [1; J]$, формується шляхом об'єднання наборів ознак M_t усіх загроз цієї підмножини. Потім для кожної загрози з підмножини Z_j визначається множина можливих значень ознак з множини $\mathcal{M}_j$. На множині можливих значень визначається ступінь відповідності кожного значення кожній загрозі підмножини Z_j (відповідність її існуванню, виникненню (актуалізації)). Далі відбувається формалізація — створення моделі загрози, що являє собою завдання агрегації ознак (як правило, агрегація ієрархічна) в інтегральний показник (ознаку) виникнення (існування) загрози. Фактично, на I етапі вирішення задачі розпізнавання загроз ІС КІ відбувається формування нечітких моделей (шаблонів) загроз на основі набору ознак, що їх визначають і піддаються моніторингу. Усі загрози з будь-якої підмножини $Z_j \subset Z$, $j \in [1; J]$ описуються ідентичною множиною різнорідних у загальному випадку ознак.

I етап слід виконати заздалегідь. У процесі функціонування конкретної ІС КІ може бути уточнений як перелік загроз, так і показники, що визначають загрози, і спосіб агрегування показників в ознаку існування загрози.

На II етапі виконання завдання розпізнавання загроз ІС КІ, етапі «розпізнавання» станів ІС КІ, перехід у які призведе до зниження, або навіть втрати, функціональної стійкості, перевіряється, чи входить кожний показник, отриманий завдяки моніторингу, до множин ознак загроз $\mathcal{M}_j$. Якщо «так» — значення показника подається як «вхід» до підмножини шаблонів загроз Z_j. Якщо «ні» — показник ігнорується. У заздалегідь визначеному темпі, відбувається агрегування множини отриманих ознак за шаблоном кожної із загроз конкретної підмножини з отриманням значення ознаки виникнення (існування) загрози. Динаміка агрегування значень показників функціонування ІС КІ залежить від можливої швидкості прийняття управлінських рішень у системі. Для окремих груп загроз (або загроз у групах), що становлять значну небезпеку для функціонування ІС КІ та мають швидкий розвиток у часі, вимагається максимально можлива швидкість визначення стану загрози.

Розглянемо створення нечітких еталонів загроз.

Після визначення переліку характерних ознак загрози, їх формалізують у вигляді нечітких множин $\{x, \mu(x)\}$, носіями яких виступають чіткі множини можливих значень ознаки $x \in X$. Функція належності $\mu(x)$ кожної нечіткої множини має відображати ступінь відповідності конкретного значення ознаки x чіткої множини X загрозі, для якої формується шаблон (еталонний опис). Наступним кроком є визначення вагових коефіцієнтів кожної ознаки з позиції її внеску в ідентифікацію (виявлення) саме цієї загрози. Необхідно обрати модальність агрегування, тобто спосіб їхньої згортки в єдину інтегральну ознаку загрози. Наприклад, якщо загрозу можна ідентифікувати за наявності хоча б одної з ознак, модальність згортки має наближатись до логічної операції «АБО». Якщо ж встановлення факту загрози потребує врахування всіх ознак, доцільною є модальність, близька до логічного «І». В інших випадках модальність агрегування визначається як компроміс між цими граничними підходами.

Запропонований еталонний опис загрози є дворівневим, а саме, на першому рівні відбувається визначення окремих ознак на множині їхніх можливих значень, а на другому — формування інтегральної ознаки загрози шляхом їхньої згортки. У загальному випадку опис загрози може мати багаторівневу структуру:

— на нижчому рівні формуються множини можливих значень окремих ознак загрози, які зіставляються з їхніми конкретними реалізаціями;

— на другому рівні виконується згортка окремих ознак у комплексні ознаки вищого рівня.

— на подальших рівнях комплексні ознаки послідовно агрегуються у ще більш узагальнені характеристики аж до отримання інтегральної ознаки загрози.

На кожному рівні для згортки використовується один і той самий нечіткий інтеграл, але з різною модальністю, що відображає характер агрегування ознак [6]. Загалом, за допомогою нечіткого інтеграла можна реалізувати різні модальності згортки, впорядковані за їхнім посиленням [6]: «можливість», «подібність», «імовірність», «довіра», «необхідність». Такий спектр модальностей дозволяє наблизити зміст інтегральних оцінок до інтуїтивного сприйняття і експертних уявлень людини.

Важливим є питання визначення такого рівня відповідності сукупності виявлених ознак еталонному опису загрози, який дає підстави стверджувати, що загрозу виявлено. Рішення про достатність рівня відповідності залежить від якості еталонного опису (його точності та повноти), достовірності даних моніторингу, ступеня подібності (близькості в описі) між різними типами загроз, а також вартості помилок класифікації (як хибного віднесення, так і невіднесення поточного образу до відомих класів загроз. Ось чому задача визначення достатнього рівня відповідності для розпізнавання загрози зазвичай покладається на експерта, його досвід і знання. Однак, слід зазначити, що в процесі практичного застосування підходу, за умови накопичення достатнього обсягу статистичних даних, стає можливим формування чіткої або нечіткої шкали для автоматичного вирішення цієї задачі, зокрема із використанням методів штучного інтелекту.

Формалізація задачі оцінювання функціональної стійкості інформаційної інфраструктури в умовах кібератак

Прогнози масштабів можливої шкоди об’єктам КІ при реалізації різних загроз зазвичай базуються на апріорних оцінках потенціалу загрози. Ризик для КІ тим вищий, чим більший потенціал має загроза. Численні атаки на ІС КІ є значущим фактором порушень функціонування КІ. Завдання забезпечення кібербезпеки КІ як захисту від кібератак і забезпечення функціональної стійкості ІС КІ в умовах кібератак стало надзвичайно актуальним.

Інформаційно-комунікаційна інфраструктура КІ являє собою складну сукупність взаємопов’язаних компонентів, частина з яких є вразливою до кібератак, зокрема ІС КІ. На етапі проєктування для кожного компонента передбачаються спеціалізовані засоби захисту, спрямовані на мінімізацію впливу деструктивних чинників. Більш того, вимоги до резильєнтності КІ зумовлюють необхідність інтеграції до складу інформаційно-комунікаційної інфраструктури системи відновлення функціонування, яка має певний, хоча й обмежений, ресурс. Така система забезпечує реагування на ураження будь-якої складової інфраструктури та, використовуючи наявні ресурси, здійснює її відновлення, що, у свою чергу, дозволяє відновити функціонування інформаційно-комунікаційної інфраструктури КІ в цілому.

Припустимо:

ΔT — період часу від початку до кінця негативного впливу, зокрема кібератаки;

$\Delta T = (0, T]$, де T — момент часу, коли кібератака завершилася;

$\mathfrak{h} = \{F, N, T\}$ — характеристики кібератаки;

$F = \{F_i(t)\}$, де $F_i(t)$ — функція розподілу випадкового η_i-го інтервалу часу до початку i-ї кібератаки, $i = \overline{1, N}$, N — кількість кібератак;

$\mu = \{T_{rec}, S\}$ — показник функціональної стійкості певного j-го компонента інформаційно-комунікаційної інфраструктури КІ, який характеризує здатність відновити порушену функціональність компонента внаслідок реалізованої i-ї кібератаки;

$T_{rec} = \{\tau_i^{low}, \tau_i^{up}\}$ — множина нижнього τ_i^{low} та верхнього τ_i^{up} значень часових інтервалів для відновлення функціональності j-го компонента (оцінки τ_i^{low} та τ_i^{up}, що отримані або за допомогою експертних методів, або шляхом проведення спеціальних досліджень);

$S = \{S_i(t)\}$, $i = \overline{1, N}$ — множина функцій розподілу випадкових часових інтервалів відновлення функціональності компонента після i-ї кібератаки;

$\wp$ — множина показників функціональної стійкості компонентів φ, яка характеризує здатність компонента зберігати свою функціональність після відбиття кібератаки.

$\wp = \{p_i\}$, $i = \overline{1, N}$, N — кількість кібератак, p_i — ймовірність пошкодження компонента під час i-ї кібератаки (отримана або за допомогою експертних методів, або в результаті статистичного моделювання);

$K_{or}(u, t) = K_r(u)P(t, \Delta T)$ — коефіцієнт нестаціонарної робочої готовності компонента, який визначається ймовірністю безвідмовної роботи компонента під час реалізації кібератаки та ліквідації наслідків;

u — показник надійності та відновлюваності компонента інформаційної інфраструктури КІ за нормальних умов експлуатації;

$K_r(u)$ — коефіцієнт доступності компонента, розрахований для стандартних умов;

$P(t, \Delta T)$ — ймовірність безвідмовної роботи компонента протягом періоду часу ΔT, де $\Delta T = (0, T]$.

Функціональна стійкість компонента інформаційно-комунікаційної інфраструктури КІ в умовах кібератак може бути охарактеризована функцією $\varphi(t, \mathfrak{h}, \mu, \wp)$, середнє значення якої на інтервалі ΔT [7]:

$$\varphi_{\text{с}} = \frac{1}{T}\int_0^T \varphi(\ t, \mathfrak{h}, \mu, \wp)dt.$$

Для оцінки функціональної стійкості компонента інформаційно-комунікаційної інфраструктури КІ може бути використаний показник, який характеризує ймовірність перебування компонента в стані повної функціональності в будь-який момент часу $t \in (0, T]$ [7]:

$$\kappa_\varphi = \lim_{\substack{t \to T \\ n \to N}} \varphi(t, \mathfrak{h}, \mu, \wp),$$

T та N — максимально можливий момент реалізації набору кібератак і максимальна прогнозована кількість кібератак у наборі — визначаються, відповідно, за допомогою експертних методів.

Щодо практичного застосування запропонованої оцінки функціональної стійкості слід зазначити, що обчислення показників κ_φ із використанням методів статистичного моделювання є ресурсо- та часозатратним. Унаслідок чого існує ризик отримання оцінки із запізненням, коли вона втрачає актуальність для прийняття управлінських рішень. До того ж, проблема забезпечення належної достовірності такої оцінки потребує додаткового дослідження та обґрунтування.

Для ідентифікації загрозливих для функціональної стійкості ІС станів необхідно однозначно визначити, який стан системи за сукупністю ознак (параметрів) належить до класу загрозливих. Доцільно застосовувати метод ідентифікації, що базується на покроковому аналізі ознак стану системи. Стан ІС можна розглядати як деякий інформаційний об'єкт (ІО). Кожний ІО має образ, що являє собою впорядкований набір ознак, які з певною повнотою характеризують його. Процедура ідентифікації ІО зводиться до зіставлення його ознак з еталонними, заданими у запиті на ідентифікацію. Якщо ознаки ІО з необхідною та достатньою мірою узгоджуються з еталонними (з можливим використанням семантичних запитів або нечітких мір близькості), вважається, що ІО ідентифіковано.

Формально множину інформаційних об'єктів θ, що визначають загрозливі стани ІС КІ, можна подати у вигляді: $\theta = \{IO_1, IO_2, \dots, IO_m\}$, де ІО описується вектором ознак (P_1, P_2, …, P_n). Усі ІО мають однакову розмірність простору ознак, однак на практиці можливі ситуації неповноти даних — відсутності значень окремих ознак, що зумовлено обмеженою доступністю відповідних параметрів для засобів моніторингу. Кожний ІО вважається унікальним, тобто множина θ не містить однакових об'єктів.

Слід зазначити, що універсальної технології формування множини загрозливих станів ІС КІ на сьогодні не існує. Конкретні підходи визначаються предметною областю, особливостями функціонування системи та її програмно-апаратною реалізацією. Водночас при побудові таких множин, як правило, враховуються базові системні принципи: структурна декомпозиція ІС КІ на підсистеми; багаторівнева ієрархічна організація, що поєднує централізовані та децентралізовані механізми управління; а також принцип необхідного розмаїття, відповідно до якого функціонально складна система не може бути реалізована на основі спрощеної структури чи однорідних елементів.

Протидія загрозам різної природи, зокрема і кібератакам, у сучасній інформаційно-комунікаційній інфраструктурі КІ здійснюється як на рівні окремих компонентів, так і спеціальними засобами програмно-апаратних платформ.

Інтелектуалізовані підходи до забезпечення функціональної стійкості інформаційних систем критичних інфраструктур

Функціональна стійкість інформаційно-комунікаційної інфраструктури КІ визначається рівнем розвитку та надійності впроваджених інформаційних технологій. Їхня надійність і безпека значною мірою залежать від організації обробки користувацьких запитів (з боку посадових осіб і персоналу), забезпеченості необхід-

ними обчислювальними та комунікаційними ресурсами, а також відповідністю цих ресурсів виконуваним завданням, потік яких доцільно розглядати як зовнішній відносно ІС. Порушення в процесах обслуговування запитів можуть бути спричинені не лише відмовами або несправностями технічних засобів, але й перевантаженням ІС, дефіцитом ресурсів чи їхнім нераціональним розподілом. Наслідками таких порушень є втрата запитів або перевищення допустимих часових меж їхньої обробки. Невиконання запиту в заданий інтервал часу може вважатися збоєм у функціонуванні інформаційно-комунікаційної інфраструктури або її окремих компонентів. Отже, врахування критичних затримок обслуговування є важливим в оцінюванні функціональної стійкості ІС КІ з огляду на те, що ці системи, як правило, функціонують у режимі реального часу, де перевищення гранично допустимих затримок є неприпустимим і можливості повторного виконання функцій після збоїв, а також реалізації повноцінних процедур відновлення є суттєво обмеженими.

Завдання забезпечення функціональної стійкості ІС, а отже й інформаційно-комунікаційної інфраструктури КІ, доцільно формулювати як загальносистемне вже на етапі проєктування, коли традиційно передбачається впровадження різних видів резервування (структурного, програмного, часового, ресурсного), створення вбудованих систем керування та механізмів захисту, а також відбувається добір компонентів із підвищеними показниками надійності та безпеки. Зазначені рішення загалом сприяють підвищенню функціональної стійкості ІС за умов дії відомих дестабілізуючих факторів, оскільки орієнтовані на врахування типових станів системи та передбачуваних реакцій її елементів. Водночас їхні можливості є обмеженими. Так, нарощування резервування неминуче супроводжується погіршенням техніко-економічних характеристик системи. Вбудовані системи керування забезпечують моніторинг визначеного набору параметрів, проте не завжди здатні сформувати адекватну реакцію на аварійні ситуації і, як правило, не впливають на ймовірність їхнього виникнення. Захисні механізми дозволяють знизити вплив прогнозованих зовнішніх факторів, однак не усувають їх повністю. Використання елементної бази з підвищеними показниками надійності підвищує відмовостійкість ІС, але не гарантує функціональної стійкості в умовах уже реалізованих відмов. Таким чином, забезпечення функціональної стійкості потребує комплексного підходу, що виходить за межі традиційних інженерних рішень і передбачає здатність системи адаптуватися до непередбачуваних впливів і зберігати працездатність у динамічно змінних умовах функціонування.

Якість і безпека функціонування інформаційно-комунікаційної інфраструктури критичної інфраструктури суттєво залежать від впровадження сучасних технологій, зокрема засобів управління даними, хмарних сервісів і технологій штучного інтелекту.

Аналіз інцидентів в ІС КІ свідчить, що у більшості випадків початковий несанкціонований доступ до ресурсів системи отримується заздалегідь, через використання скомпрометованих VPN-акаунтів, а також унаслідок помилок конфігурації та/або наявності вразливостей програмного забезпечення. Зокрема, у першому кварталі 2024 року в Україні було зафіксовано 15 інцидентів, під час яких застосовувалися п’ять типів шкідливого програмного забезпечення: Remcos RAT, QuasarRAT, Venom RAT, Remote Utilities та Lummastealer. Масштаб атак і характер використаних інструментів, що базуються на викрадених облікових даних, дозволяють

припустити, що компрометація автентифікаційної інформації є головною передумовою несанкціонованого доступу до ІС КІ. Тому пріоритетного значення набуває комплексний захист даних ІС КІ, що охоплює забезпечення їхньої надійності, цілісності та конфіденційності на всіх етапах життєвого циклу — від збору та передавання до обробки, аналізу та зберігання із використанням сучасних криптографічних механізмів, технологій маскування даних у процесах їхнього передавання та міграції, а також запровадження жорстких політик і процедур управління доступом до інформаційних ресурсів.

В умовах сучасних комплексних і гібридних загроз традиційна периметральна система безпеки для КІ стає недостатньою. Виникає необхідність впровадження додаткових засобів безпеки як на рівні всієї інфраструктури, так і з акцентом на безпосередній захист даних, а не окремих програмних компонентів і технічних засобів. Доцільним стає застосування інформаційно-орієнтованої моделі безпеки (Data-Centric Security, DCS), яка передбачає формування політик захисту залежно від цінності даних, тобто адаптивно визначати рівень і засоби захисту з урахуванням критичності інформаційних ресурсів. Використання інструментів аналітики даних і методів машинного навчання для класифікації даних та виявлення аномальної або підозрілої активності користувачів дозволяє підтримувати необхідний рівень захисту в умовах роботи з різнорідними пристроями та динамічними потоками даних. Оцінювання цінності даних має здійснюватися на регулярній основі, оскільки цінність даних змінюється з часом і залежить від контексту їхнього використання. Модель DCS орієнтована на захист критично важливих даних на всіх етапах їхнього життєвого циклу. Її реалізація передбачає застосування криптографічних методів, технологій маскування даних у процесі їхнього переміщення, а також запровадження жорстких механізмів контролю та регламентації доступу для авторизованих користувачів.

Поява нових класів задач, пов’язаних із багатовимірним аналізом даних, потоковою аналітикою, інформаційними сховищами, соціальними мережами та Інтернетом речей, стимулювала розвиток технологій управління даними. Кожний із цих класів висуває специфічні вимоги до інструментів обробки і зберігання, що зумовлює появу нових систем управління даними. Основними підходами до організації універсальних платформ управління даними є мультимодельні системи та інтегровані платформи, які забезпечують роботу з різнорідними типами даних у межах єдиного середовища. Існує широкий спектр рішень класів SQL, NoSQL та NewSQL, орієнтованих як на операційну, так і на аналітичну обробку даних в межах сховищ даних (Data Warehouse), озер даних (Data Lake) та хмарних платформ [8]. Сучасні застосування характеризуються обробкою великих обсягів різнорідних даних і потребують високої продуктивності, масштабованості та належного рівня безпеки. Системи різних класів реалізують відмінні підходи до захисту структурованих, напівструктурованих і неструктурованих даних.

Системи управління даними класу SQL, що побудовані на реляційній моделі, традиційно застосовуються для задач онлайн-обробки транзакцій (OLTP) та аналітичної обробки (OLAP) у межах класичних сховищ даних. Вони добре працюють із фіксованими схемами даних і забезпечують їхню цілісність завдяки використанню обмежень і тригерів, підтримуючи виконання транзакцій відповідно до принципів ACID (Atomicity, Consistency, Isolation, Durability / атомарність, узго-

дженість, ізоляція, довговічність). Виконання обчислювальних процедур безпосередньо в межах бази даних дозволяє мінімізувати обсяги передавання даних. Висока доступність досягається за рахунок реплікації і розподілу даних між носіями, тоді як підвищення продуктивності традиційно забезпечується переважно за рахунок вертикального масштабування.

Традиційні SQL-системи мають обмеження у сфері застосування, зумовлені жорсткістю схем даних, підвищеними затримками виконання запитів у масштабних середовищах, недостатньою пристосованістю до роботи з неструктурованими даними, а також складністю реалізації ефективного горизонтального масштабування. Подолання цих обмежень пов'язане з використанням NoSQL-систем, що є розподіленими, як правило, нетранзакційними платформами управління даними. Такі системи забезпечують ефективне горизонтальне масштабування із залученням великої кількості однотипних серверів, підтримують гнучкі (динамічні) схеми та спеціалізовані моделі даних, а також демонструють високу продуктивність при обробці значних обсягів неструктурованої інформації, що надходить у режимі реального часу. СУБД класу NoSQL можуть не відповідати строгим вимогам ACID, використовуючи модель BASE (базова доступність, м'який стан, остаточна узгодженість), що передбачає компроміс між узгодженістю та доступністю даних.

Подальший розвиток технологій управління даними — поява СУБД класу NewSQL, сучасних реляційних СУБД (Clustrix, VoltDB, MemSQL, NuoDB, MySQL Cluster, TokuDB, Spanner), які поєднують переваги класичних SQL-рішень і NoSQL-підходів. Вони орієнтовані насамперед на OLTP-обробку як структурованих, так і частково неструктурованих даних, підтримують SQL як основну мову взаємодії і надають доступ до інструментарію традиційних реляційних систем. Висока продуктивність таких систем досягається завдяки використанню оперативної пам'яті та сучасних носіїв даних, зокрема флеш-пам'яті (SSD), як основного середовища зберігання.

Еволюція функціональних можливостей NoSQL- і NewSQL-рішень сприяла їхній поступовій конвергенції і появі багатомодельних СУБД, що забезпечують уніфіковану роботу з різними моделями даних і дозволяють розв'язувати задачі, які пов'язані з узгодженістю, перетворенням і захистом даних у гетерогенних інформаційних середовищах [9].

Сьогодні можливо використовувати інтегровану платформу управління даними, яка складається з інфраструктурної платформи, платформи зберігання структурованих та неструктурованих даних, а також платформи обробки даних. Це надає можливість вибору різноманітних інструментів обробки даних для різних завдань на основі однієї платформи. Прикладами є програмні пакети для розгортання, моніторингу та управління кластером Enterprise Hadoop, такі як Hortonworks Data Platform (HDP), IBM BigInsight, Arenadata Hadoop (ADH). Інтегрована платформа включає поточні стабільні версії усіх найпопулярніших інструментів, таких як Apache Hive, Apache Spark та Apache Atlas, а також інструменти для забезпечення правильної інтеграції цих інструментів один з одним [9].

Компанія Oracle випустила варіанти СУБД Oracle Autonomous Database та Oracle Autonomous Data Warehouse з можливостями самокерування, самозахисту та самовідновлення, які дозволяють автоматично виявляти та усувати загрози під час роботи СУБД. Система безпеки СУБД автоматично розпізнає загрози, такі як

можливість крадіжки даних, і відповідно налаштовує СУБД. Усі планові та профілактичні операції з даними виконуються автоматично без втручання адміністратора СУБД.

Слід зазначити, що для систем управління даними нового покоління (NoSQL, NewSQL) питання безпеки здебільшого розглядаються в межах конкретних реалізацій. Темпи наукових досліджень у сфері безпеки СУБД не встигають за динамічним розвитком ринку баз даних, хмарних обчислень і практичних рішень щодо інтеграції різнорідних даних.

Поява багатомодельних СУБД суттєво стимулювала розвиток хмарних баз даних, що надаються як послуга за моделлю DBaaS (Database as a Service). Сьогодні спостерігається стійка тенденція до міграції систем управління даними у хмарні середовища, що забезпечують високу масштабованість, відмовостійкість, глобальну доступність ресурсів, а також спрощують процеси розгортання, клонування і адміністрування даних. Та нажаль, хмарний підхід має низку обмежень, насамперед у сфері безпеки. Так досягнення гарантованого рівня захисту ускладнюється відсутністю повного фізичного контролю над даними, які розміщуються та обробляються на інфраструктурі хмарного провайдера. Це означає, що критично важлива інформація фактично зберігається в середовищі з обмеженим рівнем керованості з боку власника, що потребує впровадження додаткових організаційних і технічних механізмів захисту.

Хмарні системи надають широкий спектр послуг, включаючи підтримку прикладних програм, зберігання та управління даними, а також мережеві та обчислювальні ресурси. Серед популярних хмарних сервісів — веб-застосунки електронної пошти, такі як Gmail від Google або Office 365 Outlook від Microsoft; сервіси зберігання даних для кінцевих користувачів, зокрема Google Drive, Microsoft OneDrive та Dropbox; а також бізнес-застосунки, включно із системами управління взаємовідносинами зі споживачами (Customer Relationship Management, CRM Cloud) та платформами для управління бізнес-процесами, наприклад Workday.

Моделі розгортання хмарних технологій (публічна хмара, приватна, хмара спільноти, гібридна тощо) конфігуруються залежно від кількості користувачів, типу сервісів і необхідних ресурсів. Хмари можуть бути розгорнуті приватно на інфраструктурі споживача або провайдера, або ж публічно одним або кількома постачальниками хмарних послуг. Кожна модель розгортання передбачає певні компроміси щодо контролю споживачем своїх ресурсів, а також масштабу, вартості та доступності цих ресурсів [9].

Впровадження моделей хмарних обчислень — інфраструктури як послуги (IaaS), платформи як послуги (PaaS) та програмного забезпечення як послуги (SaaS) — в інформаційно-комунікаційну інфраструктуру КІ потребує запровадження адекватних і відповідних заходів захисту. У середовищах хмарних сервісів управління різними рівнями відповідальності розподіляється між постачальником і споживачем послуг залежно від моделі хмарного сервісу. Різні рівні архітектурного стеку хмарних сервісів відрізняються за ступенем контролю та відповідальності, що відображено в рекомендаціях Альянсу безпеки хмарних послуг. Хоча існує загальний консенсус щодо загроз і цілей безпеки для кожного рівня, специфіка реалізації різних моделей або середовищ хмарних сервісів зумовлює різний рівень контролю над компонентами та визначає набір можливих і ефективних заходів захисту в конкрет-

них умовах. До основних заходів забезпечення безпеки даних у хмарних середовищах належать: шифрування даних, резервне копіювання, багаторівневий контроль доступу, аудит і моніторинг для виявлення підозрілої активності та потенційних загроз, впровадження систем виявлення вторгнень і аналізу загроз, а також дотримання міжнародних стандартів і нормативних вимог [10–12].

Недостатня увага до практик безпеки постачальників хмарних послуг, недотримання державних і галузевих стандартів, а також нечіткий розподіл відповідальності між провайдером і споживачем створюють суттєві прогалини в захисті інформації і негативно впливають на функціональну стійкість інформаційних систем. Зокрема, неналежна реалізація заходів безпеки з боку постачальника може призвести до помилок конфігурації хмарного середовища і, як наслідок, до підвищення вразливості до кіберзагроз, таких як витоки даних, атаки програм-вимагачів, поширення шкідливого програмного забезпечення чи фішинг. Додаткові ризики виникають у процесі інтеграції даних із зовнішніх джерел, що розширює поверхню атак і підвищує залежність від третіх сторін. Постачальники послуг можуть виступати як потенційні джерела загроз для інформаційно-комунікаційної інфраструктури, особливо якщо їхні системи захисту є недостатніми. У цьому контексті особливу небезпеку становлять атаки на ланцюги постачання, коли зловмисники отримують доступ до ІС КІ через зовнішніх користувачів або довірених провайдерів, яким надано доступ до систем і даних.

Серед заходів, що можуть ефективно зменшити ризики безпеки та підвищити функціональну стійкість інформаційно-комунікаційної інфраструктури КІ в умовах використання хмарних технологій і уникнути втрати та модифікації даних доцільно виокремити наступні:

— впровадження механізмів захисту хмарних сервісів, орієнтованих на дані;

— оцінювання потенційних векторів атак на інформаційні активи як з боку зовнішніх, так і внутрішніх контурів взаємодії між ІС КІ;

— ідентифікація і аналіз ризиків, які пов’язані з постачальниками послуг, включаючи третіх і четвертих сторін;

— розроблення та впровадження планів реагування на інциденти безпеки;

— систематичний моніторинг і оцінювання стану безпеки постачальників хмарних сервісів;

— підвищення рівня обізнаності та навчання персоналу з питань кібербезпеки;

— регулярна перевірка відповідності впроваджених заходів чинним нормативним вимогам і стандартам.

Невідомі вразливості програмного забезпечення (так звані вразливості нульового дня) також становлять загрозу для ІС КІ, оскільки можуть бути використані для їхньої компрометації ще до появи засобів захисту або виправлень. Усвідомлення цієї небезпеки зумовило формування узгодженої «дорожньої карти» рекомендацій для розробників програмного забезпечення. Зазначені рекомендації орієнтовані на створення програмних продуктів за принципом «безпека за замовчуванням», підвищення прозорості та підзвітності процесів розробки, а також активне впровадження автоматизованих механізмів конфігурації, моніторингу та регулярного оновлення програмного забезпечення. Ініціатива була започаткована Агент-

ством з кібербезпеки та безпеки інфраструктури США у співпраці з 13 країнами та міжнародними організаціями.

У більшості КІ інформаційно-комунікаційна інфраструктура функціонує за принципом централізованого управління, коли ключові функції контролю зосереджені на центральному сервері, що спрощує адміністрування, однак підвищує ризик компрометації усієї системи, оскільки створює єдину критичну точку відмови та розширює спектр потенційних уразливостей і загроз. Сучасні інноваційні тенденції свідчать про поступовий перехід до децентралізованих архітектур і автономних механізмів управління, які здатні забезпечити більш гнучке, стійке та масштабоване функціонування систем. Використання розподілених децентралізованих рішень в інформаційно-комунікаційній інфраструктурі дозволить знизити рівень уразливості за рахунок усунення єдиних точок відмови, підвищення відмовостійкості та покращення здатності системи протидіяти зовнішнім і внутрішнім загрозам.

Аналіз інформаційних впливів на КІ та її складові свідчить про їхню ескалацію в напрямі підвищення ефективності, руйнівності та масштабності атак. За оцінками Всесвітнього економічного форуму («Глобальні ризики 2024»), середньорічні збитки від атак на технологічні активи та сервіси КІ можуть перевищити 23 трлн дол. США до 2027 року (проти 8,4 трлн дол. у 2022 р.) [8].

З огляду на активне використання технологій штучного інтелекту (ШІ) для створення кіберзагроз (зокрема GenAI, ускладнює характер кіберзагроз, підвищуючи ефективність фішингу і атак програм-вимагачів), робить зрозумілою інтеграцію ШІ в системи кіберзахисту. Основними напрямами застосування ШІ є виявлення та блокування загроз, аналіз поведінки користувачів, автоматизація рутинних процесів, моніторинг мережевого трафіка та прогнозування потенційних уразливостей [13]. Це підтверджується і динамікою ринку: за оцінками Spherical Insights, обсяг ринку рішень ШІ для кібербезпеки може зрости з 15,25 млрд дол. у 2022 році до майже 97 млрд дол. у 2032 році.

Алгоритми ШІ вже сьогодні впроваджуються в ІС для моніторингу підозрілої активності, виявлення уразливостей, оцінювання ризиків, розпізнавання згенерованого контенту та реагування на кіберінциденти. ШІ здатний виявляти приховані закономірності у даних і використовувати отримані результати для підтримки або автоматизації прийняття рішень. Практичне застосування ШІ охоплює автоматизовану обробку звітів про безпеку, виявлення вторгнень, аналіз мережевого трафіку, зменшення кількості хибних тривог і прогнозування загроз. Крім того, інструменти ШІ є ефективними при модернізації інформаційно-комунікаційної інфраструктури КІ, зокрема під час впровадження нових систем, міграції до хмарних середовищ, інтеграції різнорідних рішень і технологічних оновлень. Алгоритми ШІ спрощують аналіз і налаштування конфігурацій, підвищують якість тестування на сумісність, продуктивність і безпеку, а також дозволяють своєчасно виявляти конфлікти, помилки та потенційні уразливості. Та слід враховувати подвійний характер технологій ШІ: поряд із підвищенням рівня захисту системі і покращення якості інфраструктури вони можуть бути використані зловмисниками для створення нових типів атак і посилення їхньої ефективності, і це вимагає постійного вдосконалення підходів до забезпечення безпеки.

Висновки

З огляду на складність, взаємозалежність і взаємопов'язаність КІ та їхніх інформаційно-комунікаційних систем, забезпечення резильєнтності КІ та необхідної функціональної стійкості ІС КІ має ґрунтуватися на системному підході, що передбачає комплексне поєднання рішень, спрямованих як на підвищення надійності та відмовостійкості комп'ютерних ресурсів, так і на протидію очікуваним і новим негативним впливам і кіберзагрозам.

Забезпечення функціональної стійкості ІС КІ потребує перманентного аналізу загроз, невизначеностей і ризиків, щоб підтримувати здатність ІС протидіяти реалізації загроз, зберігати працездатність в умовах динамічних і непередбачуваних впливів. Це можна забезпечити завдяки своєчасному формуванню і адаптації захисних механізмів, орієнтованих не лише на запобігання інцидентам, а й на забезпечення деградаційно-стійкого функціонування ІС та її здатності до швидкого відновлення.

Враховуючи, що значна частина сучасних кіберзагроз реалізується через компрометацію даних, особливого значення набувають стратегії організації, зберігання та передавання інформації. Перехід до даноорієнтованих моделей безпеки, у поєднанні з використанням когнітивних технологій і ШІ, є підґрунтям для формування адаптивних інтелектуальних засобів захисту систем управління даними. Такі системи здатні до самоаналізу та самоналаштування з урахуванням поточного контексту функціонування, накопиченого досвіду та великої кількості параметрів стану. Вони забезпечують виявлення поведінкових аномалій, зниження ризиків, пов'язаних із людським фактором, ідентифікацію вразливих місць у системах безпеки, а також прогнозування можливих сценаріїв атак. Застосування таких засобів у поєднанні з обґрунтованими структурно-функціональними рішеннями дозволять підвищити рівень захищеності та забезпечити необхідний рівень функціональної стійкості ІС КІ в умовах постійно змінного середовища загроз.

1. Dodonov O., Gorbachyk O., Kuznietsova M. Automated Organizational Management Systems of Critical Infrastructure: Security and Functional Stability. In: XXI International Scientific and Practical Conference «Information Technologies and Security» (ITS 2021). *CEUR Workshop Proceedings* 2021, **324**1, P. 1–12. URL: http://ceur-ws.org/Vol-3241/paper1.pdf

2. Моделі структурного синтезу для управління параметрами інфокомунікаційних мереж систем критичної інфраструктури: моногр. / В. В. Косенко, І. Ш. Невлюдов. Харків: Харківський національний університет радіоелектроніки, 2019. 163 с.

3. 205 Cybersecurity Stats and Facts for 2026. URL: https://www.vikingcloud.com/blog/cybersecurity-statistics

4. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37 %. URL: https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37

5. Dodonov O., Gorbachyk O., Kuznietsova M. Critical Infrastructure Resilience and Cybersecurity of Information Management Systems //Selected Papers of the XXIII International Scientific and Practical Conference «Information Technologies and Security» (ITS 2023) Kyiv, Ukraine, November 30, 2023. Online: http://ceur-ws.org/Vol-3887/ paper1.pdf

6. Бочарников В.П. Fuzzy Technology: модальность и принятие решения в маркетинговых коммуникациях. 2002. Киев: Ника-Центр, Эльга. 224 с.

7. Voevodin V.A. Monte Carlo method for predicting the stability of functioning of the informatization object in conditions of massive computer attacks. International Conference «MSR-2021» *Journal of Physics: Conference Series*. 2021.Vol. 2099.

8. Cybersecurity statistics to lose sleep over in 2025. URL: https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020

9. Спасітєлєва С.О., Жданова Ю. Д., Чичкань І. В. Проблеми безпеки універсальних платформ управління даними**.** *Кібербезпека: освіта, наука, техніка*. 2019. Т. 2, № 6. С. 122–133. URL: https://csecurity.kubg.edu.ua/index.php/journal/issue/view/9

10. ENISA: Compendium of risk management frameworks with potential interoperability. Technical report, European Union Agency for Cybersecurity. 2022.

11. Freund J., Jones J. Measuring and Managing Information Risk. Butterworth-Heinemann, Waltham. 2015. Online: https://doi.org/10.1016/C2013-0-09966-5.

12. Law M. Top 10 data security risks faced by businesses in 2023. URL: https://cybermagazine.com/top10/top-10-data-security-risks-faced-by-businesses-in-2023.

13. How AI could change threat detection. URL: https://www.techtarget.com/searchsecurity/tip/How-AI-could-change-threat-detection

Надійшла до редакції 24.02.2026
Прийнята до друку 17.03.2026
Опублікована 17.03.2026