КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.24.282297
УДК 005.056

**Гулак Євген Геннадійович**
аспірант
Інститут проблем математичних
машин і систем НАН України, Київ, Україна
ORCID ID: 0000-0003-4984-686X
*evgeniygulak@gmail.com*

# МЕТОДИКА РАЦІОНАЛЬНОГО СИНТЕЗУ ПІДСИСТЕМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

**Анотація.** У статті розглянуто стан розвитку методології побудови підсистем захисту інформації інформаційних систем об'єктів критичної інфраструктури, окремо виділене питання створення комплексного захисту для складних систем. Відмічено, що складним системам притаманні наявність значної кількості різнорідних елементів, які для досягнення певної мети об'єднані в єдину систему; існування складних, іноді суперечливих зв'язків та впливів; потужні інформаційні потоки між складовими підсистемами. Проведений аналіз характеристик складних інформаційних систем, які негативно впливають на побудову підсистем захисту інформації, визначено актуальність розв'язання завдань створення комплексного захисту для таких систем, особливо в рамках побудови мережі ситуаційних центрів. Зазначено, що вирішенню значної кількості завдань захисту та підвищенню його ефективності сприяє впровадження вдало спроєктованої підсистеми криптографічного захисту інформації (КЗІ), яка може забезпечити надійний захист конфіденційності та цілісності інформації, що обробляється в системі. В рамках визначення умов застосування підсистеми КЗІ в складних системах об'єктив критичної інфраструктури для убезпечення інформації з обмеженим доступом та контролю її цілісності запропоновано методику декомпозиції складних систем одного виду та вдосконалено модель криптографічного захисту в таких системах. Виходячи з необхідності реалізації в рамках процесу вибору певних апаратно-програмних технологічних рішень багаторазової реалізації процедур швидкого порівняння значної кількості якісних (семантичних) та кількісних показників підсистеми захисту інформації на підставі властивостей функціональних профілів запропоновано методику раціонального вибору на основі найбільшого значення функції безпеки засобів придатних для використання в підсистемі.

**Ключові слова:** криптосистема; складна система; критична інфраструктура; мережа ситуаційних центрів; декомпозиція складної системи; функціональний профіль захищеності.

## ВСТУП

**Постановка проблеми.** Сучасний стан науково-методологічного забезпечення процесів створення систем захисту інформації дозволяє ефективно проєктувати системи захисту інформації, які створюються одночасно з побудовою інформаційно-комунікаційних систем (ІКС), що захищаються.

Дещо інакше складається ситуація у випадку побудови системи захисту для вже існуючих ІКС, оскільки деякі їх концептуальні рішення потенційно можуть ускладнювати реалізацію заходів захисту. Проблем переважно не виникає з побудовою системи захисту, якщо захищається інтегрована ІКС [1], для якої існує достатньо простий варіант її декомпозиції на декілька відносно самостійних функціональних підсистем, наприклад, у вигляді центрального компонента, підсистеми інформаційного

транспорту та майже однакових віддалених робочих станцій. В такому випадку звичайно не виникає суттєвих труднощів з побудовою комплексної системи захисту ІКС та вона створюється як сукупність підсистем захисту для її складових.

В той же час, на практиці суттєві проблеми з реалізацією комплексного підходу щодо захисту інформації мають місце у випадках коли декомпозиція існуючої ІКС стикається із нелінійним характером взаємозв'язків між її складовими, різними вимогами щодо їх безпеки та захисту інформації в них, значною динамікою подій в ІКС та суттєвими обмеженнями щодо часу обробки та передачі документальних матеріалів. Тут і далі під документальними матеріалами в ІКС ми розуміємо структуровану інформацію в електронному вигляді з певними атрибутами (зокрема, гриф обмеження доступу, позначки часу обробки, підписи посадових осіб тощо) що створена для забезпечення службових потреб.

Зважаючи на викладене зміст статі концентрується розв'язанні в рамках комплексного підходу завдань побудови підсистем захисту інформації до ІКС, які виходячи з їх організаційно-технічних, технологічних та архітектурних рішень та неповноти даних про них далі класифікуються як складні системи.

**Аналіз останніх досліджень і публікацій**. Теорія та практика побудови систем захисту для державних та комерційних об'єктів критичної інфраструктури свідчить про виникнення сучасних реалій, що потребують пошуку нових підходів до вирішення завдання убезпечення інформації з обмеженим доступом, яка обробляється та зберігається в ІКС різних за підпорядкованістю організаційних структур, але необхідність ознайомлення з нею виникає в рамках «надбудови» над цими ІКС деякої мережі взаємодії відповідних органів.

Прикладом такої ІКС може бути мережа ситуаційних центрів, що утворюється для підвищення ефективності діяльності таких центрів та їх взаємодії [2]. Для кожного з ситуаційних центрів мережі детальний зміст його завдань та функцій, порядок і швидкість їх реалізації, здатність їх адаптування до швидкоплинної обстановки визначається залежно від його відомчої приналежності, форми власності, інформації що обробляється та інших факторів [3].

Перелічені чинники фактично ускладнюють умови реалізації та вжиття низки необхідних організаційно-технічних заходів що спрямовані на забезпечення належного рівня безпеки інформації, яка обробляється [4], [5], що дає підстави надалі їх ідентифікувати як складні.

Такі системи вивчаються науковцями достатньо давно, зокрема, за допомогою методів математичного моделювання [6], [7]. При цьому основний наголос в дослідженнях робився на аспектах аналізу та вивчення процесів функціонування складних систем. Можливо звернути увагу, що єдиного визначення складних систем на поточний час не існує, переважна більшість визначень має описовий характер. Серед наведених дослідниками [8] характеристик слід виділити: наявність значної кількості різнорідних елементів, які об'єднані в єдину систему для досягнення певної мети; існування складних, іноді суперечливих зв'язків та впливів; потужні інформаційні потоки між складовими підсистемами.

Виходячи з методів та принципів системного аналізу [9] можливо стверджувати, що поведінка складної системи [6] має бути характеризована деякою множиною ключових показників, які є результатом взаємодії її складових та їх властивостями, до яких доцільно віднести, зокрема: надійність і стабільність як складові гарантоздатності, ефективність, захист від завад тощо.

В [10] узагальнені наукові здобутки в галузі моделювання та аналізу складних систем з точки зору мережевої науки, включаючи мережеве моделювання та аналіз життєво важливих вузлів, невразливості мережі, дезінтеграції мережі, аналіз стійкості та прогнозування складних мережевих зв'язків, що дає загальні риси формування вимог до системи захисту.

Слід звернути увагу, що складні інформаційні системи можуть утворюватися на різних об'єктах критичної інфраструктури, тому важливим є розуміння вимог до загальної безпеки відповідних галузей, а саме — профілів безпеки. На поточний момент галузь енергетики в плані забезпечення безпеки ОКІ посідає одне з перших місць. Для класифікації рівні безпеки підсистем, що складають електроенергетику, в [11] під егідою Міжнародного енергетичного агентства запропоновано Модель короткострокової енергетичної безпеки (MOSES), в якій профілі безпеки кодифікуються літерними символами від A до E.

Зважаючи на те, що границі між рівнями безпеки в першоджерелі кількісно не визначені, на рис. 1 подане умовне зображення наведеної в [11] моделі, де A відповідає найменшим ризикам і максимальній стійкості, а E — найбільшим ризикам і найнижчій стійкості. Якщо застосувати лінгвістичні змінні [12] до класифікації захищеності підсистем, що складають електроенергетику, то можна отримати наступні наближені відповідності: A-відмінно, B-нормально, C-непогано, D-погано та E-дуже погано.

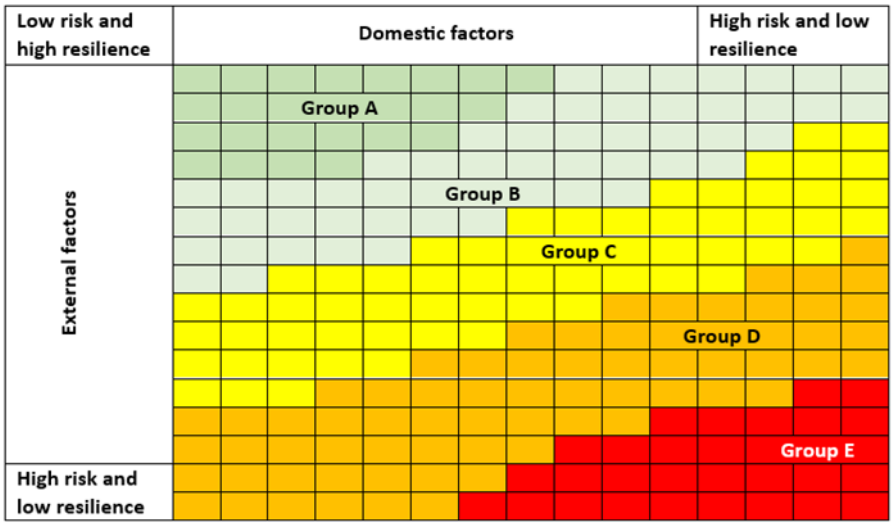


*Рис. 1 Модель профілів безпеки галузі електроенергетики MOSES*

Хоча наведена модель не дає прямої відповіді щодо кількісних показників системи захисту інформації, тим не менш у подальшому ми скористаємся цією моделлю.

**Мета статті** полягає у визначенні умов застосування підсистеми криптографічного захисту інформації (КЗІ) в складних системах об'єктив критичної інфраструктури для убезпечення інформації з обмеженим доступом та контролю її цілісності, а також у формуванні методики раціонального синтезу надійної підсистеми КЗІ.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

**Методика декомпозиції складної системи критичної інфраструктури**

Вище було зазначено, що процедура віднесення деякої реальної інформаційної системи до множини «складних» або «простих» на поточний час поки ще не формалізована, оскільки на умови такої класифікації суттєво впливає багато факторів, включаючи конкретні цілі та завдання дослідження функціонування цієї системи.

В той же час виходячи з існуючих наукових публікацій спробуємо окреслити множину таких систем на основі їх властивостей, що безпосередньо впливають на процеси побудови та функціонування підсистем інформаційної безпеки, що покликані забезпечити конфіденційність, цілісність та доступність інформації, яка обробляється.

На підставі аналізу та узагальнення факторів що наведені в [6] – [8], [10] та з урахуванням методологічних основ забезпечення інформаційної безпеки та кібербезпеки доцільно вважати, що складна з точки зору захисту інформації в ІКС (далі — складна система, *complex system* — CS) характеризується деякими з перерахованих властивостей:

- нетривіальна (нелінійна) взаємодія між її компонентами (складовими), що негативно впливає на можливість її автоматизованої декомпозиції [13] – [15] або декомпозиції за участю експертів на більш прості підсистеми з метою її системного аналізу та визначення плану захисту;
- прояв на макрорівні складних властивостей, які мають ознаки штучного інтелекту, зокрема, таких як самоорганізація та висока невизначеність;
- потенційно висока динаміка можливого розвитку небезпечних подій у системі внаслідок реалізації вірогідних загроз інформаційної безпеки значно перевищує потенціал персоналу безпеки в плані прийняття ефективних управлінських рішень та оперативного адекватного реагування на них;
- високий рівень залежності характеристик гарантоздатності (надійності) системи і ефективності її функціонування від таких самих характеристик лише кількох підсистем;
- існування в CS певної множини взаємодіючих між собою підсистем, що приймають, передають та зберігають інформацію, вимоги щодо захисту якої визначаються їх різними власниками: суб’єктами або технологічними процесами. При цьому можуть існувати підсистеми, в яких доступ суб’єктів до об’єктів (процесів) реалізується за допомогою технологій, що не узгоджені з політиками безпеки інших складових CS. Наприклад, це може стосуватись припустимості використанням в окремих підсистемах мобільних пристроїв загального користування для реалізації дистанційного доступу до деяких ресурсів.

Зрозуміло, що наведені фактори за суттю можуть бути визначальними для побудови та дослідження моделей захисту складних систем та потребують відпрацювання належного комплексу організаційно-технічних (технологічних) рішень.

В загальному випадку розв’язання задач побудови комплексної системи захисту інформації для CS у кожній з наведених ситуацій може бути дуже складною проблемою, хоча в окремих випадках можуть бути запропоновані доволі ефективні рішення після їх детального вивчення та вдалої декомпозиції CS на складові.

Зокрема, проаналізуємо задачу убезпечення інформаційного обміну деякої множини взаємодіючих між собою підсистем, в яких обробляється інформаційні ресурси, вимоги що захисту якої визначаються їх різними власниками. В цьому випадку

модель CS може бути подана у вигляді графа $G$ з множинами вершин та дуг відповідно $V$ та $A$:

$$G(V,A) = \langle V,A\rangle, V = \{v_1(r_1), v_2(r_2), \dots, v_n(r_n),\}, A \subseteq V \times V, \quad (1)$$

де $v_i(r_i), i = \overline{1,n}$ — вершини графа що відповідають конкретним підсистемам CS, а значення $0 \le r_i \le m$ є деякими позначеннями рівнів безпеки для забезпечення можливості обробки інформації з умовними рівнями конфіденційності від 0 (відкрита інформація) до $m$ (відповідає вищому рівню конфіденційності).

Кажемо, що вершини $v_i(r_i)$ та $v_j(r_j)$ з'єднує безумовна спрямована дуга $\left(v_i(r_i), v_j(r_j)\right)$, якщо має місце співвідношення $r_i \le r_j$. Інакше кажучи, рівень безпеки інформації з обмеженим доступом в підсистемі CS, що є потенційним її споживачем, не менше рівня безпеки такої інформації в підсистемі, яка є утримувачем. При цьому, можна вважати, що будь якій документ може бути переданий з першої підсистеми у другу.

Очевидно, що вершини $v_i(r_i)$ та $v_j(r_j)$ з'єднують дві безумовні спрямовані дуги $\left(v_i(r_i), v_j(r_j)\right)$ та $\left(v_j(r_j), v_i(r_i)\right)$ тільки в разі $r_i = r_j$. В цьому випадку вершини $v_i(r_i)$ та $v_j(r_j)$ будемо називати тотожними у сенсі забезпечення їх безпеки та позначати як $v_i(r_i) \sim v_j(r_j)$.

Нескладно бачити, що введене бінарне відношення на множині вершин $V$ є симетричним, рефлексивним та транзитивним [27], тобто воно є відношенням еквівалентності відносно якого множина вершин може бути подана у вигляді прямої суми класів еквівалентних вершин:

$$V = \bar{V}_0 \dot{+} \bar{V}_1 \dot{+} \dots \dot{+} \bar{V}_m,\ \bar{V}_i \cap \bar{V}_j = \emptyset, i \ne j \quad (2)$$

Фактично зроблено перший крок на шляху декомпозиції нашої системи на підсистеми, а граф з'єднань між підсистемами набув вигляд дерева — зв'язного ациклічного графу:

$$\bar{V}_0 \longrightarrow \bar{V}_1 \longrightarrow \cdots \longrightarrow \bar{V}_m. \quad (3)$$

При цьому передача документи з будь якім рівнем конфіденційності з класу з меншим рівнем безпеки в клас вищим рівнем безпеки не впливає на загальну безпеку системи. Зазначимо, що передача такого документа в зворотній бік у загальному випадку суперечить існуючим принципам побудови систем захисту.

Далі введемо поняття умовно спрямованої дугі наступним чином: будемо говорити, що вершини $v_i(r_i)$ та $v_j(r_j)$ де $r_i > r_j$ з'єднує умовна спрямована дуга $\left(v_i(r_i), v_j(r_j) \setminus U\right)$, якщо виконується деяка формалізована умова безпеки $U$. Факт неявності умовно спрямованої дугі будемо позначати як $\underset{U}{\rightarrow}$.

Логічною вимогою для формулювання умови безпеки для передачі інформації з більш високими вимогами щодо її захисту з адекватного їй безпекового класу $\bar{V}_i$ в клас $\bar{V}_j, j < i$ з меншим рівнем захищеності є необхідність мінімізації ризику в разі реалізації загрози витоку інформації. Які можливі кроки для досягнення вказаної мети?

***U***1. Очевидно, передача інформації потребує, щоб рівні безпеки підсистеми отримувача та підсистеми відправника були максимально близькими. Це означає, зокрема, що умовна спрямована дуга може застосовуватись в (3) тільки між сусідніми еквівалентними класами, тобто умовні спрямовані дугі можуть з'єднувати тільки безпекові класи:

$$\bar{V}_{i+1} \underset{U}{\rightarrow} \bar{V}_i, i = \overline{0, m-1}.$$

***U***2. Для мінімізації ризиків рівні безпеки сусідніх класів мають бути максимально наближені один до одного, що можливо досягти шляхом побудови максимально припустимої низки рівнів (інакше — рівнів конфіденційності даних що передаються).

***U***3. Довжина конфіденційного повідомлення що передається в цих умовах має бути максимально обмежена.

***U***4. Особи (суб'єкти) що можуть отримати доступ до відповідного конфіденційного повідомлення мають бути погоджені (визначені) власником інформації.

***U***5. Інформація що передається визначеним особам має бути захищена за допомогою схвалених організаційно-технічних заходів.

***U***6. Має бути реалізований механізм автоматичного знищення цієї інформації в підсистемі з нижчим рівнем безпеки одразу же після завершення встановленого терміну її використання. Для продовження терміну використання має бути надісланий повторний запит на її отримання, якій реєструється у системі, яка відправляє інформацію.

В разі виконання визначених умов ***U***1 — ***U***6 початкова складна система (1) може бути подана у вигляді поєднання її підсистем, що більш пристосовані для забезпечення безпеки конфіденційності інформації в цій системі:

$$G(V,A) = \langle V,A \rangle \Longrightarrow G(\bar{V}_0 \dotplus \bar{V}_1 \dotplus \ldots \dotplus \bar{V}_m, A, U). \quad (4)$$

Отриману декомпозицію CS ілюструє рис. 2.

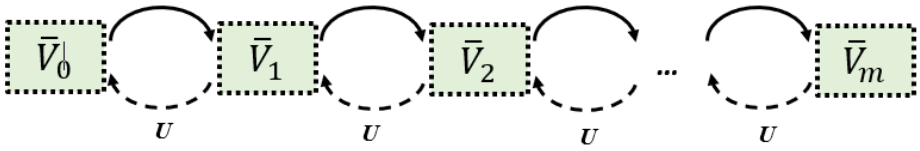


*Рис. 2 Декомпозиція складної інформаційної системи*

Далі уточнимо умови безпеки для передачі інформації з більш високими вимогами щодо її захисту з адекватного їй безпекового класу в клас з меншим рівнем захищеності з використанням технології криптографічного захисту інформації.

**Вдосконалення моделі захисту інформації**

Серед умов ***U***1 — ***U***6 найбільш важливим є фактор ***U***5 що передбачає визначення відповідних моделей та методів захисту. Серед найбільш ефективних технологій розв'язання значної кількості проблем забезпечення інформаційної безпеки та кібербезпеки слід виділити сучасні технології криптографічного захисту інформації, які надають можливість гарантованого забезпечення конфіденційності та цілісності інформації, а також підтвердження її авторства.

Зокрема, підсистема криптографічного захисту інформації за допомогою шифраторів, які працюють у режимі VPN, може забезпечити необхідний рівень безпеки різних сегментів мережі виконуючи при цьому функції міжмережевого екранування, приховування архітектури сегмента, що захищається, а також конфіденційності та цілісності даних. При цьому, в разі застосування імітостійкого шифру [16] суттєво знижується ймовірність вірусної атаки з боку глобальної мережі, оскільки спроба вбудувати злоякісний код в зашифрований потік або пакет даних з високим рівнем ймовірності буде марною, оскільки розшифрування потоку зруйнує логічну структуру цього коду.

Вирішення прикладного завдання синтезу апаратно-програмного комплексу захисту інформації ускладняється низкою факторів, включаючи необхідність врахування значної кількості критеріїв для оцінки їх раціонального варіанту, які мають не тільки

кількісний, а й якісний (нечіткий) характер, що обмежує застосування класичних математичних методів обробки даних, включаючи методи оптимізації.

Базовим принципом кіберзахисту є постулат, що вартість організаційно-технічних заходів та засобів захисту інформації, витрати на створення та підтримку функціонування системи кібербезпеки мають бути узгоджені з потенційно можливими збитками у разі реалізації вірогідних кіберзагроз [16], [17].

В умовах, коли зростання кількості та потужності кібератак на об'єкти критичної інфраструктури (ОКІ) є безперечним фактом, а ресурси, що можуть бути використані для реалізації завдань кіберзахисту, залишаються доволі обмеженими, актуалізується питання створення та застосування методики раціонального вибору засобів захисту інформації [19] для убезпечення ОКІ.

Зокрема, процедура вибору засобів криптографічного захисту інформації (КЗІ) повинна забезпечити визначення такого їх складу, який в комплексі забезпечує необхідний рівень конфіденційності та контроль цілісності даних в інформаційно-комунікаційної системи (ІКС) ОКІ, мінімізуючи при цьому вартість утримання. Під складом засобів КЗІ далі розуміємо сукупність криптографічного обладнання, що реалізує повний комплекс необхідних функцій, включаючи шифратори конфіденційної інформації, систему генерації та розподілу ключів, носії ключової інформації, засоби менеджменту та налаштування захищеної мережі тощо.

В загальному випадку відповідно до методології побудови системи управління інформаційною безпекою методика раціонального вибору повинна враховувати результати виконання наступних важливих кроків: визначення інформаційних ресурсів, які підлягають захисту, та оцінка їх початкової вартості; формування моделі загроз для ІКС ОКІ; оцінка ризиків для визначених інформаційних ресурсів; розробка моделі системи кіберзахисту, що максимально повно враховує наслідки реалізації потенційно можливих загроз та включає перелік завдань і функцій для комплексу апаратних, програмних та програмно-апаратних засобів захисту; збір, систематизація та аналіз відомостей щодо існуючих на ринку засобів захисту інформації, включаючи їх профілі захисту [20] та відгуки експертів щодо результатів їх практичного застосування; проведення фінансових розрахунків реалізації кожного варіанту набору ЗЗІ, включаючи їх інсталяцію та підтримку; порівняльний аналіз опрацьованих варіантів з точки зору їхньої придатності та переваг щодо виконання завдань за призначенням та вартісних показників.

Аналіз потенціалу засобів КЗІ в плані можливості виконання завдань щодо забезпечення конфіденційності та цілісності інформаційних ресурсів включає вивчення двох груп факторів їхнього застосування: суттєві вимоги до засобів КЗІ [21] та їх загальні властивості, як продуктів мікроелектронної та програмної інженерії.

Перша група факторів визначає аспекти безпеки застосування засобів шифрування та формується за результатами криптографічного та інженерно-криптографічного аналізу засобів КЗІ [22], [23], а також, за необхідності, шляхом проведення їх спеціальних досліджень стосовно виникнення технічних каналів витоку інформації з обмеженим доступом. Дані щодо вказаних факторів уточняються у процесі оцінки відповідності засобів КЗІ згідно діючих нормативних актів [22].

Друга група факторів включає, зокрема, такі функціональні характеристик як:

1. Ступінь сумісності засобів КЗІ з вимогами запланованої до застосування транспортної інформаційної мережі (поширеними протоколами взаємодії);
2. Сумісність з операційною системою, підтримка вимог застосовних апаратної платформи та прикладного програмного забезпечення;
3. Типи файлів, що обробляються;

4. Швидкість обробки інформації;
5. Функціональність та зручність застосування та адміністрування;
6. Ергономічні, масо-габаритні характеристики;
7. Здатність (час) автономної роботи без обслуговування;
8. Гарантоздатність.

Виходячи з визначених умов забезпечення безпеки конфіденційної інформації що циркулює в CS можливо запропонувати вдосконалену модель програмно-апаратного засобу КЗІ — шлюзу безпеки (рис. 3).

У вдосконаленій моделі використовуються модулі (вузли), які реалізують наступні необхідні функції та перетворення: симетричного та асиметричного шифрування (через дефіс — позначення модулю) — ШС-А, індикація станів — ІС, автентифікація та екранування — АЕ, інтерфейс абонентський — ІА, інтерфейс глобальної мережі — ІМ, ручне управління — РУ, управління системою (шлюзом) — УС, генерація ключів — ГК, контроль (тестування) ключів/параметрів безпеки — КК, введення ключів — ВК, тестування та блокування — ТБ, реєстрація подій — РП, комутатор режимів — КР, авторизація оператора — АО.

Переривчастими лініями на рисунку показані сигнали управління та інформації про стан вузлів шлюзу. Суцільними лініями показана передача параметрів (символ →) та інформації, яка підлягає шифруванню (символ ⇔).

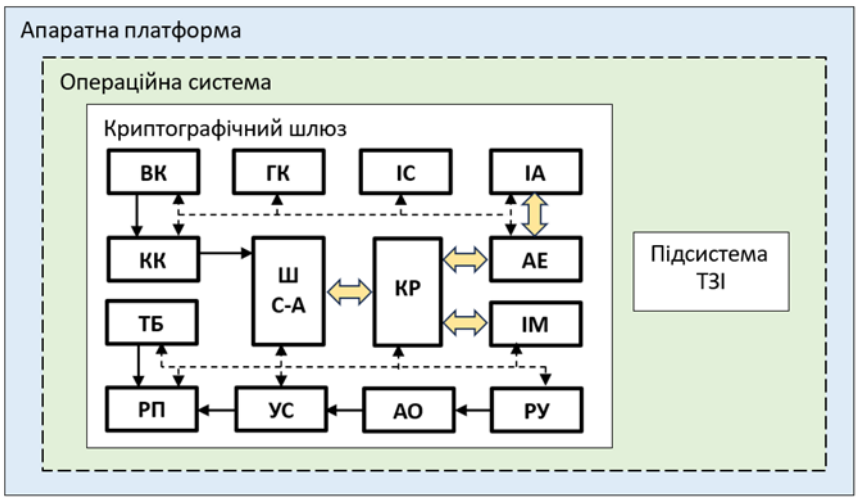


*Рис. 3 Вдосконалена модель підсистеми КЗІ — шлюз безпеки*

На відміну від прототипу [23] у вдосконаленої моделі передача документів з обмеженим доступом або особливо цінних із одної ІКС $S_1$ в іншу $S_2$ здійснюється через шлюз за умов наявності в них дозвільних відміток, що завірені кодом автентифікації повідомлення (MAC).

$$S_1 \underset{MAC}{\Longrightarrow} S_2.$$

Відповідний MAC створюється менеджером з безпеки що уповноважений на такі дії, при цьому створений код обов'язково повинен зберігатись разом з документом протягом всього його життєвого циклу. В разі зміни документу, навіть часткової, MAC встановленим порядком формується на ново.

Для реалізації визначених функцій вдосконалена модель також має додаткові елементи. Головною відмінністю наведеної моделі порівняно з прототипом [23] є введення наступних процедур, що відповідають необхідності виконання умові ***U***5:

– контролю за наявністю відміток про погодження можливості передачі певного документу до іншої системи обробки даних вузла АЕ — автентифікації і екранування;
– реєстрації подій РП в шлюзі для збору даних про функціональне обслуговування шлюзу, про спроби надсилання за межі системи документів, передача яких не погоджена встановленим порядком, дані роботи підсистеми тестування та блокування, зокрема, про збої в роботі шлюзу тощо;
– автентифікації оператора АО шлюзу, якій здійснює його налаштування та обслуговування;
– застосуванням першого контуру шифрування повідомлення з використанням відкритого ключу отримувача, що перебуває підсистемі складної мережі, з меншим рівнем безпеки.

З метою надійного функціонування криптографічного шлюзу всі його елемент мають бути убезпечені за допомогою підсистеми технічного захисту інформації, на яку, зокрема, покладаються завдання антивірусного захисту та розмежування доступу.

**Характеристика показників захисту**

Раціональний вибір конкретної архітектури підсистеми захисту інформації у загальному випадку є складною задачею оптимізаційного типу оскільки вона визначається значною кількістю критеріїв в умовах пошуку кращого в певному сенсі рішення за співвідношенням таких показників, як вартість та ефективність рішення [24]. При цьому показник ефективність може включати такі субпоказники, як ймовірність виявлення та блокування небезпечної події, час що необхідний для однократної реалізації певної захисної функції, повернення інвестиційних коштів [24] [,25] тощо.

Виходячи з необхідності реалізації в рамках процесу вибору певних апаратно-програмних технологічних рішень багаторазової реалізації процедур швидкого порівняння значної кількості якісних (семантичних) та кількісних показників підсистеми захисту інформації $\bar{\alpha} = \{\alpha_1, \dots \alpha_n\} \in \mathcal{A}$, де $\mathcal{A}$ множина її показників, можливо визначити [17], що базовим елементом методики раціонального вибору засобів КЗІ має бути побудова рейтингової шкали відображення цих показників у зіставні числові значення:

$$\bar{\alpha} \mapsto \bar{x} = (x_1, \dots, x_n) \in \mathbb{R}^n, \quad (4)$$

де $\mathbb{R}^n$ — простір розмірності $n$ над полем дійсних чисел.

Доволі простим варіантом реалізації шкали відображення в (4) є зіставлення показника (кількісного або якісного) з очікуваним результатом від його досягнення у відсотках або дійсними числами з інтервалу $[0,1]$. Для оцінки результату можуть бути використані розрахунковий метод, метод моделювання або експертний метод.

Очевидним шляхом, зокрема, можна побудувати перетворення значень критеріїв функціонального профілю захисту що формуються згідно [20].

Позначимо через: $K_j^C, j = \overline{1,5}$; $K_j^I, j = \overline{1,4}$; $K_j^A, j = \overline{1,4}$; $K_j^O, j = \overline{1,9}$ — критерії конфіденційності, цілісності, доступності та спостережності відповідно.

1. Далі для визначених підсистем (засобів) захисту інформації для кожного конкретного значення критерія захищеності, що наведений в його профілі захисту, розраховуємо зіставлене йому дійсне число $x = {}^{n_\text{ф}}/_{N_\text{м}}$, де $N_\text{м}$ — максимальне значення критерія, $n_\text{ф}$ — фактичне значення критерія що визначене у профілі захисту (рівень послуги). Наприклад, критерій захищеності «Конфіденційність адміністративна» передбачає чотири рівня послуги, тобто $N_\text{м} = 4$, якщо в профілі захисту визначений

ISSN 2663 - 4023

критерій КА-2, тоді зіставлене число дорівнює $x = {}^{2}/_{4} = 0.5$ Умовно кажучи, в цьому випадку механізм захисту використаний тільки наполовину від його потенціалу.

2. Для кожної групи критеріїв (конфіденційності, цілісності, доступності та спостереженості) розраховується вагова функція безпеки (за суттю це функція потенціалу безпеки):

$$\mathcal{F}(x_1, x_2, \dots) = \frac{W}{M}\sum_j x_j \quad (5)$$

де $M = m_C, m_I, m_A, m_O$ — послідовно набуває значення кількості критеріїв однакової спрямованості в групі, що аналізується (для [20] маємо $m_C = 5, m_I = 4, m_A = 4, m_O = 9$), $W = w_C, w_I, w_A, w_O$ — вагові коефіцієнти — пріоритети для різних типів загроз (конфіденційності, цілісності, доступності та спостереженості) що встановлюються експертами, $w_C + w_I + w_A + w_O = 1$.

3. Підсумкове значення для функції безпеки розраховується як сума її значень для конкретних груп критеріїв:

$$\mathcal{F} = \mathcal{F}_\mathrm{C} + \mathcal{F}_I + \mathcal{F}_A + \mathcal{F}_O. \quad (6)$$

4. Засіб з найбільшим значенням функції безпеки вважаємо найбільш придатним для використання в підсистемі на підставі властивостей його профілю захисту.

В табл. 1 наведені реальні дані щодо функціональних профілів двох засобів захисту інформації (ЗЗІ), лише деякі їх показники були змінені для наочності.

З таблиці без додаткових розрахунків складно зробити висновок щодо переваг одного ЗЗІ перед іншим, оскільки з 14 наведених критеріїв шість забезпечують однакові рівні послуг, 4 свідчать на користь одного засобу та 4 на користь іншого (умовні позначення =, <, > в останньому стовпчику таблиці).

Ненормована сума по всіх критеріях свідчить про перевагу на користь першого засобу (7.37 проти 7.2). Але ця сума не враховано той факт, що кількість критеріїв в групах різна (параметр $M$), тому відповідне корегування уточнює результат на користь другого засобу (2.12 для ЗЗІ-1 та 2.2 для ЗЗІ-2).

У останньому рядку таблиці наведені розрахунки за формулами (5) і (6) для зваженої суми середніх значень для груп критеріїв виходячи з пріоритету забезпечення конфіденційності інформації: $w_C = 0.4,\ w_I = 0.2, w_A = 0.2, w_O = 0.2$.

Слід відмітити наступні особливості реалізації запропонованої методики:

- для розрахунку функції безпеки обираються всі критерії захищеності, що присутні в функціональному профілі хоча б одно з засобів. Для засобів, у профілі яких цей критерій відсутній, вважається, що зіставлене число дорівнює $x = 0$;
- всі семантично подані вимоги мають бути попередньо вивчені та досліджені експертами для формування зіставних значень;
- у випадку необхідності порівняння функціональних профілів більше двох засобів ($K > 2$) спочатку обчислюються значення функцій безпеки для всіх засобів: $\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_K$, на основі яких формується порівняння їх варіаційний ряд:

$$\mathcal{F}_{i_1} \le \mathcal{F}_{i_2} \le \ \dots \ \le \mathcal{F}_{i_K}, \text{де } i_1, i_2, \dots, i_K \in \overline{1, K}, i_m \ne i_n, \quad (7)$$

де $m \ne n$.

Якщо для засобів що порівнюються відома вартість кожного з них: $C_1, C_2, \dots, C_K$, тоді значення функцій безпеки нормуються: ${\mathcal{F}_1}/{C_1}, {\mathcal{F}_2}/{C_2}, \dots, {\mathcal{F}_K}/{C_K}$, після чого варіаційний ряд (7) набуває нової якості:

$$\mathcal{F}_{j_1}\Big/_{C_{j_1}} \le \mathcal{F}_{j_2}\Big/_{C_{j_2}} \le \cdots \le \mathcal{F}_{j_K}\Big/_{C_{j_K}}, \text{ де } j_1, j_2, \dots, j_K \in \overline{1,K}, j_m \ne j_n, \quad (8)$$

де $m \ne n$.

Фактично, найбільший член варіаційного ряду відповідає засобу з номером $j_K$, що в ряду однотипних засобів має краще співвідношення «потенціал безпеки — вартість», а це фактично відповідає меті раціонального вибору.

Слід звернути увагу, що абсолютне значення різниці між функціями безпеки $\left|\mathcal{F}_{i_K} - \mathcal{F}_{i_1}\right|$ засобів, якім відповідають двом крайнім членам варіаційного ряду, є потенційним приростом потенціалу безпеки у випадку можливості додаткового витрачання коштів у сумі $\left|C_{i_K} - C_{i_1}\right|$.

Водночас можливо також відмітити, що в разі відмінності двох функціональних профілів захищеності лише в значенні тільки одного критерію, відповідна різниця у вартості засобів буде умовно свідчити про витрати на модернізацію одного засобу до рівня другого, що дає певний орієнтир для планування майбутніх заходів.

За суттю запропонована функція безпеки є інтегральною характеристикою багатьох показників засобу КЗІ що досліджується. Це, с одного боку, спрощує проведення розрахунків та зменшує складність методики. З іншого боку, інтегральна характеристика може приховувати деякі малі відхилення між параметрами двох засобів, що потребує прискіпливої уваги з боку дослідника в плані виявлення цих відхилень та їхньої значущості.

*Таблиця 1*

**Функціональні профілі безпеки та зіставлені показники**

| № № | Критерії безпеки | ЗЗІ - 1 | | ЗЗІ - 2 | | Краще? |
|---|---|---|---|---|---|---|
| | | $\alpha_j$ | $x_j$ | $\alpha_j$ | $x_j$ | |
| **Критерії конфіденційності $K_j^C$** | | | | | | |
| 1. | Довірча конфіденційність | - | 0.0 | КД-2 | 0.5 | < |
| 2. | Адміністративна конфіденційність | КА-2 | 0.5 | КА-2 | 0.5 | = |
| 3. | Повторне використання об'єктів | КО-1 | 1.0 | КО-1 | 1.0 | = |
| 4. | Конфіденційність при обміні | КВ-1 | 0.25 | КВ-2 | 0.5 | < |
| | Середнє по групі критеріїв | - | 0.44 | - | 0.83 | < |
| **Критерії цілісності $K_j^I$** | | | | | | |
| 5. | Адміністративна цілісність | ЦА-1 | 0.25 | ЦА-2 | 0.5 | < |
| 6. | Відкат | ЦО-2 | 1.0 | ЦО-1 | 0.5 | > |
| 7. | Цілісність при обміні | ЦВ-2 | 0.66 | ЦВ-1 | 0.33 | > |
| | Середнє по групі критеріїв | - | 0.64 | - | 0.44 | > |
| **Критерії доступності $K_j^A$,** | | | | | | |
| 8. | Використання ресурсів | ДР-2 | 0.66 | ДР-1 | 0.33 | > |
| 9. | Стійкість до відмов | ДС-1 | 0.33 | ДС-1 | 0.33 | = |
| 10. | Відновлення після збоїв | ДВ-1 | 0.33 | ДВ-1 | 0.33 | = |
| | Середнє по групі критеріїв | - | 0.44 | - | 0.33 | > |
| **Критерії спостереженості $K_j^O$** | | | | | | |
| 11. | Реєстрація | НР-2 | 0.4 | НР-2 | 0.4 | = |
| 12. | Ідентифікація і автентифікація | НИ-3 | 1.0 | НИ-2 | 0.66 | > |
| 13. | Цілісність КЗЗ | НЦ-1 | 0.33 | НЦ-2 | 0.66 | < |
| 14. | Самотестування | НТ-2 | 0.66 | НТ-2 | 0.66 | = |
| | Середнє по групі критеріїв | - | 0.60 | - | 0.60 | = |
| Ненормована сума по всіх критеріях | | - | 7.37 | - | 7.2 | |
| Сума середніх для груп критеріїв | | - | 2.12 | - | 2.2 | |
| Зважена сума середніх для груп критеріїв | | - | 0,512 | - | 0.606 | |

Методика була б неповною, якщо не згадати про критерії гарантій [20], що включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації.

Виходячи з моделі класифікації захищеності підсистем, що утворюють інфраструктуру електроенергетики [12], можна евристичним шляхом на основі досвіду сертифікації продукції в сфері захисту інформації запропонувати наступні відповідності «клас захищеності — рівень гарантій»: А (відмінно) — Г4, В (нормально) — Г3, С (непогано) — Г2.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведений аналіз стану методологічного забезпечення процесів побудови підсистем захисту інформації інформаційних систем об’єктів критичної інфраструктури свідчить про необхідність детального опрацювання питань комплексного захисту складних систем.

Можливо відмітити, що складним системам притаманні такі характеристики, як нетривіальна взаємодія між її елементами, що негативно впливає на можливість її декомпозиції складної системи на більш прості підсистеми з метою обстеження та визначення плану захисту:

- на макрорівні їм притаманні складні властивості, такі як самоорганізація та висока невизначеність;
- потенційна динаміка можливого розвитку небезпечних подій у складних системах може значно перевищувати здатність персоналу безпеки забезпечувати оперативне та адекватне реагування на них;
- гарантоздатність складної системи і ефективність її функціонування суттєво залежить від таких самих характеристик кількох підсистем;
- в складній системі можуть взаємодіяти між собою декілька підсистем, в яких обробляється інформація, вимоги що захисту якої визначаються їх різними власниками: суб’єктами або технологічними процесами. Зокрема, існують підсистеми, в яких доступ суб’єктів до об’єктів (процесів) реалізується за допомогою технологій, що не узгоджені з політиками безпеки інших складових системи (наприклад, з використанням мобільних пристроїв загального користування).

У підсумку дослідження складних інформаційних систем, визначено актуальність розв’язання завдань формування специфічних моделей та методик захисту в таких системах, зокрема, це стосується створення мереж ситуаційних центрів. У рамках дослідження запропоновано методику декомпозиції одного типу складної системи, вдосконалено модель криптографічного її захисту та запропоновано методику формування оцінки функції безпеки та порівняння на її основі різних засобів захисту.

Подальші дослідження доцільно спрямувати на уточнення властивостей складних систем що впливають на умови захисту інформації, які обробляється в цих системах, вдосконалення моделей та методів їх ефективного захисту, а також раціонального синтезу підсистем захисту для різних типів складних систем.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. ДСТСЗІ СБ України. (2005). *Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі* (НД ТЗІ 3.7-003 -2005)
2. Гречанінов, В.Ф. (2018). Мережа ситуаційних центрів органів державної влади — базис для підвищення ефективності їх діяльності (взаємодії). *Математичні машини і системи, 3,* 32–39.
3. Оксанич, І. М., Гречанінов, В. Ф., & Лопушанський, А. В. (2020). Інформаційна взаємодія у розрізнених інформаційних системах ситуаційних центрів. *Математичні машини і системи, 3,* 60–68.
4. Grechaninov, V., Hulak, E., Hulak, H., Skladannyi, P., & Sokolov, V. (2021). Decentralized Access Demarcation System Construction in Situational Center Network. *Cybersecurity Providing in Information and Telecommunication Systems (CPITS-II-2021), Vol. 3188,* 197–206.
5. Grechaninov, V., et al. (2022). Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center. In *Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, Vol. 3149,* 107–117.
6. Бусленко, Н. П. (1968). *Моделювання складних систем.* Наука.
7. Шаракшане, А. С. (1977). *Складні системи: Навчальний посібник.* Вища школа.
8. Ізраілов, К. Є. (2022). Оцінювання та прогнозування стану складних об'єктів: застосування для інформаційної безпеки. *Питання кібербезпеки, 6(52),* 2–19.
9. Горбань, О. М., & Бахрушин, В. Є. (2004). *Основи теорії систем і системного аналізу. Навчальний посібник.* ГУ «ЗІДМУ».
10. Yang, K., et al. (2023). Complex systems and network science: a survey. *Journal of Systems Engineering and Electronics, 34(3),* 543–573. https://doi.org/10.23919/JSEE.2023.000080
11. Jewell, J. (2011). *The IEA Model of Short-term Energy Security (MOSES).* Primary Energy Sources and Secondary Fuels, IEA.
12. Nasibov, V., et al. (2018). Models of Electric Power Industry Security Study for Medium-Term Periods. *IFAC PapersOnLine, 51(30),* 405–409. https://doi.org/10.1016/j.ifacol.2018.11.342
13. Paulson, D. & Wand, Y. (1992). An Automated Approach to Information-Systems Decomposition. *IEEE Transactions on Software Engineering, 3,* 174–189. https://doi.org/10.1109/32.126767
14. Chiriac, N., et al. (2011). Three approaches to complex system decomposition. *13th International DSM Conference,* 3–15
15. Pancerz, K., & Suraj, Z. (2013). A Rough Set Approach to Information Systems Decomposition. *Fundamenta Informaticae, 127 (1–4),* 257–272.
16. Бурячок, В. Л. (2017). Швидкий алгоритм генерації підстановок багато алфавітної заміни. *Захист інформації, 2,* 173–177.
17. Гулак, Є. Г., & Трофімов, О. С. (2024). Формування методики раціонального вибору засобів шифрування для застосування в мережах критичної інфраструктури. *Збірник тез XI Всеукраїнської науково–практичної конференції молодих учених Інформаційні Технології,* 228–230.
18. Корченко, О. Г. (2004). *Системи захисту інформації: Монографія.* НАУ.
19. Гулак, Г. М., Лахно, В. А., & Адилжанова, С. А. (2020). Метод раціонального керування системами кіберзахисту та забезпечення гарантоздатності радіотехнічних систем. *Вісник НТУУ «КПІ». Серія Радіотехніка. Радіоапаратобудування, 83,* 62–68.
20. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. (1999). *Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу* (НД ТЗІ 2.5-004-99).
21. КМ України. (2020). *Про затвердження Технічного регламенту засобів криптографічного захисту інформації.*
22. Бурячок, В. Л. (2011). Метод оцінювання ефективності кібернетичного озброєння з подолання засобів криптографічного захисту інформації. *Інформаційна безпека людини, суспільства, держави, 1(8),* 100–106.
23. Гулак, Г. М. (2018). Оцінка інженерно криптографічних якостей під час тематичних досліджень криптосистем. *Тези 13 Міжнародної наук.-практ. конференції «Математичне та імітаційне моделювання систем МОДС 2018»,* 326–330.
24. Mpekoa, N. (2023). An Analysis of Cybersecurity Architectures. *19th International Conference on Cyber Warfare and Security,* 200–207.
25. Hallman, R., et al. (2020). Return on Cybersecurity Investment in Operational Technology Systems: Quantifying the Value that Cybersecurity Technologies Provide After Integration. *5th International*

*Conference on Complexity, Future Information Systems and Risk.* https://doi.org/10.5220/0009416200430052

26. Hallman, R., et al. (2021) Determining a Return on Investment for Cybersecurity Technologies in Networked Critical Infrastructures. *International Journal of Organizational and Collective Intelligence, 11(2),* 91–110. https://doi.org/10.4018/IJOCI.2021040105
27. Alkiviadis, G. A. (1989). *Elements of Computer Algebra With Applications 1st Edition.* Wiley-Interscience.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

**Yevhen Hulak**
Postgraduate
Institute of Problems of Mathematical Machines and
Systems of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0003-4984-686X
*evgeniygulak@gmail.com*

# METHOD OF RATIONAL SYNTHESIS OF SUBSYSTEMS FOR CRYPTOGRAPHIC PROTECTION OF INFORMATION IN CRITICAL INFRASTRUCTURE NETWORKS

**Abstract.** The article examines the state of development of the methodology for building information protection subsystems of information systems of critical infrastructure objects, and separately highlights the issue of creating complex protection for complex systems. It is noted that complex systems are characterized by the presence of a significant number of disparate elements, which are combined into a single system to achieve a certain goal; the existence of complex, sometimes contradictory relationships and influences; powerful information flows between component subsystems. The analysis of the characteristics of complex information systems, which negatively affect the construction of information protection subsystems, was carried out, and the relevance of solving the tasks of creating complex protection for such systems, especially within the framework of the construction of a network of situation centers, was determined. It is noted that the implementation of a well-designed cryptographic information protection subsystem (CIP), which can provide reliable protection of the confidentiality and integrity of the information processed in the system, contributes to solving a significant number of protection tasks and increasing its effectiveness. As part of determining the conditions for the application of the CIP subsystem in complex systems, the lens of critical infrastructure to ensure information with limited access and control its integrity, a method of decomposition of complex systems of the same type was proposed and a model of cryptographic protection in such systems was improved. Based on the need for implementation as part of the selection process. certain hardware and software technological solutions for the multiple implementation of procedures for quick comparison of a significant number of qualitative (semantic) and quantitative indicators of the information protection subsystem based on the properties of functional profiles, a method of rational selection based on the greatest value of the security function of the means suitable for use in the subsystem is proposed.

**Keywords:** cryptosystem; complex system; critical infrastructure; network of situation centers; decomposition of a complex system; functional security profile.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

1. DSTSZI SSS of Ukraine (2005). *Procedure for conducting work on the creation of a comprehensive information security system in the information and telecommunications system* (ND TZI 3.7-003 -2005)
2. Grechaninov, V.F. (2018). Network of situational centers of public authorities - the basis for improving the efficiency of their activities (interaction). *Mathematical machines and systems, 3,* 32–39.
3. Oksanych, I. M., Grechaninov, V. F., & Lopushansky, A. V. (2020). Information interaction in disparate information systems of situational centers. *Mathematical machines and systems, 3,* 60–68.
4. Grechaninov, V., Hulak, E., Hulak, H., Skladannyi, P., & Sokolov, V. (2021). Decentralized Access Demarcation System Construction in Situational Center Network. *Cybersecurity Providing in Information and Telecommunication Systems (CPITS-II-2021), Vol. 3188,* 197–206.
5. Grechaninov, V., et al. (2022). Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center. In *Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, Vol. 3149,* 107–117.
6. Buslenko, N. P. (1968). *Modeling of complex systems.* Science.
7. Sharakshan, A. S. (1977). *Complex systems: A textbook.* Higher school.
8. Israelov, K.E. (2022). Assessment and prediction of the state of complex objects: application to information security. *Issues of cybersecurity, 6(52),* 2–19.

9. Horban, O. M., & Bakhrushin, V. E. (2004). *Fundamentals of system theory and system analysis. Study guide.* GU "ZIDMU".
10. Yang, K., et al. (2023). Complex systems and network science: a survey. *Journal of Systems Engineering and Electronics, 34(3),* 543–573. https://doi.org/10.23919/JSEE.2023.000080
11. Jewell, J. (2011). *The IEA Model of Short-term Energy Security (MOSES).* Primary Energy Sources and Secondary Fuels, IEA.
12. Nasibov, V., et al. (2018). Models of Electric Power Industry Security Study for Medium-Term Periods. *IFAC PapersOnLine, 51(30),* 405–409. https://doi.org/10.1016/j.ifacol.2018.11.342
13. Paulson, D. & Wand, Y. (1992). An Automated Approach to Information-Systems Decomposition. *IEEE Transactions on Software Engineering, 3,* 174–189. https://doi.org/10.1109/32.126767
14. Chiriac, N., et al. (2011). Three approaches to complex system decomposition. *13th International DSM Conference,* 3–15
15. Pancerz, K., & Suraj, Z. (2013). A Rough Set Approach to Information Systems Decomposition. *Fundamenta Informaticae, 127 (1–4),* 257–272.
16. Buryachok, V. L. (2017). A fast algorithm for generating multi-alphabet substitutions. *Information security, 2,* 173–177.
17. Gulak, E. G., & Trofimov, O. C. (2024). Formation of a methodology for the rational selection of encryption tools for use in critical infrastructure networks. *Collection of abstracts of the XI All-Ukrainian scientific and practical conference of young scientists Information Technologies,* 228–230.
18. Korchenko, O. G. (2004). Information security systems: Monograph. NAU.
19. Gulak, G. M., Lakhno, V. A., & Adilzhanova, S. A. (2020). Method of rational management of cyber defense systems and ensuring the reliability of radio engineering systems. *Bulletin of NTUU "KPI". Series Radio engineering. Radio apparatus construction, 83,* 62–68.
20. Department of Special Telecommunication Systems and Information Protection of the Security Service of Ukraine (1999). *Criteria for assessing the security of information in computer systems from unauthorized access* (ND TZI 2.5-004-99).
21. CM of Ukraine (2020). *On approval of the Technical Regulations of cryptographic information protection means.*
22. Buryachok, V. L. (2011). Method for assessing the effectiveness of cyber weapons to overcome cryptographic information security. *Information security of a person, society, state, 1(8),* 100–106.
23. Gulak, G. M. (2018). Evaluation of engineering and cryptographic qualities during case studies of cryptosystems. *Abstracts of the 13th International Scientific and Practical Conference "Mathematical and Simulation Modeling of MODS 2018",* 326–330.
24. Mpekoa, N. (2023). An Analysis of Cybersecurity Architectures. *19th International Conference on Cyber Warfare and Security,* 200–207.
25. Hallman, R., et al. (2020). Return on Cybersecurity Investment in Operational Technology Systems: Quantifying the Value that Cybersecurity Technologies Provide After Integration. *5th International Conference on Complexity, Future Information Systems and Risk.* https://doi.org/10.5220/0009416200430052
26. Hallman, R., et al. (2021) Determining a Return on Investment for Cybersecurity Technologies in Networked Critical Infrastructures. *International Journal of Organizational and Collective Intelligence, 11(2),* 91–110. https://doi.org/10.4018/IJOCI.2021040105
27. Alkiviadis, G. A. (1989). *Elements of Computer Algebra With Applications 1st Edition.* Wiley-Interscience.