ІНСТИТУТ ПРОБЛЕМ МАТЕМАТИЧНИХ МАШИН І СИСТЕМ
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

ГУЛАК ЄВГЕН ГЕННАДІЙОВИЧ

УДК 004.056.5

ДИСЕРТАЦІЯ

МОДЕЛІ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ ТА КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ЕНЕРГЕТИЧНОГО СЕКТОРУ

Спеціальність 122 «Комп’ютерні науки»

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Є.Г. Гулак

Науковий керівник Складанний Павло Миколайович, кандидат технічних наук, доцент

КИЇВ – 2024

АНОТАЦІЯ

Гулак Є.Г. Моделі та методи забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки». – Інститут проблем математичних машин і систем Національної академії наук України, Київ, 2024.

Дисертація присвячена вирішенню актуального наукового завдання, сутність якого полягає в розробці моделей та методів забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору для підвищення спроможностей Об'єднаних Енергетичних Систем України (ОЕС-У) протистояти кризовим ситуаціям.

Енергетика є високотехнологічною галуззю народного господарства, вона потребує для вирішення завдань управління відповідними електроенергетичними комплексами застосування новітніх інформаційних технологій, що спроможні у реальному часі забезпечувати збирання, передачу, обробку та відображення технологічної інформації для її аналізу персоналом й прийняття на її основі необхідних управлінських рішень.

Зазначене, зокрема, стосується систем управління технологічними процесами, диспетчерського управління електротехнічними підприємствами, контролю якості електричної енергії, обліку електричної енергії тощо.

Складним інформаційним та управляючим системам енергетичного сектору притаманні існування складних, іноді суперечливих зв'язків та взаємних впливів, наявність значної кількості різнорідних компонентів, які для досягнення певної мети об'єднані в єдину систему, наявність багатьох власників та розпорядників у різних підсистемах, що призводить до неузгодженості заходів з захисту та контролю безпеки.

Зазначені фактори, безперечно, ускладнюють впровадження єдиних підходів до реалізації комплексу організаційно-технічних заходів та засобів захисту, виникає низка науково-технічних проблем, які стосуються:

– узгодження порядку та умов корпоративного захисту інформаційно-технологічної системи, яка складається з підсистем різних власників (розпорядників);

– встановлення принципів побудови та вимог з безпеки до шлюзу взаємодії між інформаційно-технологічними підсистемами, щодо яких визначені різні вимоги з безпеки тощо.

Отже, актуальним постає наукове завдання, щодо забезпечення необхідного рівня гарантоздатності та кібербезпеки складної критичної інформаційної інфраструктури енергетичного сектору шляхом побудови корпоративного сегменту кіберзахисту та кіберстійкості, а також реалізації підсистеми криптографічного захисту, що забезпечуватиме підвищений рівень конфіденційності, цілісності та імітостійкості під час взаємодії між різними підсистемами.

Метою дисертаційного дослідження є підвищення гарантоздатності та кібербезпеки інформаційних систем енергетичного сектору завдяки поєднанню корпоративного захисту складної критичної інформаційної інфраструктури на основі розробки відповідних моделей і методів забезпечення кіберзахисту та кіберстійкості з використанням вдосконаленої архітектури та децентралізованого підходу до розмежування доступу в мережі центру кібербезпеки, а також криптографічних рішень для безпечного інформаційного обміну між підсистемами енергетичного сектору.

У відповідності до сформованої мети для вирішення зазначеної науково-прикладної проблеми забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору для підвищення кіберстійкості ОЕС-У в роботі були отримані такі наукові результати:

1. Вперше на основі формування класів еквівалентності запропоновано методику декомпозиції складних систем, що підлягають кіберзахисту, яка

враховує можливість інформаційного обміну між підсистемами з різними вимогами до захисту інформації з обмеженим доступом.

2. Вдосконалено модель побудови корпоративного центру кібербезпеки енергетичного сектору на основі сервіс-орієнтованої архітектури з визначеною бізнес-логікою та відповідним набором функцій, що забезпечуватиме динамічне оброблення кіберінцидентів у реальному часі. Вдосконалена модель відповідає сучасним викликам безпеці та ураховує специфіку завдань і функцій ОЕС-У.

3. Вдосконалено модель побудови децентралізованої системи розмежування доступу в мережі центру кібербезпеки на основі оригінальної методики розподілу секрету. Запропонована модель припускає її масштабування та мінімізує ризик несанкціонованого доступу до інформаційних ресурсів.

4. Подальшого розвитку набула модель побудови підсистеми криптографічного захисту інформації, що забезпечуватиме можливість двоконтурного шифрування для розмежування доступу в децентралізованій системі розмежування доступу до інформаційних ресурсів, розроблені та обґрунтовані рекомендації щодо підвищення безпеки криптографічного захисту інформації коротких службових повідомлень.

5. Подальшого розвитку набула методика оцінки та раціонального визначення характеристик захисту криптографічної підсистеми.

У вступі обґрунтовані актуальність та важливість теми дисертаційного дослідження, сформульована мета та задачі дослідження, визначені основні положення, а також наукова та практична цінність отриманих результатів та зазначено особистий внесок автора.

У першому розділі проведено аналіз поточного стану дослідження наукової проблеми. Сформульовані проблеми та пріоритети забезпечення безпеки у фізичному та цифровому середовищах енергетики. Надано визначення складної системи, обґрунтована необхідність та перспективи аналізу, забезпечення кіберстійкості та гарантоздатності складних

інформаційних систем, до яких, зокрема, відноситься інформаційна інфраструктура Об’єднаних Енергетичних Систем України. Сформульовані функції та завдання суб’єктів управління енергосистемою України. Відмічені особливості убезпечення інтелектуальних енергетичних систем як різновиду систем інтернету речей, мобільного доступу та хмарних технологій в енергетиці та роль мікросервісів.

Проаналізовані проблеми ситуаційного управління в енергетичному секторі та шляхи їх розв’язання. Сформульовані об’єкти захисту в інформаційних системах енергетики, особливості ландшафту кіберзагроз, визначені підходи до формування моделей загроз. Запропонована модель логічних ланцюгів впливу загроз на погіршення спроможності стійкого функціонування енергетичних систем. Дано огляд методів оцінки ризиків стійкості енергосистем. Визначені заходи з кіберзахисту та забезпечення гарантоздатності енергетичних систем. Обґрунтовані мета та задачі дослідження, сформульовані висновки за розділом.

У другому розділі проаналізовані методологічні засади створення та функціонування центру кібербезпеки інформаційної інфраструктури енергетичного сектору.

На прикладі об’єктів ядерної енергетики запропоновано моделі управління кібербезпекою, визначені завдання та функції корпоративного центру кібербезпеки та запропоновано модель його функціонування, визначені інструменти кібербезпеки та модель забезпечення гарантоздатності та кіберзахисту в енергетичних системах в нотації IDEF0, обґрунтовані керівні принципи проєктування та архітектури корпоративного центру кібербезпеки. Запропоновані методика опрацювання кіберінцидентів у центрі кібербезпеки та логічна модель його функціонування.

У рамках аналізу динамічної моделі центру кібербезпеки визначені рівні управління, розглянуті ключові показники ефективності управлінських дій, зокрема, управління культурою кібербезпеки. Визначені та обґрунтовані механізми частково децентралізованого управління доступом у мережі центру

кібербезпеки, основані на криптографічних методах розподілу секретів, та запропонована відповідна методика управління доступом. Зроблені висновки за розділом.

У третьому розділі проаналізовані вразливості шифрування коротких повідомлень у мобільних компонентах та сформульовані критерії їх оцінки на основі статистичного розподілу довжин повідомлень. Піддані аналізу атаки на захищений обмін із метою розпізнавання стану об’єкта та визначені механізми протидії ним.

Запропонована методика декомпозиції складної інформаційної системи критичної інфраструктури та сформульовані відповідні шість спеціальних умов, що позначені, як U1 – U6 передачі інформації з більш захищеної підсистеми в підсистему з меншим рівнем захисту. Запропонована вдосконалена модель криптографічного захисту інформації – шлюзу безпеки, що відповідає визначеним спеціальним умовам. Запропонована методика характеристики показників підсистеми криптографічного захисту та їх раціонального визначення для складних систем. За розділом сформульовані висновки.

У четвертому розділі запропонована вдосконалена на основі результатів дослідження методика побудови системи захисту, що пройшла практичну апробацію. Зроблено висновок про необхідність обов’язкової реалізації пілотного проєкту для проведення дослідної експлуатації складних систем, за результатами якої може бути прийняте рішення щодо уточнення процедури початкової декомпозиції системи. Наведені результати побудови та тестування макетного варіанта мікросервісу – шифратора двоконтурного шифрування. За розділом зроблені висновки.

Узагальнюючим результатом проведених досліджень є сталі моделі функціонування та архітектури корпоративного центру кібербезпеки з частково децентралізованим розмежуванням доступу на основі схеми розподілу секрету з використанням криптографічного захисту, а також вдосконалена модель криптографічного захисту, що відповідає спеціальним

умовам передачі інформації з підсистем із вищим рівнем безпеки у підсистеми з більш низьким рівнем безпеки, що відповідає актуальним потребам убезпечення інформаційних систем енергетичного сектору.

Дисертація виконувалась в Інституті проблем математичних машин і систем Національної академії наук України.

Результати наукових досліджень були використані під час наукової і науково-технічної діяльності Інституту проблем математичних машин і систем Національної академії наук України в рамках виконання за державним замовленням науково-дослідних робіт: шифр «Ситуаційне управління» (№0122U201115, ІПММС, м. Київ) та шифр «ІПММС-2021» (№0121U000107, ІПММС, м. Київ), прийняті до реалізації у науково-дослідній діяльності Інституту проблем безпеки атомних електростанцій Національної академії наук України з метою покращення кіберзахисту енергосистем та впроваджені в освітній процес Київського столичного університету імені Бориса Грінченка.

Ключові слова: кібербезпека, захист інформації, модель загроз, вразливість, розмежування доступу, складна система, автентифікація, сервіс-орієнтована архітектура, криптографічний захист, шифрування, конфіденційність, ситуаційний центр, інтернет речей, об’єкт критичної інфраструктури.

ABSTRACT

Hulak Y.H. Models and methods of guaranteeing capability and cyber security of information and communication systems of the energy sector. – Qualifying scientific work on manuscript rights.

Dissertation for obtaining the degree of Doctor of Philosophy in the specialty 122 «Computer Science». – Institute of Problems of Mathematical Machines and Systems of the National Academy of Sciences of Ukraine, Kyiv, 2024.

The dissertation is devoted to the solution of an actual scientific task, the essence of which is the development of models and methods for ensuring the guarantee capability and cyber security of information and communication systems of the energy sector in order to increase the capabilities of the United Energy Systems of Ukraine (UES-U) to withstand crisis situations.

Energy is a high-tech branch of the national economy, it requires the use of the latest information technologies capable of providing real-time collection, transmission, processing and display of technological information for its analysis by personnel and making the necessary management decisions based on it in order to solve the tasks of managing the relevant electric power complexes.

This applies, in particular, to systems for managing technological processes, dispatching control of electrical engineering enterprises, quality control of electrical energy, accounting for electrical energy, etc.

Complex information and management systems of the energy sector are characterized by the existence of complex, sometimes contradictory relationships and mutual influences, the presence of a significant number of heterogeneous components that are combined into a single system to achieve a certain goal, the presence of many owners and managers in different subsystems, which leads to inconsistencies in security protection and control measures.

These factors undoubtedly complicate the implementation of unified approaches to the implementation of a complex of organizational and technical

means and protection measures, a number of scientific and technical problems arise, which concern:

– coordination of the order and conditions of corporate protection of the information technology system, which consists of subsystems of different owners (administrators);

– establishment of construction principles and security requirements for the gateway of interaction between information technology subsystems, for which various security requirements are defined, etc.

Therefore, the scientific task of ensuring the necessary level of cyber security and guarantee capability of the complex critical information infrastructure of the energy sector by building a corporate segment of cyber protection and cyber resilience, as well as implementing a cryptographic protection subsystem, which will ensure an increased level of confidentiality and impersonation resistance during interaction between different subsystems, becomes urgent.

The aim of the dissertation research is to increase the cyber security and guarantee capacity of information systems of the energy sector thanks to the combination of corporate protection of complex critical information infrastructure based on the development of appropriate models and methods for ensuring cyber protection and cyber resilience using an improved architecture and a decentralized approach to delimiting access in the network of the cyber security center and new cryptographic solutions for secure information exchange between subsystems of energy sector systems.

In accordance with the formed goal to solve the specified scientific and applied problem of ensuring the guaranteeability and cyber security of information and communication systems of the energy sector to increase the cyber resilience of UES-U, the following scientific results were obtained in the work:

1. For the first time, based on the formation of equivalence classes, a method of decomposition of complex systems subject to cyber protection is proposed, which takes into account the possibility of information exchange between subsystems with different requirements for protecting information with limited access.

2. The model of building a corporate cyber security center of the energy sector based on a service-oriented architecture with a defined business logic and a corresponding set of functions that will ensure dynamic processing of cyber incidents in real time has been improved. The improved model meets modern security challenges and takes into account the specific tasks and functions of the UES-U.

3. The model of building a decentralized system of delimiting access in the network of the cyber security center based on the original method of secret distribution has been improved. The proposed model assumes its scaling and minimizes the risk of unauthorized access to information resources.

4. The model of building a subsystem of cryptographic protection of information gained further development, which will provide the possibility of double-circuit encryption for delimiting access in a decentralized system of delimiting access to information resources, developed and substantiated recommendations to increase the security of cryptographic protection of information of short service messages.

5. The method of evaluation and rational determination of the characteristics of the protection of the cryptographic subsystem acquired further development.

The introduction substantiates the relevance and importance of the topic of the dissertation research, formulates the purpose and tasks of the research, defines the main provisions, as well as the scientific and practical value of the obtained results, and indicates the personal contribution of the author.

In the first chapter, an analysis of the current state of scientific problem research is carried out. Formulated problems and priorities of ensuring security in physical and digital energy environments. The definition of a complex system is provided, the justified need and prospects for analysis, ensuring cyber resistance and guarantee capability of complex information systems, which, in particular, include the information infrastructure of the United Energy Systems of Ukraine. Formulated functions and tasks of entities managing the energy system of Ukraine. The features

of securing intelligent energy systems as a type of Internet of Things systems, mobile access and cloud technologies in energy and the role of microservices are noted.

The problems of situational management in the energy sector and ways to solve them are analyzed. The objects of protection in energy information systems are formulated, features of the landscape of cyber threats, approaches to the formation of threat models are defined. The proposed model of logical chains of the influence of threats on the deterioration of the ability of sustainable functioning of energy systems. An overview of methods for assessing the risks of power system stability is given. Determined measures for cyber protection and ensuring the guarantee capacity of energy systems. The purpose and objectives of the research are substantiated, conclusions are formulated by section.

The second chapter analyzes the methodological foundations of the creation and functioning of the cyber security center of the information infrastructure of the energy sector.

On the example of nuclear energy facilities, cyber security management models are proposed, tasks and functions of the corporate cyber security center are defined and a model of its functioning is proposed, cyber security tools are defined and a model for guaranteeing capability and cyber protection in energy systems in the IDEF0 notation, well-founded guiding principles for the design and architecture of the corporate cyber security center . The method of processing cyber incidents in the cyber security center and the logical model of its functioning are proposed.

As part of the analysis of the dynamic model of the cyber security center, the levels of management are determined, the key indicators of the effectiveness of management actions are considered, in particular, the management of the culture of cyber security. The mechanisms of partially decentralized access control in the network of the cyber security center, based on cryptographic methods of secret distribution, are defined and substantiated, and the corresponding access control method is proposed. Conclusions are drawn according to the section.

The third section analyzes the vulnerabilities of short message encryption in mobile components and formulates criteria for their assessment based on the

statistical distribution of message lengths. Analyzed attacks on protected exchange for the purpose of recognizing the state of the object and defined mechanisms for countering them.

The method of decomposition of the complex information system of critical infrastructure is proposed and the corresponding six special conditions, marked as U1 – U6, of information transfer from a more protected subsystem to a subsystem with a lower level of protection are formulated. An improved model of cryptographic protection of information – a security gateway that meets the specified special conditions – is proposed. The method of characterizing cryptographic protection subsystem indicators and their rational determination for complex systems is proposed. Conclusions are formulated according to the section.

In the fourth chapter, based on the results of the research, the method of building a protection system, which has passed practical approval, is proposed. A conclusion was made about the necessity of mandatory implementation of a pilot project for experimental operation of complex systems, based on the results of which a decision can be made to clarify the procedure for the initial decomposition of the system. The results of construction and testing of a mock-up version of the microservice – a two-loop encryption cipher are given. Conclusions are drawn according to the section.

The general result of the conducted research was a model of the functioning and architecture of the corporate cyber security center with partially decentralized delimitation of access based on a secret distribution scheme using cryptographic protection, as well as an improved model of cryptographic protection that meets the special conditions of information transfer from subsystems with a higher level of security to subsystems with a lower level a level of security that meets the current needs of securing information systems of the energy sector.

The dissertation was completed at the Institute of Problems of Mathematical Machines and Systems of the National Academy of Sciences of Ukraine.

The results of scientific research were used during the scientific and scientific-technical activities of the Institute of Problems of Mathematical Machines and

Systems of the National Academy of Sciences of Ukraine as part of the implementation of state-ordered research works: code "Situational management" (No. 0122U201115, IPMMS, Kyiv) and cipher "IPMMS-2021" (No. 0121U000107, IPMMS, Kyiv), accepted for implementation in the research activity of the Institute of Nuclear Power Plant Safety Problems of the National Academy of Sciences of Ukraine with the aim of improving the cyber protection of power systems and introduced into the educational process of the Boris Grinchenko Kyiv Metropolitan University.

Keywords: cyber security, information protection, threat model, vulnerability, access demarcation, complex system, authentication, service-oriented architecture, cryptographic protection, encryption, privacy, situation center, Internet of things, an object of critical infrastructure.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Гулак Г. М., Скітер І. С., Гулак Є. Г. (2021) Методологічні засади створення та функціонування центру кібербезпеки інформаційної інфраструктури об'єктів ядерної енергетики. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2021. Т. 4, № 12. С. 172–186. DOI: https://doi.org/10.28925/2663-4023.2021.12.172186. *Бази: CrossRef, Google Scholar.*

2. Деренговський В.В., Кафтанатіна О.А., Кордюков П.Л., Меньшенін Є.А., Гулак Є.Г. (2021) Розробка математичної моделі впливу радіаційно небезпечних об’єктів на довкілля при пожежі. Математичні машини і системи. 2021. №4. С. 99–111. DOI: https://doi.org/10.34121/1028-9763-2021-4-99-111. *Бази: CrossRef, Google Scholar.*

3. Гулак Г., Жданова Ю., Складанний П., Гулак Є., Корнієць В. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об’єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2022. №1 (17). С. 145–158. DOI: https://doi.org/10.28925/2663-4023.2022.17.145158. *Бази: CrossRef, Google Scholar.*

4. Hulak H., Skladannyi P., Sokolov V., Hulak E., Korniiets V., Dynamic Model of Guarantee Capacity and Cyber Security Management in the Critical Automated System, 2nd International Conference on Conflict Management in Global Information Networks: November 2022, Kyiv, Ukraine. 2022. Vol. 3530. P. 102–111. ISSN: 1613-0073. *Бази: Scopus, CrossRef, Google Scholar.*

5. Гулак Є. Г. (2024) Методика раціонального синтезу підсистеми криптографічного захисту інформації в мережах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».

2024. № 4(24). С. 282–297. DOI: https://doi.org/10.28925/2663-4023.2024.24.282297. *Бази: CrossRef, Google Scholar.*

Наукові праці, які засвідчують апробацію матеріалів дисертації:

6. Гулак Г.М., Гулак Є.Г., Корнієць В.А. (2023) Безпека шифрування коротких повідомлень в інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Актуальні проблеми управління інформаційною безпекою держави. Київ, 2023. С. 260–262.

7. Гулак Г. М., Скітер І. С., Гулак Є. Г., Цирканюк Д. А. (2023) Базові засади побудови центру кібербезпеки об`єктів ядерної енергетики. Актуальні проблеми управління інформаційною безпекою держави. Київ, 2023. С. 262–266.

Наукові праці, які додатково відображають наукові результати дисертації:

8. Morozov A., Hrebennyk A., Trunova E., Skiter I., Hulak E. Design of Industry Centers of Cyber Security of Facilities of Critical Infrastructure. Workshop on Cybersecurity Providing in Information and Telecommunication Systems CPITS-II-2021: October 26, 2021, Kyiv, Ukraine, 2021. Vol. 3187. P. 27–37. ISSN: 1613-0073. *Бази: Scopus, CrossRef, Google Scholar.*

9. Hulak H., Grechaninov V., Hulak E., Skladannyi P., Sokolov V. Decentralized Access Demarcation System Construction in Situational Center Network. Cybersecurity Providing in Information and telecommunication Systems (CPITS-II-2021): October 26, 2021, Kyiv, Ukraine, 2021. Vol. 3188. P. 197–206. ISSN: 1613-0073. *Бази: Scopus, CrossRef, Google Scholar.*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АУІС – автоматизована управляюча та інформаційна система.

БМ – база даних моделей кіберінцидентів.

БШ – база даних шаблонів обробки кіберінцидентів.

ЕЕС – електроенергетичні системи.

ДТЕК – Донбаська паливно-енергетична компанія.

ЄС – Європейський Союз.

ЗГІУС – захищена гарантоздатна інформаційно управляюча система.

ІКС-ЕС – інформаційно-комунікаційна система енергетичного сектору.

МЕМ – магістральні електричні мережі.

НЕК – Національна енергетична компанія.

ОЕС-У – Об'єднана енергетична система України.

ОКІ – об'єкт(и) критичної інфраструктури.

ОЯЕ – об'єкти ядерної енергетики.

КІ-ЕС – критична інфраструктура енергетичного сектору.

КЗІ – криптографічний захист інформації.

КтГ – кібербезпека та гарантоздатність.

КЦК ОЯЕ – корпоративний центр кібербезпеки об'єкта ядерної енергетики.

МХПП – множина характеристичних показників поведінки.

ПІБ – політика інформаційної безпеки.

СЄД-ОТУ – система єдиного диспетчерського (оперативно-технологічного) управління.

СРД – система розмежування доступу.

ЦК ОКІ – центр кібербезпеки об'єктів критичної інфраструктури.

ЦСРД – централізована система управління доступом.

ACDA – Americas Cyber Defense Agency.

CBC – Cipher Block Chaining.

CS – complex system.

CPPS – Cyber-Physical Power System.

ECB – Electronic Code Book.

ENISA – European Union Agency for Cybersecurity.

IBE – Identity Based Broadcast Encryption.

IoT – Internet of Things.

MISP-UA – Malware Information Sharing Platform and Threat Sharing «Ukrainian Advantage».

SCADA – Supervisory Control and Data Acquisition.

SIEM – Security information and event management.

SMS – Short Message Service.

SNS – Social Network Service.

SOC – Security Operation Center.

SOS – speed of service.

ВСТУП

Актуальність теми

Світовий досвід розвитку сучасного постіндустріального суспільства свідчить, що підвищення його економічного добробуту, забезпечення нагальних соціальних та культурних потреб громадян, підвищення рівня національної безпеки і оборони базуються на сталому безпечному функціонуванні паливно-енергетичного комплекси країни, його стійкості щодо ризиків реалізації загроз природнього, техногенного та антропогенного характеру. За суттю енергетика дає життя всім іншим галузям промисловості.

В умовах обмежених природних ресурсів викопного палива, включаючи нафту та природний газ, складності і високої собівартості видобутку вугілля галузь електроенергетики з урахуванням екологічності її складових – сонячної, вітрової, атомної та гідроенергетики – у стратегічному плані є безумовним пріоритетом для інвестицій та інновацій.

Ця галузь народного господарства є високотехнологічною, вона потребує для вирішення завдань управління відповідними електроенергетичними комплексами застосування новітніх інформаційних технологій, що спроможні у реальному часі забезпечувати збирання, передачу, обробку та відображення технологічної інформації для її аналізу персоналом й прийняття на її основі необхідних управлінських рішень, зокрема, в системах управління технологічними процесами, контролю якості електричної енергії, диспетчерського управління електротехнічними підприємствами, обліку електричної енергії тощо.

Події останніх років свідчать про надзвичайну вразливість галузі щодо зовнішніх та внутрішніх загроз, які можуть призводити до часткового або повного руйнування інформаційного обміну в сенсі порушення конфіденційності, цілісності та доступності інформаційних ресурсів та технологічної інформації, а також спостереженості процесів і процедур.

Наслідком відповідних інформаційних інцидентів (інцидентів із кібербезпекою) можуть бути суттєве зниження якості обслуговування споживачів, тривали перебої з електропостачанням і навіть створення передумов для виникнення важких техногенних катастроф із численними людськими жертвами та матеріальними втратами.

Зважаючи на те, що ІКС-ЕК у загальному випадку є складною системою з точки зору побудови комплексу організаційно-технічних засобів та заходів захисту, виникає низка науково-технічних проблем що, зокрема, стосуються:

– порядку та умов корпоративного захисту інформаційно-технологічної системи, яка складається з підсистем різних власників (розпорядників);

– її декомпозиції на більш прості для захисту підсистеми;

– принципів побудови та вимог з безпеки до шлюзу взаємодії між інформаційно-технологічними підсистемами, щодо яких визначені різні вимоги з безпеки тощо.

Доволі ефективним інструментом вирішення багатьох проблемних питань убезпечення об’єктів інформаційної діяльності є методи та засоби криптографічного захисту інформації, застосування яких у багатьох випадках забезпечує гарантоване дотримання встановлених вимог щодо конфіденційності та цілісності інформаційних активів.

Різним аспектам забезпечення кіберзахисту та гарантоздатності ІКС-ЕС присвячені дослідження провідних вітчизняних та іноземних вчених, як-от О. Корченко, О. Федухін, В. Харченко, С. Гончар, В. Глухов, О. Богданов, Thomas R. Peltier, A. Avizienis, Pete Burnap, Andrew Blyth, Hugh Soulsby, Kevin Jones, Peter Eden, Kristan Stoddart та інші.

Вирішенню проблем інформаційної безпеки та криптографічного захисту присвячені роботи багатьох провідних вітчизняних та іноземних вчених, як-от І. Коваленко, М. Шелест, В. Бурячок, І. Горбенко, М. Савчук, С. Гнатюк, А. Олексійчук, Л. Ковальчук, C.E. Shannon, W. Diffie, M. Hellman та інші.

Водночас, незважаючи на значну кількість підходів до вирішення проблеми побудови гарантоздатних захищених систем інформаційного обміну в енергетичній галузі, вона залишається остаточно нерозв'язаною та актуальною не тільки для України, але і для всієї світової спільноти.

У зв'язку з цим існує необхідність вирішення актуального наукового завдання, сутність якого полягає в розробці моделей та методів забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору

Зв'язок роботи з науковими програмами, планами, темами

Напрям дисертаційного дослідження безпосередньо пов'язаний з реалізацією доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України. Дисертація виконана відповідно до планів наукової і науково-технічної діяльності Інституту проблем математичних машин і систем Національної академії наук України в рамках виконання за державним замовленням науково-дослідних робіт: шифр «Ситуаційне управління» (№ д.р. 0122U201115, ІПММС, м. Київ) та шифр «ІПММС-2021» (№ д.р. 0121U000107, ІПММС, м. Київ).

Мета і завдання дослідження

Забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору шляхом захисту інформаційних ресурсів та технологічної інформації від загроз конфіденційності, цілісності та доступності за рахунок реалізації концепції корпоративного кіберзахисту, розробки молей і методів криптографічного захисту інформації, що збирається, передається та обробляється в ІКС-ЕС.

Відповідно до поставленої мети, для вирішення наукового завдання в роботі сформульовані такі часткові завдання дослідження:

1. Побудувати модель центру корпоративного захисту інформації в ІКС-ЕС, що відповідає сучасним викликам безпеці та ураховує специфіку завдань і функцій ОЕС-У.

2. Розробити модель побудови децентралізованої системи розмежування доступу в мережі центру кібербезпеки.

3. Розробити методику декомпозиції складної інформаційної системи критичної інфраструктури.

4. Вдосконалити модель підсистеми криптографічного захисту інформації в ІКС-ЕС, включаючи розробку методу оцінки безпеки шифрування коротких повідомлень у мобільних компонентах ІКС-ЕС.

5. Розробити методику оцінки та раціонального визначення характеристик захисту криптографічної підсистеми.

Об’єкт дослідження – процеси забезпечення гарантоздатності та кібербезпеки інформаційної інфраструктури об’єктів критичної інфраструктури (ОКІ) енергетичного сектору.

Предметом дослідження є моделі та методи забезпечення гарантоздатності ІКС-ЕС, корпоративного захисту інформації в них та криптографічного захисту інформаційних ресурсів та технологічної інформації, що збирається, передається та обробляється в ІКС-ЕС.

Методи дослідження. Системний аналіз; методи індукції, дедукції та моделювання; системно-структурний підхід, теорія ймовірностей і математична статистика, теорія графів.

Наукова новизна отриманих результатів

Вперше запропоновано методику декомпозиції складної інформаційної системи критичної інфраструктури, оцінки характеристик підсистеми криптографічного захисту та їх раціонального визначення

Вдосконалено модель підсистеми криптографічного захисту інформації в ІКС-ЕС, що враховує можливість взаємодії інформаційних підсистем із різними рівнями щодо забезпечення безпеки інформації, та запропоновано метод оцінки безпеки шифрування коротких повідомлень у мобільних компонентах ІКС-ЕС.

Подальшого розвитку набула модель розмежування доступу в мережі центру кібербезпеки на основі часткової децентралізації підсистеми управління доступом.

Практичне значення отриманих результатів полягає у їхній застосовності для підвищення кібербезпеки інформаційно-комунікаційних систем енергетичного сектору, що є критично важливими для функціонування держави. Розроблена методика декомпозиції складних систем на основі класів еквівалентності дозволяє ефективно сегментувати системи та оптимізувати їхній захист, враховуючи специфічні вимоги до безпеки окремих підсистем.

Вдосконалена модель корпоративного центру кібербезпеки енергетичного сектору забезпечує динамічну обробку кіберінцидентів у реальному часі, відповідаючи сучасним викликам безпеки та специфіці енергосистем. Це сприяє зниженню ризиків каскадних ефектів та підвищенню стійкості енергетичних об'єктів як критичної інфраструктури.

Розроблені моделі криптографічного захисту, включаючи двоконтурне шифрування та методику розподілу секрету, дозволяють значно знизити ризики несанкціонованого доступу до інформаційних ресурсів. Їх масштабованість та адаптивність забезпечують ефективний захист у складних децентралізованих системах.

Запропоновані рішення були впроваджені у межах виконання державних науково-дослідних програм в Інституті проблем математичних машин і систем НАН України, де вони використовувались для вдосконалення архітектури та функціональності ситуаційних центрів об’єктів критичної інфраструктури. Також результати знайшли застосування в Інституті проблем безпеки атомних електростанцій НАН України для посилення кібербезпеки інформаційної інфраструктури енергосистем. Крім того, розробки інтегровані в освітній процес Київського університету імені Бориса Грінченка, що сприяє підготовці висококваліфікованих фахівців для потреб енергетичного сектору.

Особистий внесок здобувача. До дисертації увійшли наукові результати, отримані здобувачем особисто. З наукових праць, опублікованих

у співавторстві, в дисертації використано лише ті ідеї та положення, які є результатом особистої роботи здобувача.

У спільних публікаціях автору належать такі результати.

У роботах [81, 199] здобувачем запропонована архітектура центру кібербезпеки та визначені його завдання.

У науковій публікації [67] визначені вторинні наслідки реалізації загроз та особливості нанесення шкоди у разі виникнення надзвичайних ситуацій.

У публікаціях [66, 198] здобувачем проаналізовані загрози небезпеки шифрування коротких повідомлень, визначені критерії виявлення загроз та методи протидії реалізації визначених загроз.

У роботі [100] здобувачем запропонована динамічна модель управління гарантоздатністю та кібербезпекою в автоматизованих системах критичної інфраструктури.

У роботі [98] В роботі здобувачем запропонована архітектура центру кібербезпеки критичної інфраструктури та визначені його функції.

У роботі [200] Здобувачем запропонована оригінальне криптографічне рішення для розмежування доступу в мережі ситуаційного центру критичної інфраструктури.

Апробація результатів дисертації

Основні теоретичні та практичні результати досліджень були представлені та обговорені на таких наукових конференціях:

1. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS-II-2021) (Kyiv, Ukraine, October 26, 2021).

2. 2nd International Conference on Conflict Management in Global Information Networks (Kyiv, Ukraine, November, 2022).

3. Науково-практична конференція «Кібербезпека енергетики» (м. Київ, Україна, 31 травня 2023 року).

4. XI Всеукраїнська науково–практична конференція молодих учених. Інформаційні технології – 2024 (м. Київ, Україна, 16 травня 2024 року).

Публікації. Результати проведеного дисертаційного дослідження було опубліковано у 9 наукових публікаціях, а саме: 6 у наукових виданнях (із них 5 у співавторстві), включених на дату опублікування до переліку наукових фахових видань України, 3 статті (з них 3 у співавторстві) у періодичному науковому виданні, проіндексованому у базі даних Scopus.

Структура та обсяг дисертації

Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел із 200 найменувань та 3 додатків. Загальний обсяг роботи становить 201 сторінку, у тому числі 149 сторінок основного тексту. Дисертація містить 28 рисунків та 6 таблиць.

РОЗДІЛ 1
АНАЛІЗ СТАНУ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ ТА КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ ЕНЕРГЕТИЧНОГО СЕКТОРУ

1.1 Енергетика як складова критичної інфраструктури

1.1.1 Енергетична галузь та сучасне суспільство

Виходячи з принципів системного підходу до пізнання світу, можливо стверджувати, що енергетична галузь сучасного постіндустріального суспільства є базисом для існування, безпечного функціонування та поступового розвитку інших галузей та об'єктів суспільного виробництва. Зокрема, це стосується практично всіх структур, що, відповідно до законодавчих визначень, мають бути віднесені до об'єктів критичної інфраструктури, включаючи підприємства машинобудування, зв'язку, транспорту тощо.

Так само стан та розвиток ОКІ поза межами енергетики безпосередньо впливають на її стійке функціонування та невпинний прогрес. Прикладом цього є процеси цифровізації галузі, які сприяють підвищенню її ефективності, функціональної безпеки, інвестиційної привабливості.

Цифровізація та повсюдне використання інформаційних технологій в енергетичному секторі надають можливість оперативного управління надскладними технологічними процесами, скорочують час, необхідний для оцінки ситуацій та прийняття адекватних управлінських рішень, забезпечують дистанційне діагностування і контроль стану обладнання та якості електроенергії, підтримують взаємодію складових системи, автоматизують процедури обліку спожитої енергії, а також вирішують багато інших важливих завдань [1].

Надзвичайно тісне переплетіння проблем інформаційних технологій і процесів в енергетичному секторі висвітлено у всеосяжному документі ЄС

Стратегії безпеки Союзу [2], що визначає орієнтири забезпечення безпеки як у фізичному, так і в цифровому світі в усіх складових європейського суспільства.

Ця Стратегія, відмічаючи потребу у реалізації визначених галузевих ініціатив, особливо в секторі енергетики, окреслює ініціативу майбутнього, яка спрямована на підвищення стійкості (resilience) критичної енергетичної інфраструктури по відношенню до потенційних загроз фізичного, кібернетичного або гібридного характеру. Це, на думку євродепутатів, повинно також забезпечувати рівні умови для транскордонної взаємодії операторів енергетичного сектору.

Стратегія включає заходи та інструменти та, які необхідно розробити для забезпечення безпеки у нашому фізичному та цифровому середовищах. На рис. 1.1 зображена загальна структура документа, яка фокусується на чотирьох пріоритетах:

1. Перспективне середовище безпеки.
2. Протидія зростаючим загрозам.
3. Захист європейців від тероризму та організованої злочинності.
4. Потужна екосистема безпеки.

У Стратегії зазначено [2], що існуюча в ЄС загальна правова основа кібербезпеки дає основні орієнтири для реалізації заходів із кіберзахисту енергетичному сектору водночас необхідно враховувати притаманні йому специфічні властивості та умови функціонування, а саме:

1. Вимоги реального часу. Деякі енергетичні системи повинні реагувати настільки швидко, що типові заходи безпеки, як-от, наприклад, автентифікація команди за допомогою цифрового підпису, просто не можуть бути реалізовані внаслідок часової затримки, яка обумовлена реалізацією такої процедури.

2. Каскадні ефекти. Електричні мережі та газогони тісно взаємопов'язані по всій Європі та за межами ЄС. Вимкнення електроенергії в одній країні може спровокувати відключення електроенергії або перебої в електропостачанні в інших регіонах та країнах.

Поєднання застарілих рішень із сучасними технологіями. Багато складових енергетичних систем було спроєктовано та побудовано задовго до того, як виникли реалії забезпечення кібербезпеки. В сучасних умовах цей комплекс засобів та обладнання попри виникаючи загрози повинен стабільно взаємодіяти з найновішим обладнанням для автоматизованого управління та контролю, включаючи інтелектуальні лічильники, пристрої Інтернету речей.

Рисунок 1.1 – Структура Стратегії безпеки ЄС

З метою вирішення проблем кібербезпеки, підвищення освіченості та готовності до дій в енергетиці ЄС у рамках Рекомендації [3] та робочого документа персоналу [4] затвердила вказівки для окремих секторів, які покращують процеси впровадження горизонтальних правил кібербезпеки.

Американська агенція з кібероборони (Americas Cyber Defense Agency – ACDA) – національний координатор безпеки та резільєнтності критичної інфраструктури констатує [5], що без стабільного енергопостачання здоров'я та добробут знаходяться під загрозою, а економіка США не може функціонувати. Директива Президента визначає енергетичний сектор як виключно критичний, оскільки він забезпечує «функцію сприяння» в усіх секторах критичної інфраструктури.

Запропонований агенцією ACDA План для окремих енергетичних секторів (Energy Sector-Specific Plan) докладно описує [6], як реалізується управління ризиками відповідно до Національного плану захисту інфраструктури з урахуванням особливостей галузі і ландшафту кіберизиків у цьому секторі. Секторальні агентства з управління ризиками, координуючи зусилля з партнерами з державного та приватного секторів, розробляють конкретні плани для відповідних секторів. Функції Агентства з управління ризиками в енергетичному секторі при цьому виконує Міністерство енергетики США.

Слід звернути увагу, що визначення умов захисту автоматизованих управляючих та інформаційних систем суттєво залежить від типу ОКІ, його складності та вразливості, 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 рівнів безпеки підсистем, що складають електроенергетику, під егідою Міжнародного енергетичного агентства розроблено та запропоновано в [7] Модель короткострокової енергетичної безпеки (MOSES), в якій профілі безпеки в умовах впливу зовнішніх та внутрішніх факторів залежно від можливого рівня ризику та стійкості кодифікуються літерними символами від A до E .

Зважаючи на те, що границі між рівнями безпеки в першоджерелі кількісно не визначені, на рис. 1.2 подане умовне зображення наведеної в [7] моделі, де зона позначена, як Група A. Вона відповідає найменшим ризикам і високій стійкості. Група E – найбільшим ризикам і найнижчій стійкості. Якщо застосувати лінгвістичні змінні [8] до класифікації захищеності підсистем, що складають електроенергетику, то можна отримати такі наближені відповідності: A – відмінно, B – нормально, C – непогано, D – погано та E – дуже погано.

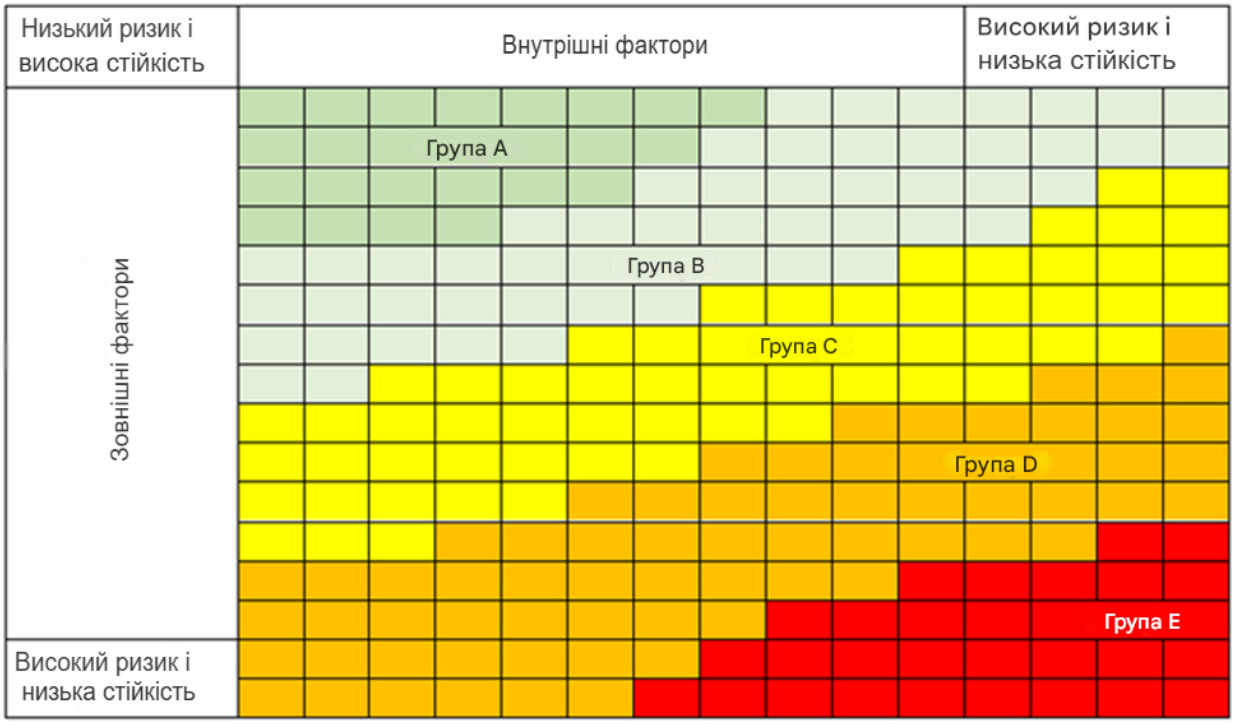

Рисунок 1.2 – Модель профілів безпеки галузі електроенергетики MOSES

Хоча наведена модель не дає прямої відповіді щодо кількісних показників системи захисту інформації, проте у подальшому вона буде в нагоді для формування функціональних профілів захисту інформаційних систем сектору електроенергетики.

Базовим документом для дослідження концептуальних засад забезпечення фізичної та кібернетичної безпеки галузі електроенергетики є Стратегія енергетичної безпеки України [8], спрямована на досягнення стійкості функціонування її енергетичного сектора та визначає серед інших викликів безпеці галузі такі загрози антропогенного, техногенного та природнього походження.

Закон визначає становище погіршення спроможності стійкового функціонування енергетичного сектору та його головного показника – якості електричної енергії [1] як надзвичайну ситуацію в об’єднаній енергетичній системі України, за якої виникає загрози порушення сталого режиму роботи цієї системи або її складових, зокрема, внаслідок дефіциту електричної енергії

та/або потужності, зниження частоти нижче гранично допустимих меж, порушення режиму допустимих перетоків і перевантаження мережевих елементів, зниження напруги в контрольних точках енергосистеми до аварійного рівня, руйнування окремих елементів технологічної інфраструктури.

Загалом все це може мати наслідком підвищення ризиків нанесення шкоди життю і здоров'ю людини, безпеці суспільства, стану навколишнього середовища [67].

У визначених умовах логічним постає визначення в стратегії енергетичної безпеки серед пріоритетних завдань [7] досягнення стратегічної цілі – стійкості функціонування енергетичного сектору шляхом:

– забезпечення кібербезпеки та фізичної безпеки критичної інфраструктури енергетичного сектору;

– формування системи запобігання реалізації загроз будь-якого типу та реагування на випадок кризових ситуацій, запровадження плану енергетичної стійкості України;

– запровадження системи проведення оцінки ризиків та обміну інформацією про ризики та загрози критичній інфраструктурі енергетичного сектору.

З метою більш детального вивчення енергетичного сектору як об'єкта інформатизації та об'єкта побудови системи кіберзахисту уявляється доцільним проаналізувати його структуру та ключові властивості, що мають суттєвий вплив на архітектуру та принципи побудови системи захисту.

Основою вітчизняної електроенергетики, згідно з Законом [1], є об'єднана електроенергетична система України (ОЕС-У), яка здійснює енергопостачання побутовим та промисловим споживачам і взаємодіє з енергосистемами інших країн шляхом імпорту та експорту електричної енергії.

З позицій системного аналізу, сучасна електроенергетична система є організаційно-технічним комплексом, який включає певну множину різноманітного електричного обладнання, що поєднане за допомогою

електричних мереж та взаємодіє у регульованому режимі зі споживачами електричної енергії.

Головним завданням функціонування енергетичної системи (метою бізнесу) є забезпечення майже безперервного процесу виробництва, перетворення та розподілу електроенергії та тепла за допомогою електростанцій, електричних та теплових мереж за умови ефективного керування (менеджменту) цим процесом за допомогою автоматизованих систем управління. Відповідно до Закону [1], під безпекою постачання електричної енергії розуміється спроможність електроенергетичної галузі забезпечувати потреби споживачів в електричній енергії відповідно до встановлених вимог.

Менеджмент в енергетиці, використовуючи сучасні інформаційні технології, забезпечує оперативне керування процесами раціонального використання електричної енергії на всіх стадіях її виробництва, передачі, розподілу і споживання, включаючи розв'язання комплексу технологічних, економічних та екологічних проблем, що обумовлені відповідними процесами.

Реалізація зазначеної мети забезпечується технологічними складовими виробництва енергії, що включають:

– єдину централізовану диспетчерську систему оперативно-технологічного управління (ЦД-ОТУ) виробництвом, передачі та розподілу електричної енергії;

– суб’єкти договору Оптового ринку електричної енергії, який регулюється правилами, що визначають механізм його функціонування, порядок розподілу навантаження між джерелами генерації енергії, а також правила формування оптової ціни на електроенергію;

– електроенергетичні системи (ЕЕС) та магістральні електричні мережі (МЕМ) Національної енергетичної компанії (НЕК) «Укренерго»;

– генеруючі компанії, що включають теплові, атомні, гідравлічні та вітрові електричні станції;

– енергопостачальні компанії з електричними стаціями, що входять до їхнього складу;

– теплоелектроцентралі, а також магістральні теплові мережі з під’єднаними до них джерелами теплопостачання.

Можливо констатувати, що з позицій теорії управління та системного аналізу енергосистема України являє собою складну систему, яка включає у ролі підсистем потужності з генерації електричної енергії – електростанції, магістральні та розподільчі електричні мережі.

Забезпечення цілісності, надійне та ефективне функціонування цього комплексу електроустановок – сукупності взаємопов’язаних устаткування і споруд, що призначені для виробництва або перетворення, передачі, розподілу, споживання електричної енергії чи зберігання енергії досягається за допомогою системи єдиного диспетчерського (оперативно-технологічного) управління (далі СЄД-ОТУ).

Для вирішення окремих завдань діспетчерського управління підстанціями та збору даних використовуються сучасні SCADA-системи, які вирішують такі завдання [72]:

– обробка даних та обмін даними з обладнанням зв'язку з об'єктом, що включає промислові контролери та плати вводу-виводу в реальному часі;

– ведення бази даних технологічної інформації в режимі реального часу;

– візуалізація інформації на моніторах у зрозумілій та зручній для сприйняття людиною формі;

– аварійна сигналізація про надзвичайні стани та управління оповіщеннями;

– логічне управління, підготовка та генерування звітів про стани технологічного процесу;

– забезпечення взаємодії з зовнішніми додатками, включаючи системи управління базами даних, текстові процесори, електронні таблиці тощо.

Система SCADA є дуже ефективним інструментом диспетчерського управління, але вона потребує особливої уваги з точки зору забезпечення кібербезпеки її функціонування [71].

З урахуванням ключового значення СЄД-ОТУ для безперебійного надійного функціонування енергетичного сектору далі проаналізуємо її суттєві для цілей кіберзахисту та забезпечення гарантоздатності властивості та відмінності від поширених типів інформаційно-комунікаційних систем інших секторів реального суспільного виробництва.

1.1.2 Особливості забезпечення кіберстійкості та гарантоздатності інформаційного обміну в складних системах

Спочатку доцільно звернути увагу на визначення двох понять, що винесені у назву розділу. Відповідно до [10], «*кіберстійкість* критичної інформаційної інфраструктури – стан критичної інформаційної інфраструктури, за якого забезпечується її спроможність надійно функціонувати та надавати основні послуги в умовах кіберзагроз».

Водночас у [11] визначено, що для досягнення цілі К1 кіберзахисту необхідно «забезпечити режим постійної готовності до реальних та потенційних кіберзагроз, виявляти та усувати передумови до їх виникнення, *забезпечивши тим самим кіберстійкість*, передусім об'єктів критичної інформаційної інфраструктури».

У першому визначенні кіберстійкість являє певний стан критичної інформаційної інфраструктури, що дає можливість стійкого функціонування в умовах кіберзагроз, у другому випадку – кіберстійкість є наслідком усунення умов виникнення кіберзагроз.

На думку експертів армії США [12], кіберстійкість слід розглядати у контексті *складних систем*, які охоплюють фізичну, інформаційну, когнітивну

та соціальну сфери. При цьому вона гарантує здатність відновлення кіберінфраструктури (системи), включаючи її апаратну і програмну платформи та сенсорні компоненти, виконуючи роль сполучної ланки між підтримкою функцій системи та забезпеченням виконання її місії.

У [13] визначення стійкості уточняється як здатність систем передбачати несподіванки та відмови та адаптуватися до їх потенціалу.

Відмітимо, що акценти інженерії стійкості [14] зосереджені на чотирьох властивостях, які є суттєвими для її досягнення, а саме на здатності

реагувати на те, що відбувається;

стежити за критичними подіями;

передбачати майбутні загрози та можливості;

вчитися на минулому досвіді – як успіхах, так і невдачах.

Робота з вказаними властивостями, на думку дослідників, забезпечує [14] структурований підхід до аналізу проблем кіберстійкості, а також методологію напрацювання практичних рішень, включаючи методи, інструменти тощо.

Іншою суттєвою характеристикою інформаційних технологій, що використовуються на ОКІ, є їх гарантоздатність – це спроможність надавати послуги, яким виправдано можна довіряти [15–17].

Актуальність проблеми забезпечення гарантоздатності інформаційних технологій в енергетичному секторі обумовлена потенційно небезпечними наслідками для людини, суспільства і екології у разі відмов їх складових, збоїв та помилок проєктування системи тощо.

Гарантоздатність є комплексною характеристикою інформаційної системи (рис. 1.3), що включає такі характеристики, як готовність, безвідмовність, ремонтопридатність, функціональна безпека, конфіденційність, цілісність [16].

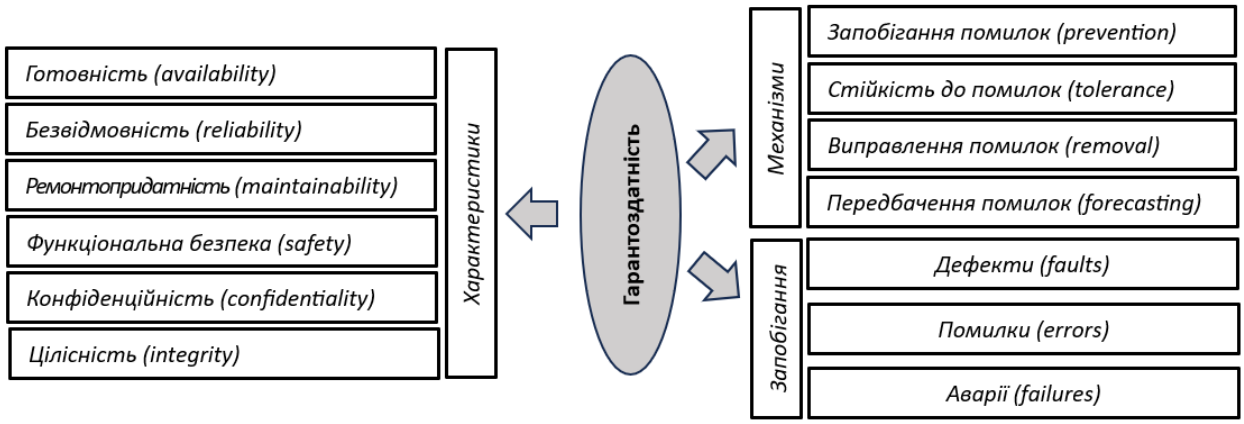

Рисунок 1.3 – Архітектура гарантоздатності [16, 23]

Базові поняття та положення щодо гарантоздатних комп'ютерних систем сформульовані в [16], де визначена, зокрема, така їх властивість, як «гарантоздатність обчислень» (dependable computing), що означає їх спроможність виконувати завдання за призначенням у випадках відмов або збоїв їхніх апаратних та програмних складових, що можуть бути обумовлені проявом помилок або дефектів, які виникли на етапах проєктування та випробувань.

Проблеми забезпечення та оцінювання гарантоздатності комп'ютерних систем набула подальшого розвитку в [18–21], зокрема, в [20] запропоновано підхід до побудови гарантоздатної інтегрованої навігаційної системи рухомих наземних об'єктів, яка суттю може бути класифікована, як ОКІ.

В [21] узагальнено досвід управління безпекою організаційно складних систем, визначені основні принципи реалізації управління безпекою для різних сфер життєдіяльності людини, а також приділено увагу як складовим безпеки ІТ-систем, включаючи функціональну, інформаційну та кібербезпеку, а також гарантоздатності складних систем.

Особливо слід звернути увагу на те, що апаратно-програмні засоби захисту інформації самі можуть бути піддані загрозам відмов та збоїв [22], як наслідок можуть не виконувати необхідні функції, тому актуальною є постановка задачі забезпечення їхньої гарантоздатності.

Зазначимо, що першість дослідження гарантоздатності криптографічних систем належіть Глухову В.С., у роботі [23] якого визначені складові гарантоздатності у загальному випадку (рис. 1.3) та наведені методи оцінки гарантоздатності криптографічних систем, що реалізують цифровий підпис.

Зважаючи на те, що системна розробка вихідних технічних вимог до побудови захищених гарантоздатних інформаційно управляючих систем (ЗГІУС) для енергетичного сектору недостатньо пророблена, з метою створення передумов для побудови відповідного вітчизняного апаратно-програмного забезпечення уявляється доцільним у рамках даного дослідження заповнити цю прогалину.

Зокрема, необхідно проаналізувати «вузькі місця» існуючих в енергетичному секторі інформаційних технологій, сформувати актуальну модель загроз безпеці функціонування ЗГІУС, визначити та обґрунтувати вимоги щодо конкретних технологій захисту. При цьому необхідно звернути увагу, що існуюче різноманіття апаратних і програмних платформ не тільки впливає на ефективність та продуктивність систем, а й ускладнює розв’язок задач реалізації кіберзахисту.

Потенційним кандидатом на забезпечення захисту конфіденційності, цілісності і, частково, доступності інформаційних ресурсів можуть бути технології криптографічних перетворень, які придатні до застосування майже на будь-яких програмних та апаратних платформах, не суттєво знижуючи при цьому обчислювальну потужність систем та, за певних умов, не суттєво затримуючи їх реагування на зміни у технологічних процесах ЕС.

На жаль, на поточний час уніфікованого вирішення наукового завдання забезпечення гарантоздатності криптографічних систем, які в багатьох випадках є невід’ємними складовими комп’ютерних систем, та методів оцінки їх гарантоздатності, поки ще не існує, а це потребує розробки відповідних моделей та методів забезпечення гарантоздатності криптографічних систем, що і визначає наступну задачу цього дослідження.

У попередньому розділі було зазначено, що на рівні Стратегії безпеки ЄС визначені специфічних властивості та особливі умови функціонування енергетичного сектору, що далі розглядається об’єкт інформатизації та кіберзахисту, це:

– підвищені вимоги до оперативності обробки інформації, включаючи процедури та процеси її захисту;

– висока ймовірність так званого каскадного ефекту в разі відмови певної складової електроенергетики, в тому числі в разі помилкового спрацювання системи кіберзахисту або реального несанкціонованого втручання в роботу системи;

– наявність поєднання деяких застарілих рішень із сучасними технологіями може суттєво обмежувати застосування моделей та методів кіберзахисту, що орієнтовані на новітні апаратні та програмні платформи, комунікаційні протоколи.

Фактори та властивості автоматизованих управляючих та інформаційних систем (АУІС) подібного роду можуть суттєво ускладнювати розв’язання завдань кіберзахисту, вступати в протиріччя з існуючими підходами до застосування типових моделей та методів технічного та криптографічного захисту або потребують деяких унікальних нестандартизованих рішень.

Це означає, що передпроєктний етап побудови систем захисту інформації для подібних АУІС повинен включати вивчення та детальний аналіз усіх їх складових та їхніх взаємозв’язків.

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 разі побудови системи захисту для вже існуючих ІКС, оскільки деякі їх концептуальні рішення потенційно можуть ускладнювати реалізацію заходів захисту.

Переважно з побудовою системи захисту проблем не виникає, якщо захищається інтегрована ІКС [28, 29], 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. У такому разі звичайно не виникає суттєвих труднощів з побудовою комплексної системи захисту ІКС та вона створюється як сукупність підсистем захисту для її складових.

Водночас 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, уявляється доцільним сконцентруватися на 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.

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

Водночас, 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 [30–32], та з урахуванням методологічних основ забезпечення інформаційної безпеки та кібербезпеки доцільно вважати, що складна з точки зору захисту інформації в ІКС (далі просто – складна система, complex system – CS) характеризується деякими з перерахованих властивостей (рис. 1.4):

– нетривіальна (нелінійна) взаємодія між її компонентами (складовими), що негативно впливає на можливість її автоматизованої декомпозиції [33–35] 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, як-от самоорганізація та висока невизначеність;

– потенційно висока динаміка можливого розвитку небезпечних подій у системі, каскадний ефект 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 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.

Рисунок 1.4 – Ознаки складної ІКС в аспекті її кіберзахисту

До останнього фактора можливо додати об'єктивну потребу користувачів в побудові підсистеми, в яких доступ суб'єктів до об'єктів (процесів) реалізується за допомогою деяких сучасних технологій, що не узгоджені з політиками безпеки інших складових CS. Наприклад, це може стосуватися припустимості використанням в окремих підсистемах мобільних пристроїв загального користування для реалізації дистанційного доступу до деяких ресурсів.

Окремо доцільно дещо проаналізувати складність, обумовлену поєднанням декількох з перерахованих факторів, проява яких може мати наслідком виникнення так званого каскадного ефекту, про який буде розмова в наступних розділах. Попередньо зазначимо, що об'єкти енергетики взаємодіють не тільки в площині інформаційних технологій, а також і в фізичному середовищі завдяки взаємному (іноді – перехресному) електроживленню, що може бути наслідком збою або відмови керуючого пристрою внаслідок тривалого збою або відмови керованого пристрою енергетичної системи.

Зрозуміло, що наведені фактори за суттю мають бути визначальними для побудови та дослідження моделей захисту складних систем, зокрема, в

енергетичному секторі, та потребують відпрацювання належного комплексу організаційно-технічних та технологічних рішень кіберзахисту.

У 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 аналізу та вдалої декомпозиції CS на складові.

Наступним кроком уявляється доцільним проаналізувати завдання та функції суб’єктів інформаційних відносин в енергетичному секторі у плані обміну даними про загрози та ризики для вирішення основних завдань оперативно-технологічного управління енергетичною системою.

1.1.3 Інформування про кіберзагрози та ризики в енергетичному секторі

Відповідно до вимог Кодексу систем передачі [25] на власників та керівників підприємств, що віднесені до ОКІ, покладається відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем ОКІ, захисту технологічної інформації відповідно до вимог законодавства, за невідкладне інформування урядової команди реагування на комп’ютерні надзвичайні події CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об’єктах.

У «Вимогах з кібербезпеки паливно-енергетичного сектору критичної інфраструктури» [26], затверджених наказом № 417 Міністерства енергетики України від 15.12.2022 р., визначено, що оператор критичної інфраструктури надає інформацію щодо кіберінцидентів та відповідає за те, що одержувачі інформації розуміють та можуть слідувати правилам щодо спільного застосування маркування повідомлень щодо кіберінцидентів.

Метою маркування повідомлень є уніфікація процесів поширення інформації про кіберінциденти та намагання обмежити коло суб'єктів інформаційного обміну, що можуть мати доступ до неї. За основу відповідної процедури обрані рекомендації Європейської агенції з кібербезпеки (ENISA) [45] щодо протоколу TLP.

Протокол TLP – це формалізована процедура, що спрощує обмін конфіденційною інформацією та забезпечує при цьому необхідний рівень захисту та контролю. Він визначає легко зрозумілу послідовну схему маркування інформації, яка циркулює в межах певної спільноти довірених суб'єктів обміну. TLP відіграє важливу роль в обміні інформацією, зокрема, у сферах кібербезпеки, розвідки та правоохоронних органів [46].

У загальних правилах обміну інформацією про кіберінциденти [47] запропоновано версію протоколу TLP, яка відповідає рекомендаціям документа «Форуму команд реагування та безпеки» (FIRST – Forum of Incident Response and Security Teams) [48]. Ця версія протоколу використовує 4 кольори для позначення того, яким чином повідомлення може в подальшому поширюватись стороною, що отримує певну інформацію.

Поточна версія протоколу, зокрема, використовується у системі MISP-UA (Malware Information Sharing Platform and Threat Sharing «Ukrainian Advantage») [49] для обміну інформацією щодо кібератак, кіберінцидентів та кіберзагроз, що здійснюється між законодавчо визначеними суб'єктами, які виконують у межах своєї компетенції заходи із забезпечення кібербезпеки.

Перевагами впровадження TLP забезпечення стандартизованої структури для безпечного обміну інформацією, покращення заходів з кібербезпеки, сприяння довірі між учасниками та зміцнення колективного захисту від сучасних кіберзагроз [48].

Останній тезис щодо покращення колективного захисту від кіберзагроз є дуже актуальним для енергетичного сектору, оскільки в ньому працює велика кількість підприємств та організацій різних форм власності та підпорядкування, що на поточний час може ускладнювати інформаційний

обмін про кіберінциденти між учасниками процесів виробництва, транспортування та розподілу електричної енергії.

На думку експертів компанії Group Sense [48], впровадження протоколу TLP може спричинити деякі проблеми для організацій, зокрема:

– небезпеку різного тлумачення, невірного розуміння та застосування колірних кодів TLP учасниками інформаційного обміну;

– певну складність управління процесом переходу від існуючої практики повідомлень про інциденти до схеми TLP;

– необхідність подолання ментального чи організаційного опору змінам;

– нагальну потребу відстеження нових загроз кібербезпеці та відповідного коригування практичних аспектів застосування протоколу TLP.

Окремо можливо відмітити, що ключових фактором впровадження та поширення ефективного застосування концепції TLP в енергетичному секторі має бути визначення операційного координатора відповідних заходів, наприклад, у вигляді підприємства з питань автоматизованого ситуаційного управління [50, 51]. Вказана структура може вирішувати низку інших життєво важливих організаційно-технічних завдань в сфері кіберзахисту, про що йде мова в наступних розділах.

1.2 Інформаційні технології у процесах управління Об'єднаною енергетичною системою України (ОЕС-У)

1.2.1 Функції та завдання суб’єктів управління енергосистемою України

Класична архітектура енергосистем, відповідно до [36], включає три основних компоненти: генерацію, передачу та розподіл. Вони утворюють їх фізичне середовище, забезпечують виконання ключових завдань та є об’єктами управління енергетичної галузі (рис. 1.5).

У наведеній на рис. 1.5 схемі під передачею електричної енергії (передача) розуміється її транспортування електричними мережами оператора системи передачі від електростанцій до пунктів підключення систем розподілу та електроустановок споживання (не включаючи постачання електричної енергії), а також міждержавними лініями.

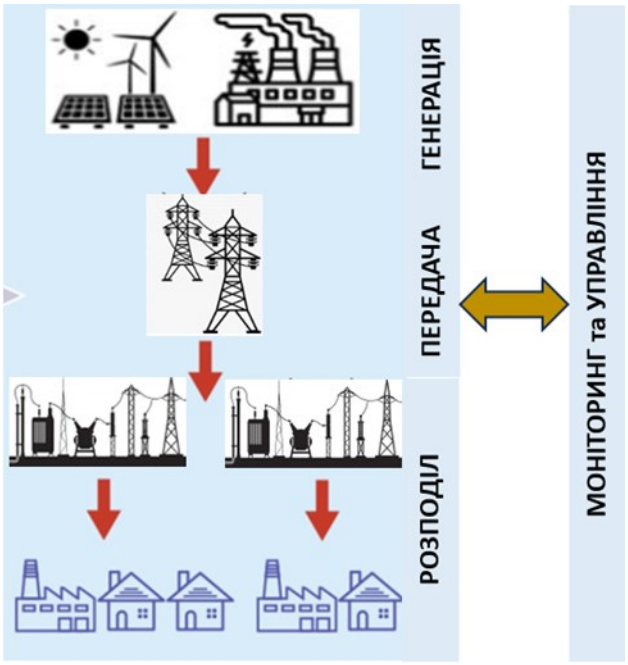

Рисунок 1.5 – Загальна архітектура енергетичної галузі

Згідно з законодавством [1, 25] одним із основних напрямків державної політики в електроенергетиці є забезпечення надійного, безпечного постачання електричної енергії. При цьому правила безпеки постачання електроенергії та здійснення моніторингу безпеки постачання енергії розробляються і затверджуються повноважним державним органом [1, 37].

Нормативно визначено [37], що перелік критеріїв, за якими оцінюється безпека постачання електроенергії, повинен включати виявлення та попередження кіберзагроз, впливають на стійке функціонування електроенергетики, а також вимоги щодо захисту ОКІ.

Підчас моніторингу оператором системи передачі виконується аналіз, узагальнення та аналітична обробка отриманої інформації, її завантаження в

структурованому вигляді у спеціалізовану базі даних, яка утримується в актуальному стані.

Що стосується виконання функцій збереження цілісності та гарантування надійного і ефективного функціонування ОЕС-У, а також енергетичної безпеки України, то можливо відмітити, що це завдання реалізується державним підприємством НЕК «Укренерго», яке реалізує серед інших такі державно важливі функції оператора системи передачі [38, 39]:

– централізоване диспетчерське управління ОЕС-У із забезпеченням надійної роботи електричних станцій України та взаємодії з енергосистемами країн Східної і Центральної Європи, попередження загроз порушення сталого функціонування та аварій системного характеру з метою мінімізації можливої шкоди;

– забезпечення надійної передачі по електричних мережах напругою 110-750 кВ енергії від електростанцій до мереж операторів розподілу, а також здійснення експорту та імпорту електроенергії;

– створення умов для ефективної роботи магістральних і міждержавних електромереж як складової частини інфраструктури ринку електроенергії України.

ЦД-ОТУ використовується для виконання таких дій:

– планування потужності електростанцій України та оперативне управління ними з урахуванням режимів централізованого теплопостачання;

– планування та контроль за додержанням режиму роботи ОЕС-У;

– запобігання аварійним ситуаціям і ліквідація їх наслідків в ОЕС-У шляхом підтримки необхідного балансу потужності та енергії, забезпечення надійного і сталого функціонування ОЕС-У та її паралельної роботи з енергетичними системами інших держав;

– розроблення та впровадженням нових систем протиаварійної автоматики та захисту, а також засобів зв'язку і диспетчерського управління;

– здійснення нагляду за експлуатацією систем протиаварійної автоматики та захисту.

Заходи диспетчерського управління поширюються на підприємства, об'єкти електроенергетики яких підключені до ОЕС-У, для яких, відповідно до закону, усі оперативні команди і розпорядження в системі диспетчерського управління підлягають обов’язковому виконанню. Вказані підприємства, зобов'язані подавати державному підприємству, що здійснює диспетчерське управління, звіти та інформацію, які передбачені нормативно-технічними документами.

Окремо слід відмітити світові тенденції розвитку технологій інтелектуальних енергетичних систем (Cyber-Physical Power System – CPPS), які є орієнтиром для майбутньої трансформації ОЕС-У.

CPPS належать до кіберфізичних систем [40], які за допомогою АУІС на основі швидкісного телекомунікаційного обладнання та цифрових сенсорних засобів забезпечують мінімальну часову затримку для моніторингу та оперативного управління технологічними процесами фізичної інфраструктури енергосистеми (рис. 1.6).

Складність зв’язків між управляючою інформаційною та фізичною (керованою) інфраструктурами дедалі зростає, час для реагування на кіберінциденти об’єктивно зменшується, тому кібератаки можуть призводити до важків наслідків для стійкості функціонування енергосистем [41, 42].

Рисунок 1.6 – Інтелектуальна енергетична система CPPS

Відмови та їх поширення в кіберфізичних електроенергетичних системах суттєво відрізняються від таких у традиційних енергосистемах. Кібератаки у керуючій підсистемі стали важливим фактором виникнення збоїв не тільки в інформаційно-комунікаційній підсистемі, а й у фізичній підсистемі через тісніший зв'язок між цими підсистемами [42].

Тому для підтримки надійної та безперебійної роботи CPPS важливим є забезпечення кіберстійкості керуючої підсистеми. Зокрема, у [43] досліджено обумовлений кібератакою каскадний збій енергосистеми, що виникає внаслідок ураження (функції φ_1, φ_2, рис. 1.7) вузлів кіберсередовища зловмисним програмним забезпеченням та через сполучні зв’язки створює небезпеку (функції ψ_1, ψ_2) для фізичних вузлів. Відповідна модель для кіберфізичних енергетичних систем наведена на рис. 1.7.

Модель надає візуальне уявлення, як кібервузли (node) N_C^N, N_C^I, N_C^{ID} інформаційного середовища кіберфізичних енергосистем під впливом збурюючого фактору змінюють свій стан із нормального на непрацездатний, де N_C^N, N_C^I та N_C^{ID} (відповідно: нормальний, заражений та виявлений заражений вузли комунікаційної мережі).

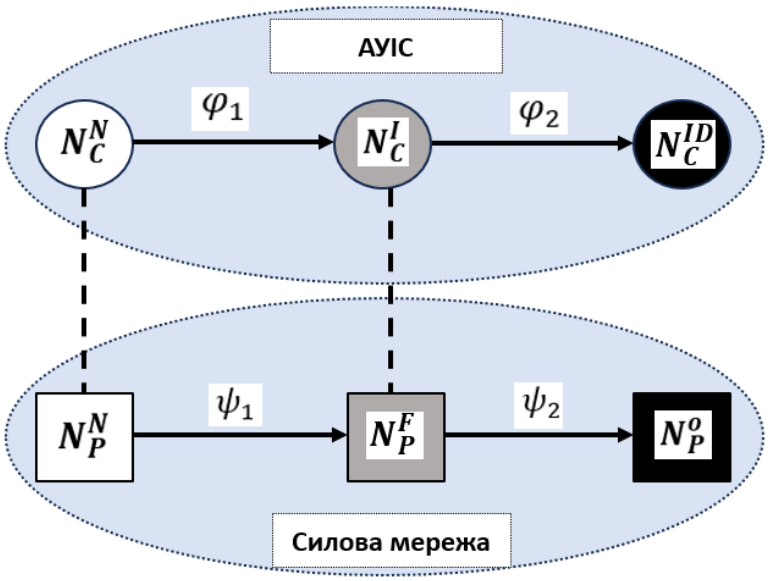

Рисунок 1.7 – Модель каскадного збою в CPPS

Це так само призводить до небажаних змін у вузлах фізичного середовища CPPS – N_P^N, N_P^F та N_P^o, які відповідно означають нормальні, хибні та перевантажені (в енергетичному сенсі) вузли.

Тут виникає наукове завдання: як і за допомогою якого методу, мінімізуючи час реагування, уникнути ефекту каскадного збою, використовуючи при цьому належним чином модифіковані моделі та методи технічного та криптографічного захисту інформації.

Це потребує також аналітичного огляду інформаційних ресурсів та даних, які збираються, передаються, обробляються, зберігаються АУІС та надсилаються керованим об’єктам енергетичної системи, про що мова далі.

1.2.3 Тренди цифровізації: мобільний доступ до АУІС енергосистем та хмарні сервіси

Питаннями цифровізації опікується Мінцифри, яке відповідно до рішення уряду [51], забезпечує формування і реалізацію державної політики у таких сферах:

– цифровізації, цифрової економіки, цифрових інновацій, електронного урядування та електронної демократії, розвитку інформаційного суспільства;

– розвитку цифрових навичок та цифрових прав громадян;

– відкритих даних, розвитку національних електронних інформаційних ресурсів та інтероперабельності, розвитку інфраструктури широкосмугового доступу до Інтернету та телекомунікацій, електронної комерції та бізнесу;

– надання електронних та адміністративних послуг;

– електронних довірчих послуг;

– розвитку ІТ-індустрії.

Оскільки концептуальні засади державної політики в сфері цифрової трансформації законодавством України на поточний час не визначені, а також

для відповідної науково-практичної сфери поняття «цифровізація», тому уявляється логічним проаналізувати складову цифрової трансформації – цифровізацію через призму інформаційних технологій, які фактично використовуються для вирішення конкретних завдань у перерахованих сферах.

Міжнародний стандарт ISO/IEC38500 [68] тлумачить поняття інформаційні технології, як ресурси, необхідні для збору, обробки, зберігання і розповсюдження інформації. Інформаційні технології забезпечують обробку інформації, яка спрямована на зміну її стану, властивостей, форми, змісту і здійснюється в інтересах користувачів.

Сучасні інформаційні технології здатні не тільки цілком задовольнити вимоги виробничих систем, але й виступають важливою передумовою їхнього розвитку. Цифрові методі обробки інформації, які замінили аналогові, дозволили в науці та техніці значно підвищити гнучкість, швидкість та точність обчислень, що за суттю є головними перевагами цифровізації в енергетичному секторі.

Останні наукові публікації, що стосуються різних аспектів цифровізації бізнес-процесів, дають загальне уявлення про її переваги.

У [53] окреслено такі переваги цифровізації загалом для підприємницької діяльності, як підвищення конкурентої спроможності та зниження витрат за рахунок автоматизації бізнес-процесів, потужна аналітика даних, розширення географії швидкої мобільної комунікації з партнерами та клієнтами через програмні застосунки.

У [54] піддана аналізу цифровізації в розподільних пристроях середньої напруги з використанням сучасних технологій, як-от вимірювальні трансформатори малої потужності, цифрові реле захисту та керування з цифровим зв’язком IEC 61850, та переваги цифрових комутаційних пристроїв з точки зору кінцевого користувача.

У [55] доведено, що концепції розумної мережі та цифровізації постійно оновлюють динаміку в системах розподілу електроенергії та інфраструктури для захисту, контролю, вимірювання та моніторингу цих систем.

У [56] на прикладі розробки мікросервісу підтримки прийняття рішень, що враховує коливання генерації та споживання енергії, а також забезпечує надійність та стабільність роботи енергосистеми, доведено, що таке рішення, завдяки гнучкості, масштабованості та легкості інтеграції, може бути ефективним способом розв'язання завдань для енергетичних систем.

У [57, 58] досліджено інформаційні технології, що використовуються для ведення бухгалтерського обліку, включаючи хмарні сервіси. Серед переваг цифровізації відмічена можливість автоматизації рутинних завдань та процесів, що допомагає зменшити час і зусилля, необхідні для виконання роботи.

Аналіз та узагальнення наукових публікацій з питань цифровізації дозволяє стверджувати, що вона є об'єктивним етапом трансформації суспільного виробництва на основі повсюдного застосування комп'ютеризованих стаціонарних та мобільних систем і пристроїв. Вона спрямована на зміну існуючих моделей управління технологічними процесами завдяки застосуванню сучасних підходів, що включать застосунки на мобільних пристроях, хмарні сервіси, блокчейн-системи, штучний інтелект, квантові обчислення, 3D-лазерні технології тощо.

Звернемо увагу на такий важливий напрям цифровізації, як створення застосунків (мікросервісів) для мобільних пристроїів, який продемонстрував свою життєздатність в рамках проєкту «Дія» [59] та чат-ботів ДТЕК [69].

Як свідчать результати науково-прикладного дослідження китайських дослідників [60], система диспетчерського управління електромережами може бути суттєво покращена за допомогою мікросервісної архітектури. У зазначеній роботі з метою підвищення ефективності навантаження та стабільності розподілену архітектуру системи диспетчерського керування електромережою трансформовано за допомогою архітектури мікросервісу. Запропонована технологія мікросервісу експериментально перевірена з метою її оцінки щодо пропускної здатності, масштабованості, відмовостійкості та ремонтопридатності (фактично це означає гарантоздатність).

Отже, перспективним напрямом цифровізації енергетичного сектору є застосування інформаційних технологій на основі архітектури мікросервісу з умов дотримання умов кібербезпеки та гарантоздатності. При цьому інструментами цифровізації управління енергосистемами виступають смартфони та прикладні застосунки – мікросервіси.

На підставі цитованих раніше наукових та нормативних джерел, можливо зробити висновок, що смартфон, як достатньо потужна обчислювальна платформа з поширеною операційною системою, може бути застосований для вирішення актуальних функцій управління енергетичними системами, включаючи:

– підтримання комунікацій менеджменту та персоналу підприємств для передачі та отримання доручень, планування та контролю заходів, оперативного отримання візуалізованої довідкової та звітної інформації тощо;

– відстежування в реальному часі уповноваженими посадовими особами параметрів поточного стану значної кількості критичних об’єктів енергетичних систем, чому сприяє мініатюризація та здешевлення сенсорів, що формують дані про об'єкт спостереження;

– оголошення надзвичайної ситуації у нормативно визначених випадках, обміну, згідно з протоколом TLP, інформацією про кіберінциденти, кібератаки та загрози безпеці ЕС;

– управління заходами з відновлення стану об’єктів, що порушений внаслідок реалізації загроз;

– проведення професійного навчання та тренінгів персоналу з використанням цифрових симуляторів електрообладнання систем, а також дистанційної атестації персоналу відповідно до нормативних вимог;

– візуалізації стану та планування фінансово-господарської діяльності та багатьох інших завдань, що виконуються згідно з Законом [1] суб’єктами енергетичного ринку.

Відповідні функції мають виконуватися програмними засобами – микросервісами, що реалізовані і працюють як невеликі й відносно незалежні

продукти, які після авторизації користувача на основі внутрішньої логіки з використанням визначеного інтерфейсу надають доступ до необхідних технологічних команд (операцій) і даних. Деякі дослідники [61] розглядають микросервіси не як самостійний напрям у програмній інженерії, а як варіант підходу до реалізації сервіс-орієнтованої архітектури (SOA) програмного забезпечення.

Зважаючи на те, що в плані розробки, експлуатації та масштабування кожен мікросервіс є відносно незалежним елементом, то, на думку дослідника [61], мікросервісна архітектура сприяє підвищенню гнучкості програмного забезпечення.

Підсумовуючи характеристики цього тренду цифровізації в енергетичному секторі можливо визнати його обнадійливу перспективу за умов вирішення основних завдань кібербезпеки та гарантоздатності. Це, зокрема, передбачає створення ефективних процедур авторизації мобільних суб’єктів інформаційного обміну та технологічних процесів забезпечення. Зокрема, на це звертається увага в [62–64], де запропоновані моделі автентифікації суб’єктів мобільного доступу в критичній системі та визначені механізми, що можуть бути реалізовані в системах, суб'єкти яких мають певні схеми руху на місцевості (в межах міста, району), що відповідає характеру дій екстрених служб енергетичного сектору.

З урахуванням характеристики інформації, яка циркулює в АУІС енергетичних систем, мають бути також відпрацьовані науково-практичні рішення щодо захисту конфіденційності та цілісності даних що обробляються. Саме кіберзахист мікросервісів мобільних користувачів може буте визначений як актуальне наукове завдання для подальшого дослідження. При цьому слід мати на увазі вразливості криптографічно захищеного обміну мобільних користувачів [66] та визначити спосіб нейтралізації відповідної загрози.

Другим, не менш важливим трендом цифровізації, є розвиток інформаційних технологій, що підтримують концепції хмарних обчислень і сервісів. Хмарні сервіси дозволяють достатньо швидко за відносно невеликі

кошти створювати сучасні обчислювальні потужності, зберігати та обробляти великі обсяги даних, раціонально використовувати виділений ресурс та не витрачати додаткові кошти на ліцензоване програмне забезпечення.

Відмітимо, що при цьому забезпечується майже одночасний доступ багатьох користувачів до збереженої у хмарі інформації без можливих черг.

Останнім часом сучасна енергетична система, що швидко розвивається у Китаї, набуває ознак інтелектуальної мережі та перетворюється на інформаційну систему з масивними та різнорідними даними [65]. У зазначеному дослідженні було запропоновано інтеграцію гетерогенного сервісного програмного забезпечення та платформ додатків Інтернету речей для створення приватної хмари для енергетичної системи (іменованої енергетичною хмарою). При цьому центральним пунктом дослідження є механізм побудови потужного хмарного сервісу, який включає центр обробки даних хмарних обчислень, віртуальний робочий стіл і поєднання хмарних додатків із системами обслуговування додатків Інтернету речей.

Зрештою, виконаний загальний проєкт структури енергетичної хмари, інтегрованої з гетерогенними системами обслуговування додатків. При цьому показано, що енергетична хмара має вагомі переваги перед традиційними прикладними системами. На думку дослідників, будівництво енергетичної хмари має велике значення для майбутнього розвитку енергетичної мережі Китаю.

Можливо висловити припущення, що реалізація подібного проєкту в Україні мала би стратегічне значення, якби воно було поєднане з ефективними рішеннями в плані забезпечення кібербезпеки та гарантоздатності.

Наступним кроком доцільно проаналізувати шляхи оперативного управління енергетичними системами в умовах виникнення надзвичайних ситуацій, яке отримало назву ситуаційного управління.

1.2.4 Питання ситуаційного управління в енергетичному секторі

Згідно з повідомленнями мас-медіа, тільки за останні 20 років різні техногенні, природні та антропогенні фактори десять разів стали причиною надзвичайних ситуацій в енергетичних системах по всьому світу.

Це тривалі блекаути у США та Канаді (2003 рік), у Західній Європі (2006), техногенна катастрофа на С-Ш ГЕС рф (2009), аварія лінії електропередачі ГЕС Ітайпу, Бразилія (2009), тривалий блекаут в Сан-Пауло і Ріо де Жанейро, Бразилія (2014), кібератака на Закарпатське Обленерго (2015), землетрус у провінції Сичуань, Кітай (2017), системна аварія внаслідок удару блискавки у Великобританії (2019), потужна злива у провінції Хенань, Кітай (2021) призвели до паралічу енергосистем, людських жертв, колосальних фінансових і матеріальних збитків.

Наведені факти вимагають прискіпливої уваги урядів дослідженню питань управління енергосистемами в надзвичайних ситуаціях.

Одна з найбільш сучасних потужних та оперативних систем екстреного реагування, так звана «повноланцюгова» система, побудова у Китаї [27].

«Повноланцюгова» система швидкого реагування на надзвичайні ситуації в електромережі було створено з використанням п’яти напрямків дослідження контрзаходів управління аварійними ситуаціями в електроенергії. Дворівнева система швидкого реагування на надзвичайні ситуації включає такі шість напрямів:

1. Створення дворівневих аварійних підрозділів швидкого реагування, які в системі були розділені на аварійні базові групи муніципальних і районних компаній і аварійні групи швидкого реагування електростанцій.

2. Розроблення 30-хвилинного циклу реагування на надзвичайні ситуації шляхом зміцнення організаційної структури блоку реагування на надзвичайні ситуації електропостачання та уточнення ролі кожного підрозділу,

забезпечення протидії на основі сценаріїв реагування на надзвичайні ситуації, що підвищило здатність швидкого реагування.

3. Створення комунікаційної платформи реагування на надзвичайні ситуації для покращення можливості реагування шляхом удосконалення навичок персоналу, інтеграції ремонтно-аварійних робіт та використання мобільного обладнання для моніторингу в реальному часі.

4. Вдосконалення всього процесу координації на випадок надзвичайних ситуацій для реалізації ефективного механізму внутрішньої та зовнішньої взаємодії.

5. Розроблення наукової стратегії резервування матеріалів для екстрених потреб та логістичного їх забезпечення.

6. Покращення роботи в надзвичайних ситуаціях шляхом стандартизації управління підрозділами швидкого реагування та накопичення та об’єднання досвіду аварій.

Перераховані напрями в певних позиціях корелюються з вітчизняною концепцією побудови мережі ситуаційних центрів, заходи з побудови якої на поточний час ще не реалізовані.

Надзвичайною ситуацією в ОЕС-У відповідно до Закону [1] вважається такий випадок, що починається з переходу системи передачі у режим системної аварії та продовжується до моменту її відновлення. При виникненні надзвичайної ситуації в ОЕС-У оператор системи передачі оголошує про це та сповіщає суміжних ОСП.

Протягом дії режиму надзвичайної ситуації в ОЕС-У оператор системи передачі набуває повноважень реалізації надзвичайних заходів відповідно до кодексу системи передачі. Всі відомості щодо виникнення, розвитку та ліквідації аварійного режиму в системі передачі має бути належним чином задокументовані ОСП для відображення у спеціальній базі даних.

Електроенергетичні підприємства у разі виникнення надзвичайної ситуації в ОЕС-У зобов’язані виконувати команди і розпорядження оператора системи передачі.

Зважаючи на те, що нормативними документами на поточний час аспекти технології побудови ситуаційних центрів ОКІ, їх завдань і функцій не врегульовані, уявляється доцільним приділити увагу дослідженню цього наукового завдання.

1.3 Види інформації, що підлягають захисту у ІКС-ЕС

У [44] надано системний огляд існуючих світових практик щодо захисту конфіденційної інформації на ОКІ. За результатами вивчення встановлено, що на поточний момент не існує комплексних методик захисту конфіденційної інформації, яка обробляється в інформаційних системах ОКІ. Зазначене питання потребує детального розгляду.

Спочатку звернемо увагу на важливу особливість інформаційної складової ОЕС-У, що полягає в потенційній обробці різних, визначених нормативними документами, видів інформації з обмеженим доступом.

Зокрема, в [1] застосовують такі поняття та їх визначення:

• «професійна таємниця – конфіденційна інформація, що отримана, передана або якою здійснювався обмін відповідно до Закону, підпадає під режим збереження професійної таємниці, встановлений цією статтею...»;

• «*інсайдерська інформація* на ринку електричної енергії – неоприлюднена інформація точного характеру, що прямо чи опосередковано стосується одного або декількох оптових енергетичних продуктів на ринку електричної енергії, розкриття або оприлюднення якої може значно вплинути на ринкову ціну відповідно до одного або декількох оптових енергетичних продуктів»;

• *«чутлива інформація* щодо захисту критичної інфраструктури (далі – чутлива інформація) – інформація, несанкціоноване розкриття якої може призвести до пошкодження або знищення ОКІ».

Стосовно першого визначення Закон дає роз’яснення, що положення цієї статті не позбавляють органи державної влади можливості обмінюватися конфіденційною інформацією або передавати її відповідно до вимог законодавства, за умови що така інформація не була отримана від регулюючих органів іноземних держав, установ Енергетичного Співтовариства, Агентства з питань співробітництва енергетичних регуляторів. Але при цьому закон не дає чіткої відповіді на питання, хто є або може бути власником або розпорядником такої інформації (держава або комерційна структура) та, відповідно, приймає рішення щодо надання допуску до неї.

Друге визначення, явно, має ознаки комерційної таємниці з відносно коротким терміном обмеження доступу, що обумовлено фактом повної або часткової втрати її комерційної цінності після завершення конкретної сесії торгів на електричну енергію. А особам, які володіють інсайдерською інформацією, забороняється її розголошувати, робити спробу вчинення певних дій на власну користь або на користь третіх осіб, або надавати рекомендації щодо вчинення правочинів.

У третьому визначенні під терміном ОКІ розуміються об’єкти [1], що віднесені до критичної інфраструктури в порядку, визначеному законодавством та які необхідні для забезпечення життєво важливих для суспільства функцій, безпеки у населення, виведення з ладу або руйнування яких матиме суттєвий вплив на національну безпеку та оборону, навколишнє природне середовище та може призвести до значних фінансових збитків і людських жертв.

Це визначення фактично ілюструється запропонованою в 1.4.2 моделлю логічних ланцюгів впливу загроз на погіршення спроможності стійкого функціонування ЕС, оскільки у цьому разі внаслідок реалізації деякої загрози може бути порушена така властивість інформації як її конфіденційність, а кінцеві наслідки для галузі, суспільства або держави можуть мати катастрофічний характер.

Зважаючи, що переважна більшість ОКІ перебуває в той чи іншої формі приватної власності, можливо припустити власниками чутливої інформації є або можуть бути недержавні юридичні особи, які відповідно законодавства самостійно визначать порядок доступу до неї в ІКС.

Безумовно, велика частина інформаційних ресурсів, що накопичується в АУІС має бути класифікована як персональні дані та потребує належного поводження

Доцільно звернути увагу, що в АУІС також циркулює відкрита інформація, до якої мають бути вжиті заходи щодо забезпечення її цілісності та доступності. Зокрема, законом [1] визначено, що всі суб'єкти господарювання у сфері електроенергетики, що здійснюють виробництво електричної енергії, її передачу, розподіл тощо повинні за встановленою формою надавати статистичні відомості про свою діяльність.

Крім зазначеної інформації, АУІС енергетичного сектору виконує низку задач організаційного управління та фінансово-економічної діяльності: планування діяльності та формування звітних матеріалів, бухгалтерський облік та розрахунки заробітної плати, матеріальне-технічне забезпечення, договірна робота тощо.

1.4 Модель загроз, модель порушника безпеки та ризики безпеки ІКС-ЕС

1.4.1 Поточний стан кібератак на вітчизняні енергетичні системи

У п. 1.2.4 вже згадані світові дані про катастрофічні наслідки реалізації різноманітних загроз безпеки енергетичних систем. Найбільш показовим прикладом реалізації кібератак на енергосистеми України можна вважати ситуацію 2015 року, коли сотні тисяч споживачів залишилися без світла.

За даними [70] протягом 2022 року – року початку повномасштабної агресії в Україні – шпигунські кібератаки найчастіше зазнавала інформаційна інфраструктура ОКІ, включаючи енергетичні компанії, Міністерство енергетики та інші.

Зокрема, як повідомляє ЗМІ [71] в жовтні 2022 року, російське хакерське угруповання Sandworm, користуючись вразливістю системи диспетчерського управління підстанціями і збору даних SCADA (Supervisory Control And Data Acquisition), провели атаку, що була спрямована до відключення підстанції та припинення електропостачання.

Forbes також інформує, за його запитом Адміністрація Держспецзв'язку України повідомила, що з початку повномасштабної війни країна-агресор реалізує декілька сотень кібератак щомісяця (рис. 1.8), більшість з яких припадає на ОКІ.

Доцільно звернути увагу, що в період літнього наступу Збройних Сил України в 2023 році загальна кількість кібератак зросла більше ніж вдвічі з 133 атак в червні до 287 атак у серпні. Тобто фактично кібернетична зброя використовувалася як засіб стримування наступального потенціалу України, що свідчить про координацію підступних зусиль хакерських угрупувань, що контролюються спеціальними службами агресора з командуванням його збройних сил.

А це означає, що підчас формування моделі порушника інформаційної безпеки та криптографічного захисту слід виходити з найбільш небезпечного порушника в особі спеціальної служби що має значний матеріально-фінансовий та науково-технічний ресурс.

Останній висновок відповідно означає необхідність у визначених умовах підвищення рівні захисту інформації, яка обробляється в енергетичному секторі.

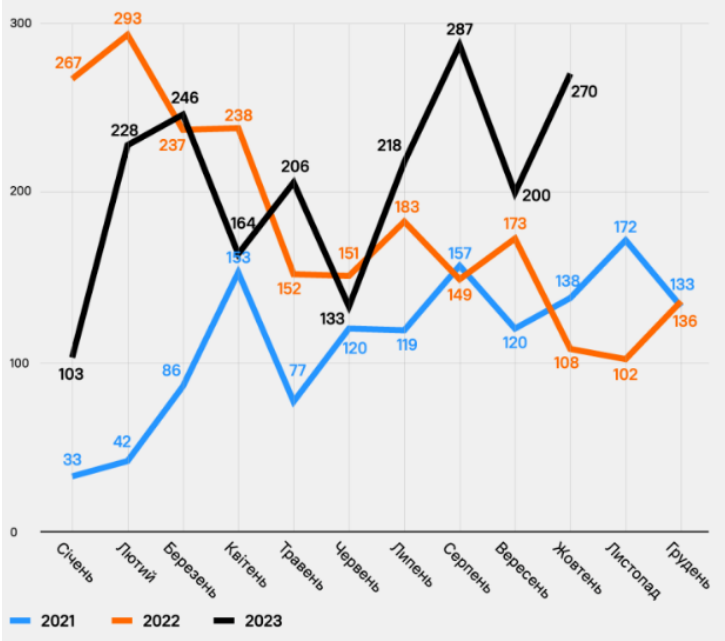

Рисунок 1.8 – Дані Держспецзв'язку щодо кількості кібератак в 2021–2023 рр. [71]

Виходячи з даних Держспецзв'язку, можливо також з'ясувати, що галузі енергетики та телекомунікацій за кількістю спостережених атак входять до п'яти пріоритетних цілей для хакерських угрупувань, що визначає актуальність захисту енергетичного сектору.

Як поінформували Forbes в Міністерстві енергетики України [71], на поточний час великі енергетичні компанії захищені краще за рахунок наявних значних бюджетів. Зокрема, НЕК «Укренерго» створила потужний центр кібербезпеки SOC (Security Operation Center), що відповідає кращим світовим практикам.

З викладеного можливо зробити висновок, що визначення базових принципів побудови корпоративного центру забезпечення кібербезпеки енергетичного сектору, обґрунтування його пріоритетних завдань та функцій є актуальним науково-прикладним завданням, яке потребує розв'язання.

1.4.2 Модель загроз та модель порушника кібербезпеки

Як було зазначено у п.1.1, концептуальні засади забезпечення фізичної безпеки та кібербезпеки електроенергетики визначені у Стратегії енергетичної безпеки України [8] серед інших викликів безпеці галузі відмічає загрози антропогенного (умовне позначення категорії – А), техногенного (позначення – Т) та природнього (позначення – П) походження.

Перераховані загрози безпеки можна подати в такій класифікації:

А.1 – Триваюча повномасштабна збройна агресія проти України.

А.2 – Загрози / кіберінциденти щодо ОКІ-ЕС як наявні та потенційно можливі явища і чинники, що створюють небезпеку, негативно впливають на стан кібербезпеки; небезпечні явища та події ненавмисного характеру, які становлять загрозу безпеці системам управління технологічними процесами та електронних комунікацій, підвищують імовірність порушення штатного режиму їхнього функціонування, загрожують безпеці інформаційних ресурсів.

А.3 – Загрози фізичній безпеці об’єктів енергетичної інфраструктури, включаючи протиправні дії, фізичні атаки, диверсії, спрямовані на відключення або пошкодження роботи операційних систем або систем забезпечення фізичної безпеки ОКІ-ЕС.

П-Т-А.1 – Несприятливі події ненавмисного характеру (природного, технічного, технологічного, помилкового характеру).

П-Т-А.2 – Відсутність спроможностей до “кризового” реагування, неадекватність реагування залучених суб’єктів у разі виникнення кризи.

П.1 – Вплив змін клімату на структуру та режими енергоспоживання.

За наявності вразливостей в інформаційних технологіях в разі реалізації потенційних загроз антропогенного, техногенного та природнього характеру підвищуються ризики породження ланцюгів можливих негативних наслідків для персоналу, об’єктів, засобів і обладнання енергетичного сектору та споживачів електричної енергії, а також для стану навколишнього середовища.

Перераховані зв'язки можливо подати у вигляді моделі логічних ланцюгів впливу загроз на погіршення спроможності стійкого функціонування ЕС, яка наведена на рис. 1.9.

Виходячи із запропонованої моделі, можливо з'ясувати, що відмічені загрози можуть безпосередньо впливати з одного боку на матеріально-фізичну складову ЕС, включаючи будівлі, споруди та обладнання, тобто на все, що утворює виробничу структуру об'єктів електроенергетики.

Цей вплив може призводити до вторинних (супутніх) наслідків реалізації загроз, а саме: небезпечних змін різких властивостей середовищ, включаючи підвищення їхньої температури, вологості, вібрацій, рівнів забруднення небезпечними речовинами або ураження небезпечним випромінюванням, що підвищує ризики виходу з ладу інформаційної інфраструктури.

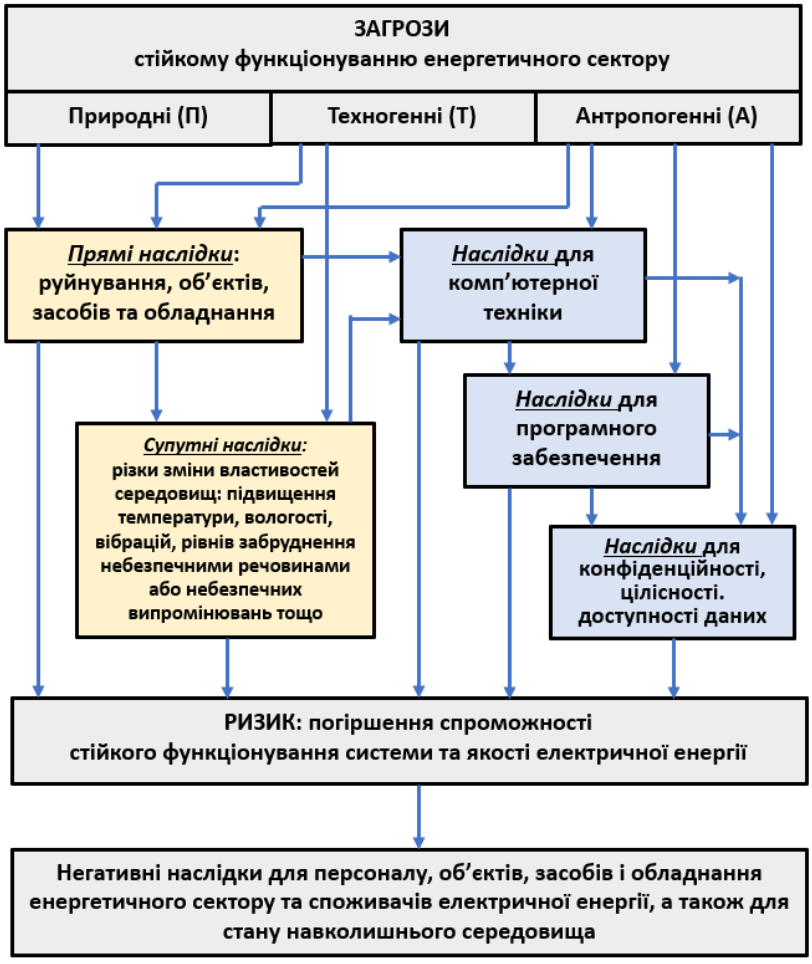

Рисунок 1.9 – Модель логічних ланцюгів впливу загроз на погіршення спроможності стійкого функціонування ЕС

З іншого боку, наслідком реалізації загроз антропогенного походження може бути цільове ураження інформаційних технологій в енергетиці, включаючи їх складові: програмні та апаратні платформи, а також технологічну інформацію та інформаційні ресурси.

Перераховані наслідки потенційно підвищують ризик погіршення спроможності стійкового функціонування енергетичного сектору та його головного показника – якості електричної енергії.

Підсумком цього каскадного процесу можуть бути згадані в п.1.2.4 катастрофічні наслідки для персоналу, об’єктів, засобів і обладнання енергетичного сектору та споживачів електричної енергії, а також для стану навколишнього середовища.

Виходячи з наданої в п. 1.4.1 характеристики кіберінцидентів і кібератак, визначеного ландшафту кіберзагроз, а також нормативних вимог щодо криптографічного захисту інформації [73], досягнення мети дослідження забезпечення кібербезпеки та гарантоздатності інформаційних систем енергетичного сектору потенційним порушником кібербезпеки доцільно вважати симбіоз спеціальної служби держави агресора та кримінальних угрупувань хакерів, які разом мають на меті руйнування української державності гібридним шляхом застосування військової сили та кібернетичного нападу.

Визначений варіант моделі порушника не узгоджується із запропонованою ієрархією таких моделей для криптографічного захисту інформації [73], але він може вважатися варіантом підвищених вимог для моделі порушника четвертого рівня. А це вимагає відповідного покращення функціональної схеми засобів криптографічного захисту – криптографічної схеми та уточнення функціонального профілю захисту засобу.

1.4.3 Оцінка та оброблення ризиків кібербезпеки для ІКС-ЕС

Визначений сімейством стандартів ISO/IEC 27-ї серії [74] процесний підхід до забезпечення інформаційної безпеки, включаючи її складову (кібербезпеки як однієї з ключових складових побудови відповідної системи управління), вимагає виконання заходів з оцінювання та оброблення ризиків інформаційної безпеки (далі – РІБ).

Згадаємо, що відповідно до вимог [74], для побудови системи управління інформаційною безпекою має бути визначений та застосований процес оброблення РІБ, що включає:

– вибір доцільних опцій оброблення РІБ, виходячи з результатів їхньої оцінки;

– визначення на підставі рекомендацій міжнародних стандартів або розробити потрібні заходи безпеки, що впроваджуються для вибраних опції оброблення ризиків.

Методологія оцінювання ризиків кібербезпеки інформаційних систем ОКІ системно досліджена в монографії Гончара С.Ф. [75], зокрема, розроблено методи обчислення сумарного ризику кібербезпеки інформаційних систем ОКІ з використанням значення максимальних наслідків.

У монографії [76] Суходоля О.М. та інших у рамках дослідження проблем забезпечення енергетичної безпеки України запропонували перспективну модель управління ризиками в енергетичному секторі, що суттєво покращує ситуацію в плані розв’язку відповідних завдань.

Водночас методологічне питання оброблення ризиків інформаційної безпеки в енергетичному секторі залишається остаточно не формалізованим завданням, тому визначення заходів з інформаційної безпеки (кіберзахисту) виконується експертами переважно за допомогою евристичних та експериментальних методів.

1.5 Визначення заходів з кіберзахисту та забезпечення гарантоздатності енергетичних систем

Проведений аналіз структури енергетичного сектору України, завдань і функцій, що реалізуються відповідними підприємствами та вимогами, які висуваються до інформаційного обміну в плані кібербезпеки та гарантоздатності, свідчить, що раціональним шляхом використання наявного потенціалу та ресурсів для досягнення головної мети – безперебійного постачання електроенергії, є створення корпоративного центру забезпечення кібербезпеки та гарантоздатності.

Концептуальні положення щодо стратегії та тактики організації та функціонування корпоративних центрів безпеки – SOC системно викладені в монографії К. Циммермана [77]. Він визначив, що SOC може вважатись такими, якщо він:

• забезпечує корпоративних учасників інформаційного обміну засобами оповіщення про підозрілі ситуації у сфері кібербезпеки;

• надає допомогу корпоративним учасникам у розв’язанні проблем навколо кіберінцидентів;

• поширює серед корпоративних учасників та заінтересованих сторін інформацію, пов'язану з кіберінцидентами.

Можливо, відмітити, що його теоретико-прикладне дослідження на поточний час має багато послідовників [78, 79]. Водночас питання особливості побудови та функціонування SOC енергетичної галузі системно не досліджені та потребують додаткового вивчення.

Зважаючи на те, що функціонування енергетичного сектору вимагає обробки команд управління та технологічної інформації в режимі реального часу, при цьому має бути забезпечено конфіденційність і цілісність відповідних ресурсів, що обмежує можливості застосування багатьох технологій кіберзахисту.

У [80] запропоновано для захисту інформації в мережі Інтернету речей (Internet of Things – IoT) використовувати методи «легкої» криптографії, що здатні забезпечити високу швидкодію на пристроях з обмеженими ресурсами, але в роботі розглядається лише питання забезпечення конфіденційності даних і команд. Для забезпечення контроля цілісності, а також вирішення завдань часткової розмежування доступу до ресурсів мережі SOC необхідні інші криптографічні рішення, які матимуть необхідну стійкість. А це потребує перегляду деяких моделей криптографічного захисту.

1.6 Постановка наукового завдання дослідження

Беручи до уваги розглянуті вище дослідження та дані з щорічних звітів щодо кіберінцидентів, слід визнати, що останнім часом, спостерігається зміна ландшафту кіберзлочинів, що потребує ретельного перегляду базових положень, моделей і методів забезпечення кіберзахисту ІКС-ЕС.

У зв’язку з цим існує необхідність вирішення актуального наукового завдання, сутність якого полягає в забезпечення виконання головного завдання енергетичного сектору – безперебійного енергопостачання завдяки підвищенню кібербезпеки і гарантоздатності його інформаційної інфраструктури.

Метою дисертаційного дослідження є подальший розвиток моделей і методів забезпечення кібербезпеки інформаційних систем енергетичного сектору завдяки комбінуванню корпоративного захисту критичної інформаційної інфраструктури та криптографічного підходів до побудови протоколів ідентифікації/автентифікації суб’єктів у ІКС-ЕС.

У відповідності до сформованої мети, для вирішення зазначеної науково-прикладної проблематики, в роботі сформульовані часткові завдання:

1. Побудувати модель центру корпоративного захисту інформації в ІКС-ЕС, що відповідає сучасним викликам безпеці та ураховує специфіку завдань і функцій ОЕС-У.

2. Розробити модель побудови децентралізованої системи розмежування доступу в мережі центру кібербезпеки.

3. Розробити методику декомпозиції складної інформаційної системи критичної інфраструктури.

4. Вдосконалити модель підсистеми криптографічного захисту інформації в ІКС-ЕС, включаючи розробку методу оцінки безпеки шифрування коротких повідомлень в мобільних компонентах ІКС-ЕС.

5. Розробити методику оцінки та раціонального визначення характеристик захисту криптографічної підсистеми.

1.7 Висновки до розділу 1

1. Визначено роль та проаналізовано сучасний стан забезпечення кібербезпеки та гарантоздатності ІКС-ЕС як одного з ключових елементів стійкого функціонування енергетичного сектору.

Встановлено, що ефективна реалізація заходів щодо кіберзахисту в енергетичному секторі повинна враховувати особливості інформаційних систем галузі, які за сукупністю визначених ознак та властивостей мають бути класифіковані як складні системи.

2. Проведено аналіз основних підходів, методів та сучасних практик забезпечення кібербезпеки та гарантоздатності ІКС-ЕС, зокрема, шляхом побудови корпоративного сегменту кібербезпеки та гарантоздатності та застосуванням інформаційних технологій криптографічного захисту.

Це дозволило виявити основні обмеження, що пов’язані з безпекою відповідних процесів та процедур забезпечення кібербезпеки та гарантоздатності в специфічних умовах функціонування енергосистем.

3. Сформульовано актуальне наукове завдання, яке полягає в подальшому розвитку моделей та методів забезпечення гарантоздатності та кібербезпеки ІКС-ЕС на основі інтегрування концептуальних принципів безпеки енергетичної галузі як складної системи взаємопов’язаних ОКІ.

Зокрема, для його вирішення визначено мету роботи, яка полягає в підвищенні ефективності захисту інформаційних ресурсів та технологічної інформації від загроз конфіденційності, цілісності та доступності за рахунок реалізації концепції корпоративного кіберзахисту, розробки покращених моделей і методів криптографічного захисту інформації, що збирається, передається та обробляється в ІКС-ЕС, та покращення процедур розмежування доступу в мережі центру кібербезпеки енергетичного сектору.

Основні результати розділу опубліковані автором у працях [1–3, 7].

РОЗДІЛ 2
МОДЕЛІ ЕТАПУ ПРОЄКТУВАННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ ІКС-ЕС ТА ЇХ КІБЕРЗАХИСТУ

2.1 Методологічні засади створення та функціонування центру кібербезпеки інформаційної інфраструктури енергетичного сектору

2.1.1 Об’єкти ядерної енергетики як елементи критичної енергетичної інфраструктури

Запропонована в п. 1.4.2 модель логічних ланцюгів впливу загроз на погіршення спроможності стійкого функціонування ЕС (рис. 1.9) дає більш чітке розуміння визначеного на законодавчому рівні поняття критична енергетична інфраструктура.

Згадаємо, що відповідно до Закону [1] під критичною енергетична інфраструктура розуміють об’єкти енергетичної інфраструктури, виведення з ладу або руйнування яких матиме суттєвий вплив на національну безпеку та оборону, навколишнє природне середовище та може призвести до значних фінансових збитків і людських жертв.

До відповідної категорії слід віднести, зокрема, об'єкти ядерної енергетики (ОЯЕ), стосовно безпеки яких існує багато напрацювань у частині регуляторних актів та науково-практичних досліджень, тому уявляється доцільним розпочати передпроєктний аналіз архітектури системи кіберзахисту та забезпечення гарантоздатності саме з цих об’єктів.

ОЯЕ є складними системами структурного типу, автоматизовані системи яких оперують великими масивами команд та даних про стан обладнання та технологічних процесів, викривлення або блокування яких потенційно може призвести до нештатних і, навіть, катастрофічних ситуацій [67, 81].

Стійке надійне автоматизоване керування засобами фізичної інфраструктури ОЯЕ є запорукою уникнення нештатних ситуацій, тому забезпечення кіберстійкості та гарантоздатності інформаційної

інфраструктури цих об’єктів в умовах зростання кількості та потужності кібератак на критичні інформаційні системи, повномасштабної війни і обмежених ресурсів концентрація та координація зусиль для забезпечення кібербезпеки ОЯЕ є єдиним шляхом для розв’язання визначених проблем в галузі.

Раціональним рішенням на цьому шляху має стати розбудова концепції корпоративного центру кібербезпеки ОЯЕ (КЦК ОЯЕ). Зауважимо, що створення в енергетичній галузі декількох корпоративних центрів узгоджується з рекомендацією в [77] щодо досягнення для центру кібербезпеки балансу між його розміром і спостережністю/гнучкістю для ефективного виконання своєї місії.

Зауважимо, що управління кібербезпекою ОКІ передбачає отримання інформації від складових системи, що утворюється множиною територіально розподілених елементів, кожний з яких функціонує за власними законами та здійснює вплив на інші елементи системи.

Необхідність моніторингу та інтеграції великої кількості різноманітної динамічної інформації, що характеризує стан кожного елемента і системи у цілому, виявлення зв’язків і закономірностей їх взаємного впливу з урахуванням комплексу зовнішніх та внутрішніх загроз, прийняття обґрунтованих оперативних стратегічних рішень по забезпеченню безпеки в режимі реального часу потребує потужних обчислювальних ресурсів та спеціальних програмних продуктів, що працюють за певними науково обґрунтованими процедурами.

У [83] звернено увагу на забезпеченні ефективності прикладних наукових досліджень у вирішенні актуальних науково-прикладних проблем, що пов’язані з ліквідацією наслідків Чорнобильської катастрофи, та необхідності системного підходу до реалізації задач, пов’язаних з забезпечення кібербезпеки та гарантоздатності автоматизованих систем ОЯЕ.

Роботи дослідників охоплюють широкий спектр підходів до проблем комп’ютерної безпеки ОЯЕ. Так, у [82, 84] зазначається, що комп'ютерна

безпека все більше визнається ключовим компонентом ядерної безпеки та проведення оцінок комп'ютерної безпеки на ядерних установках.

У [85] пропонується метод впровадження заходів та засобів кібербезпеки в рамках загальної системи безпеки на стадії її розробки. Метод запроваджує конкретні заходи безпеки, які базуються на існуючої практиці проєкту будівництва ядерної установки.

Результати проведення порівняльного аналізу результатів, отриманих у результаті застосування різних засобів контролю безпеки та оцінки ризиків, наведений у [86].

У роботі [87] проведено аналіз факторів зниження ризику ядерних та радіаційних аварій на АЕС з урахуванням специфічних умов, пов’язаних з інформаційною безпекою в системі фізичного захисту атомних електростанцій. Розглянуто зв’язок гетерогенних факторів, що можуть впливати на ризик виникнення аварій на ОЯЕ, можливість і шляхи подальшого підвищення адекватності моделювання динаміки захисту інформації з обмеженим доступом, що безпосередньо стосується функціонування автоматизованого комплексу інженерно-технічних засобів фізичного захисту АЕС.

Проблематика комп’ютерної та інформаційної безпеки у площині фізичного захисту, а також нормативно-правове забезпечення комп’ютерної безпеки на ядерних об’єктах в Україні розглянуті у [88], де основний акцент зроблено на комп’ютерну безпеку АУІС, важливих для ядерної безпеки.

Водночас поза увагою дослідників залишилося питання реалізації системного підходу до забезпечення кібербезпеки всього комплексу ядерних об’єктів як в світі, так і в Україні.

2.1.2 Моделі управління кібербезпекою

На поточний час забезпечення інформаційної безпеки ОКІ регламентується міжнародними та вітчизняними стандартами [74, 89–92].

В [93] запропонована модель кіберзахисту, яка вирішує питання делегування задач кіберзагроз для різних рівнів захисту.

На відміну від зазначеної моделі в [81, 199] розроблена комплексна модель взаємодії елементів ОЯЕ. При цьому елементами інформаційної систем ОЯЕ виступають: система захисту інформації, програмно-апаратні засоби системи ОЯЕ, інсайдери, які взаємодіють між собою та зовнішнім середовищем.

На рис. 2.1 приведена зазначена модель взаємодії суб'єктів та об'єктів в інформаційній системі ОЯЕ.

Рисунок 2.1 – Модель взаємодії елементів інформаційної системи ОЯБ [81]

Застосування вказаної моделі переважно обмежується аналізом точок впливу загроз та наслідків для керованих процесів та обладнання, при цьому

вона не розкриває послідовність бізнес-процесів для досягнення мети функціонування енергосистем.

З метою визначення методологічних засад досліджень та проєктування апаратно-програмного комплексу забезпечення кібербезпеки та гарантоздатності розроблено іншу модель, в основу якої покладено місію енергосистем та механізм її досягнення.

А саме з метою підтримки реалізації центральної задачі (місії) енергосистем – надійного безпечного постачання електроенергії – стратегічним завданням корпоративного центру кібербезпеки пропонується вважати консолідацію всіх функцій забезпечення кіберзахисту та гарантоздатності в єдиній організаційно-технічній структурі (рис. 2.2).

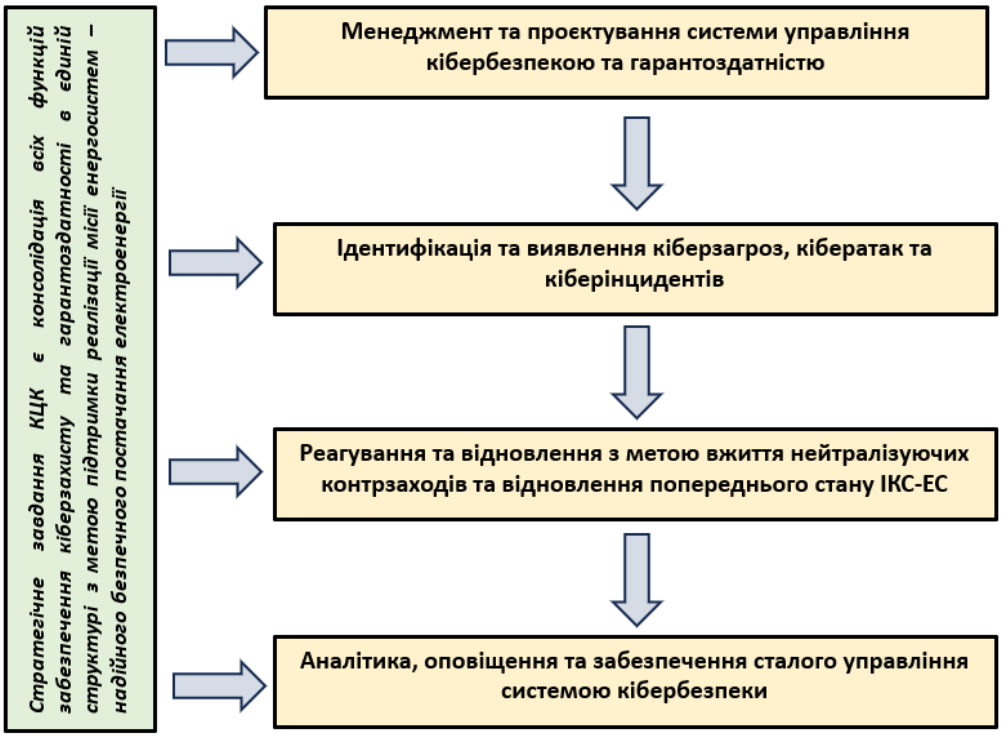

Рисунок 2.2 – Завдання та функції КЦК

З урахуванням вимог стандартів системи управління інформаційною безпекою [74] як напрямів діяльності персоналу КЦК та функціональних можливостей апаратно-програмного комплексу їх підтримки пропонується вважати такі процедури й процеси:

– Менеджмент та проєктування системи управління кібербезпекою та гарантоздатністю.
– Ідентифікація та виявлення кіберзагроз, кібератак та кіберінцидентів.
– Реагування та відновлення з метою вжиття нейтралізуючих контрзаходів та повернення попереднього стану ІКС-ЕС.
– Аналітика, оповіщення та забезпечення сталого управління системою кібербезпеки.

Виходячи з викладеного та з урахуванням нормативних вимог щодо стійкості енергосистем [24–26], можливо сформувати таку бізнес-модель забезпечення кіберстійкості та гарантоздатності інформаційних технологій ЕС (рис. 2.3), яка подана в нотації IDF0.

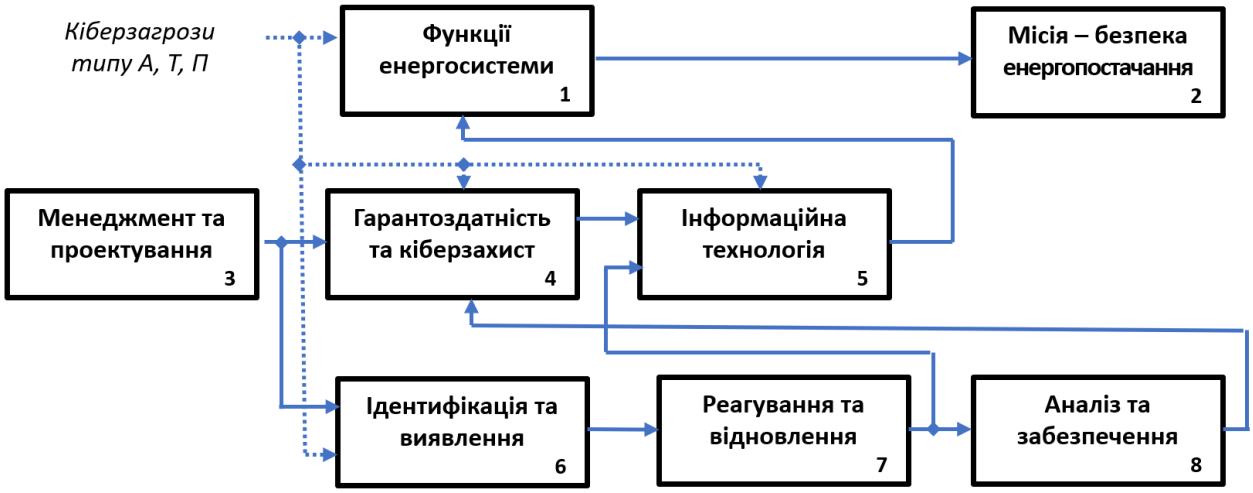

Рисунок 2.3 – Модель забезпечення гарантоздатності та кіберзахисту в ЕС у нотації IDEF0

Стохастичним фактором у моделі, що впливає на реалізацію функцій енергосистеми, стан інформаційних технологій ЕС, підсистему забезпечення гарантоздатності і кіберзахисту, а також на процедури ідентифікації та виявлення небезпечних подій, є сукупність потенційних загроз безпеки антропогенного, техногенного та природного характеру.

Процедури і процеси моделі забезпечення гарантоздатності та кіберзахисту в ЕС (рис. 2.3) поділяються на окремі функції, що визначаються

стандартами системи управління інформаційною безпекою, зокрема, персонал КЦК має виконувати функції, що визначені в [74, 94], які підтримуються апаратно-програмним комплексом центру кібербезпеки (рис. 2.4).

На реалізацію визначених процесів і процедур суттєво впливають особливості застосованих для управління енергетичним сектором інформаційних технологій та їх взаємодії з фізичним середовищем, яке керується. Саме тому в наступних розділах дослідження увага фокусується на відповідних характеристиках інформаційних систем цієї галузі.

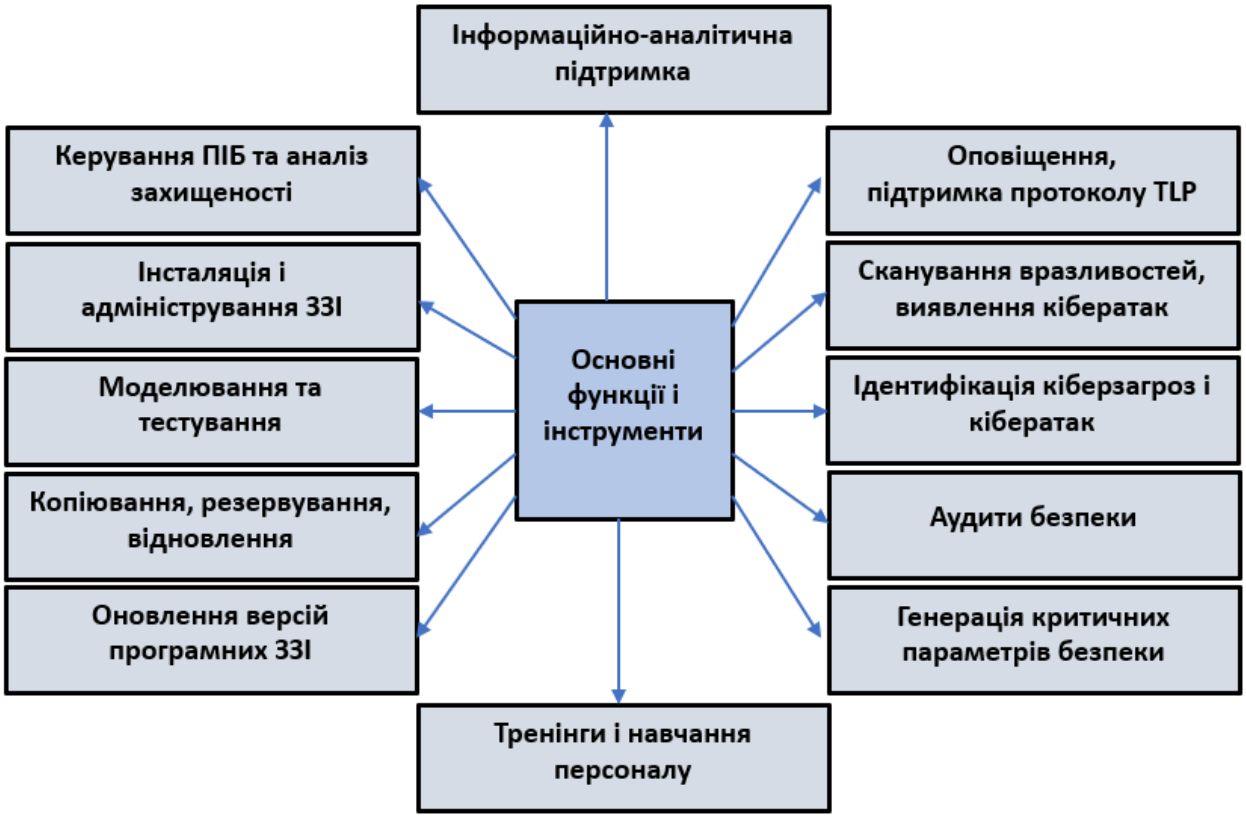

Рисунок 2.4 – Основні функції й інструменти безпеки КЦК

Відповідно до [94], для протидії кібератакам апаратно-програмний комплекс КЦК повинен, що найменш, реалізовувати такі функції (включати відповідні інструменти):

– забезпечення безпеки міжмережевої взаємодії;
– захист від шкідливого програмного забезпечення;
– захист периметра мережі;

- розмежування доступу до цифрових ресурсів;
- моніторинг подій і аудит безпеки;
- підтримка моделей оцінки ризиків:
- виявлення кібератак і запобігання ним;
- фільтрація контенту і запобігання витоку критичної (конфіденційної) інформації;
- забезпечення та контроль цілісності даних;
- резервне копіювання і відновлення даних;
- установка оновлень програмного забезпечення;
- адміністрування безпеки та керування політикою безпеки;
- підтримка графічного інтерфейсу з користувачами, візуалізація даних;
- аналіз вразливостей.

Підсумовуючи вищезазначене, можливо стверджувати, що автоматизована система управління кібербезпекою інформаційною інфраструктурою енергосистем, включаючи ОЯЕ, має бути організаційно-технічною системою, яка виконує повний комплекс визначених функції забезпечення кібербезпеки та гарантоздатності як окремих функціональних елементів і процесів, так і сукупності об’єктів енергетичного сектору в цілому.

Загалом система управління кібербезпекою та гарантоздатністю повинна забезпечити стійкість, живучість і безпеку функціонування фізичної інфраструктури енергосистем, зокрема ОЯЕ. Метою реалізації вказаної системи є досягнення такого рівня кібербезпеки, за умов якого забезпечується мінімальне значення прийнятного рівня сумарного ризику [37, 75].

Управління енергосистемою передбачає цілеспрямований вплив на керовані об'єкти для підтримки їхніх характеристик у наперед визначених інтервалах (рівнях) значень [24, 25, 37]. Тому управління кібербезпекою та гарантоздатністю вимагає постійного відстеження відповідних параметрів [25], що характеризують керований об'єкт, тобто функціонування встановленої системи контролю, моніторингу та оперативного реагування на зміну цих параметрів.

Під час формування вимог до автоматизованої системи управління кібербезпекою та гарантоздатністю відповідно до [94] необхідно враховувати, що навантаження на її функціонування обумовлюється кількістю та складністю АУІС, які захищаються, та середньою кількістю прогнозованих кіберінцидентів в них за визначений проміжок часу.

Чутливим аспектом у цьому випадку є визначення цифрових активів, які підлягають захисту [37, 94] для вибору засобів контролю та управління, які відповідають реальним ризикам. З одного боку, існує можливість виникнення несприятливої ситуації виділення необґрунтовану кількість ресурсів для забезпечення кібербезпеки цифрових активів з низьким рівнем ризику, з іншого боку, існує загроза не врахувати небезпеку для окремого контролеру, блокування якого потенційно може негативно вплинути на функціонування навіть окремого сегменту енергосистеми.

Згідно з [87, 88, 94], перелік основних суб'єктів ініціаторів кіберзагроз для інформаційних систем енергетичного сектору за категорією наявності або відсутності злого умислу включає персонал АУІС (помилки), інсайдерів, промислових шпигунів, окремих злочинців та їхні угрупування, терористичні угрупування, іноземні спецслужби. Залежно від способу реалізації атаки це можуть бути оператори ботнету, «фішери», «сніфери», «спамери» тощо.

З урахуванням нормативних вимог [11, 24, 26] основними цілями створення корпоративного центру кібербезпеки та гарантоздатності (КЦКГ) енергосистем, включаючи ОЯЕ, є такі:

– підвищення ефективності прийняття управлінських рішень за рахунок впровадження нових інструментів управління кібербезпекою, що базуються на сучасних інформаційних технологіях і відповідних кращому міжнародному досвіду в сфері управління складними системами міжнаціонального масштабу;

– уніфікація процедур оцінки рівня кібербезпеки на основі класифікації станів безпеки та множини характеристичних показників поведінки (МХПП) систем;

– утворення належних умов для проведення оперативного (поточного) аудиту кібербезпеки інформаційних систем ОЯЕ на підставі МХПП, тестування систем кіберзахисту на основі затверджених методик, включаючи технології прихованого проникнення в системи;

– забезпечення корпоративного оперативного моніторингу конфігурацій програмних і апаратних платформ інформаційних середовищ, засобів захисту;

– підвищення кваліфікації всіх учасників процесів забезпечення кібербезпеки шляхом проведення в реальному часі тренінгів і навчань, які мають бути наближені до сучасних реалій;

– забезпечення за рахунок формування єдиного інформаційного простору керівного складу і працівників енергетичного комплексу структурованою достовірною та оперативною інформацією згідно з наданими їм повноваженнями;

– скорочення часу на локалізацію наслідків реалізації кіберзагроз та відновлення штатного функціонування завдяки спеціально підготовленого персоналу та захищеного зберігання за дорученням власників систем резервних копій програмного забезпечення та інформаційних масивів;

– забезпечення системного підходу до оперативної аналітики стану кібербезпеки у кіберпросторі, виявлення та аналізу аномальної поведінки систем і мереж, оцінки ризиків, моделювання та прогнозування розвідку подій у кіберпросторі;

– реалізація заходів стримування шифруючих або руйнуючих шкідливих кодів, формування тактики їх нейтралізації та блокування;

– виявлення систематичних спроб проникнення та шкідливих ресурсів в кіберпросторі, інформування правоохоронних органів для прийняття рішень;

– масштабування, інтеграція існуючих і новостворюваних систем кіберзахисту; розвиток інструментів збору та аналітичної обробки інформації.

2.1.3 Керівні принципи проєктування та архітектура КЦК

Концептуальні засади побудови центрів онлайн управління безпекою на основі застосування математичних моделей для уточнення інформації, що отримана на основі суджень експертів та даних, що накопичуються в системі, вперше запропонована в [95]. Ця уточнена інформація утворює підґрунтя для застосування моделей оцінки ризиків, які також є джерелом вихідних даних для моделей підтримки прийняття рішень менеджментом безпеки.

Останнім часом опубліковано чимало результатів досліджень у галузі підходів до автоматизації управління безпекою ОКІ, зокрема, існує сучасна концепція побудови SOC (рис. 2.5) від компанії CISCO [96], застосування якої поширюється в світі.

Можливо звернути увагу на те, що зазначена концепція, за суттю, переважно фокусується на аспектах отримання від сенсорів інформації про ймовірні загрози безпеки інформаційних систем та на взаємодії інструментів виявлення та попередження загроз. Умовно кажучи, це по відношенню до об’єкта захисту та джерела загроз позиція третьої сторони, яка не бере участі в розв’язанні всього кола проблем щодо надійного безпечного функціонування фізичної інфраструктури, зокрема, це стосується питань забезпечення гарантоздатності.

Так, ставити крапку у цьому питанні ще зарано, оскільки, як було з’ясовано раніше, об’єкт дослідження має суттєві відмінності з точки зору забезпечення його кібербезпеки та гарантоздатності.

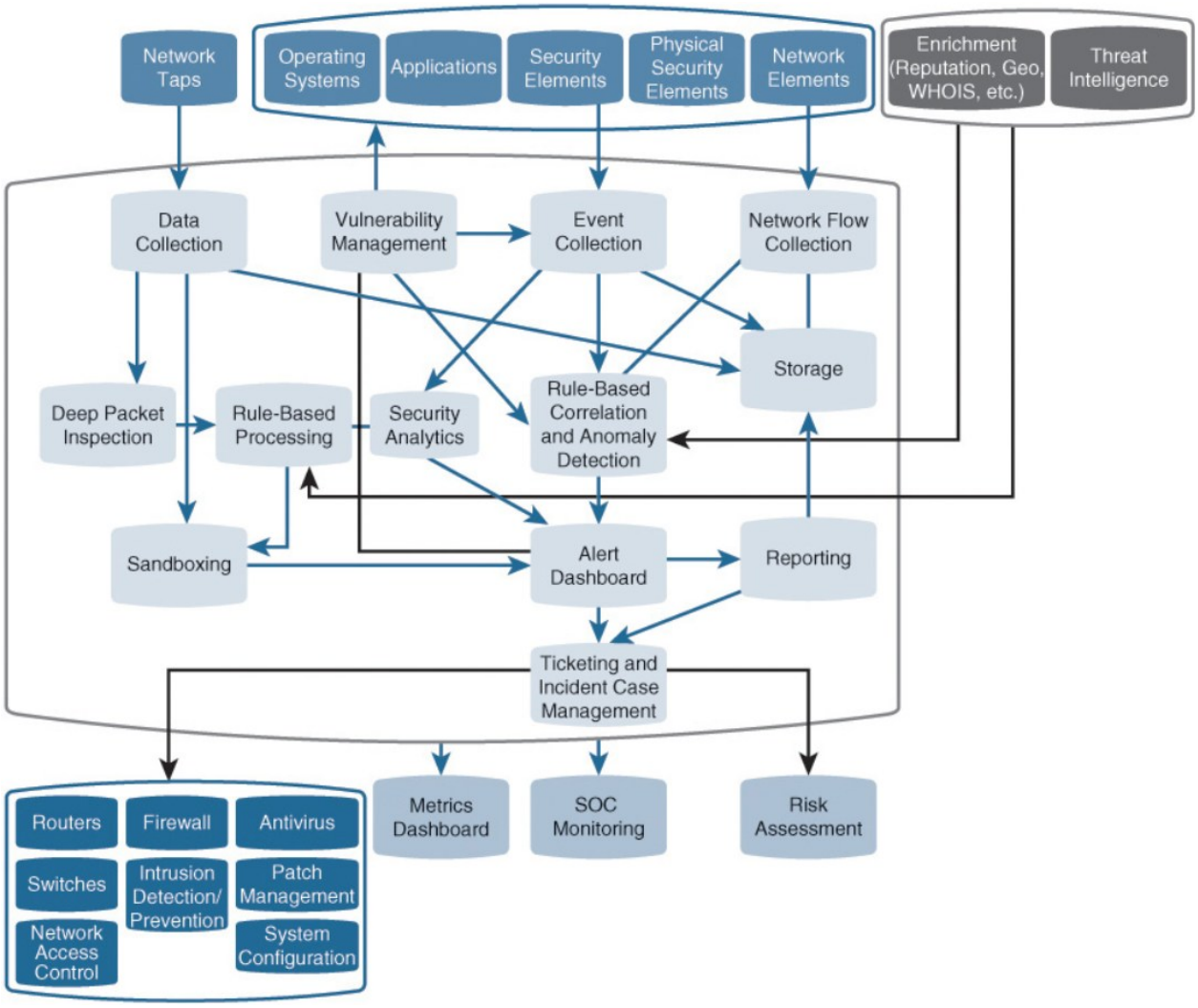

Рисунок 2.5 – Концепція CISCO архітектури SOC

(SOC’s Conceptual Architecture [96])

Постійне уточнення наведеного вище переліку функцій управління кібербезпекою та гарантоздатністю що обумовлене змінами у ландшафті кіберзагроз, нагальна потреба підтримки застосування новітніх інформаційних технологій та сенсорного обладнання, що впроваджуються внаслідок заміни застарілого обладнання та вдосконалення керуючих комплексів енергосистем, потребують подальшого пошуку адекватних рішень.

Виходячи з вищевикладеного, перспективним уявляється проєктування апаратно-програмного комплексу центру управління безпекою енергетичного сектору на основі сервіс-орієнтованої архітектури (Service-oriented architecture

– SOA) [97] із дотриманням таких базових принципів: інтеграції, централізації, уніфікації, еволюційності, масштабованості, модульності та живучості.

В аспекті предметної галузі дослідження принципи інтеграції та консолідації розглядаються як реалізовані стосовно розрізнених масивів даних про об’єкт енергетики (зокрема, ядерної) та припускають створення консолідованого сховища предметно-орієнтованих, інтегрованих, таких що зберігають цілісність та доступність, підтримують хронологію, постійно оновлюються достовірною інформацією наборів даних.

Принцип централізації стосується процедури ведення метаданих і нормативно-довідкової інформації – всі підсистеми автоматизованої системи управління повинні використовувати єдині метадані та нормативно-довідкову інформацію, забезпечувати можливість формування локальних довідників, підтримувати версійність метаданих та нормативно-довідкової інформації для забезпечення можливості проведення аналізу з використанням даних за попередні часові періоди.

Уніфікація рішень поширюється на процеси взаємодії зі структурами і організаціями, що входять в контур управління безпекою в частині єдиної інформаційно-комунікаційної системи і форматів даних.

Можливість поетапної розробки і впровадження додаткових компонент повинна забезпечуватись саме архітектурою SOA. Наслідком цього є можливість практично необмеженого розширення функціонального доповнення центру без принципової заміни системно-технічної платформи, що забезпечить відкритість і еволюційність системи;

Шляхом дотримання принципу масштабованості апаратно-програмного комплексу забезпечена можливість роботи центру в умовах зростання потоків даних, кількості автоматизованих робочих місць і обсягу завдань що виконуються без істотної перебудови його проєкту.

Принцип модульності передбачає створення центру як сукупності відносно незалежних модулів для реалізації окремих функцій і завдань, що забезпечує гнучкість формування функціональності окремих автоматизованих

робочих місць, підсистем і системи в цілому під необхідну структуру і механізми управління безпекою.

Живучість центру є найважливішою складової характеристики гарантоздатності, що забезпечувати безперебійну роботу, отримання достовірних результатів в умовах змінної обстановки.

Абстрагуючись від суто технічних заходів керування фізичним середовищем енергосистем, звернемо увагу на той факт, що виконання відповідних дій відбувається на підставі вироблених та схвалених рішень команд і доручень (*D* – decision), які сформовані шляхом виконання певних процедур прийняття рішень.

Відповідні процедури реалізуються за допомогою комп'ютерних засобів і програмних продуктів, що надають певні сервіси ($S_1, S_2, \dots, S_m$) на підставі вихідної інформації про стан об'єктів у певні моменти часу ($I(t_0), I(t_1), I(t_2), \dots$), нормативних вимог (*L* – low), а також накопичених апріорних знань і досвіду управлінської діяльності у відповідній галузі (*E* – experience).

Для обраних позначень процес функціонування системи управління безпекою енергосистеми в рамках формування конкретної команди опрацювання кіберінциденту може бути описаний ітераційним рівнянням

$$D_j = S_{i_k}\left(L, E, I(t_k), S_{i_{k-1}}\left(L, E, I(t_{k-1}), \dots S_{i_0}\left(L, E, I(t_0)\right)\right)\right), \qquad (2.1)$$

де послідовність номерів застосованих сервісів $\{i_0, i_1, \dots, i_{k-1}, i_k\}$ будемо називати шаблоном обробки кіберінцидента.

Шаблон обробки має визначатись, виходячи з моделі кіберінцидента, з урахуванням наявних програм що надають сервіси (інструментарій обробки). Множина шаблонів обробки поповнюється та уточняється на підставі аналізу нових кіберзагроз та методів їх стримування [98].

Зазначимо, що хоча в рівнянні (2.1) множини вимог (L) та знань (E) не індексуються, в загальному випадку після кожної ітерації потенційно до застосування нового сервісу може мати місце апостеріорне отримання додаткових вимог та вимог та знань:

$$L_m = L_{m-1} \cup \Delta L_{m-1},\ E_m = E_{m-1} \cup \Delta E_{m-1},\ m = \overline{1,k}, \qquad (2.2)$$

де ΔL_{m-1} та ΔE_{m-1} приріст бази вимог та бази знань після виконання чергового кроку обробки кіберінциденту. Якщо таких змін не спостерігається, то в (2.2) вважаємо, що

$$\Delta L_{m-1} = \{\emptyset\} \text{ та/або } \Delta E_{m-1} = \{\emptyset\}.$$

Підчас обробки інциденту можуть виникати ситуації невизначеності внаслідок відсутності в базі даних моделей (БМ) моделі для нього або в базі даних шаблонів обробки (БШ) відсутній шаблон обробки відповідного інциденту, або в підсумки обробки за обраним шаблоном не було отримано очікуваного результату. В цих випадках обробка кіберінциденту передається від оператора обробки до експерта з моделювання та розв’язку таких проблем.

Загальна блок-схема методики опрацювання кіберінцидентів у КЦК наведена на рис. 2.6.

На наведеній блок-схемі для її спрощення розглядається випадок лише одного сенсору, в загальному випадку схема повинна враховувати їх велику кількість та забезпечувати належне сканування даних із них, наприклад, за допомогою системи SIEM (Security information and event management).

Використовуючи запропоновану в п. 2.1.2 модель забезпечення гарантоздатності та кіберзахисту в ЕС, зроблені зауваження щодо процедур обробки інформації в КЦК (рівняння (2.1) та блок схема методики опрацювання кіберінцидентів). можливо запропонувати таку модель функціонування КЦК (рис. 2.7).

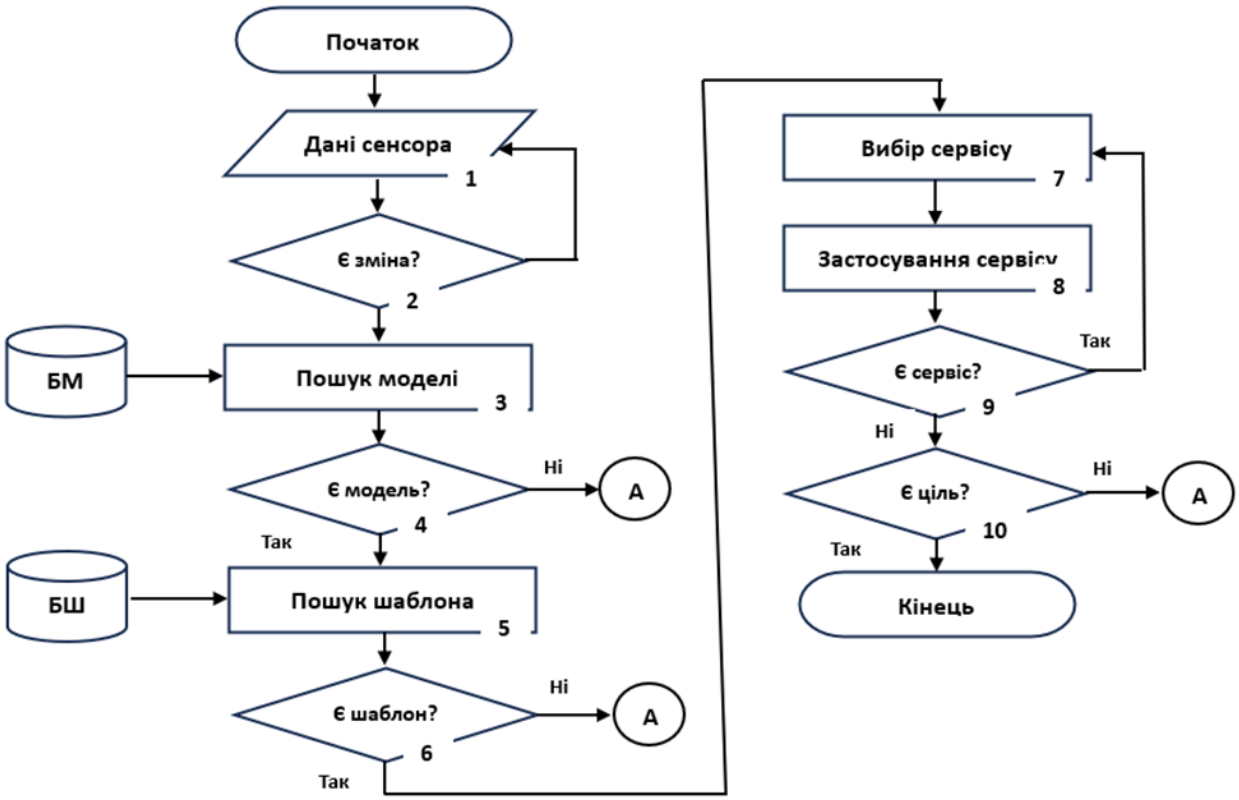

Рисунок 2.6 – Блок-схема методики опрацювання кіберінцидентів

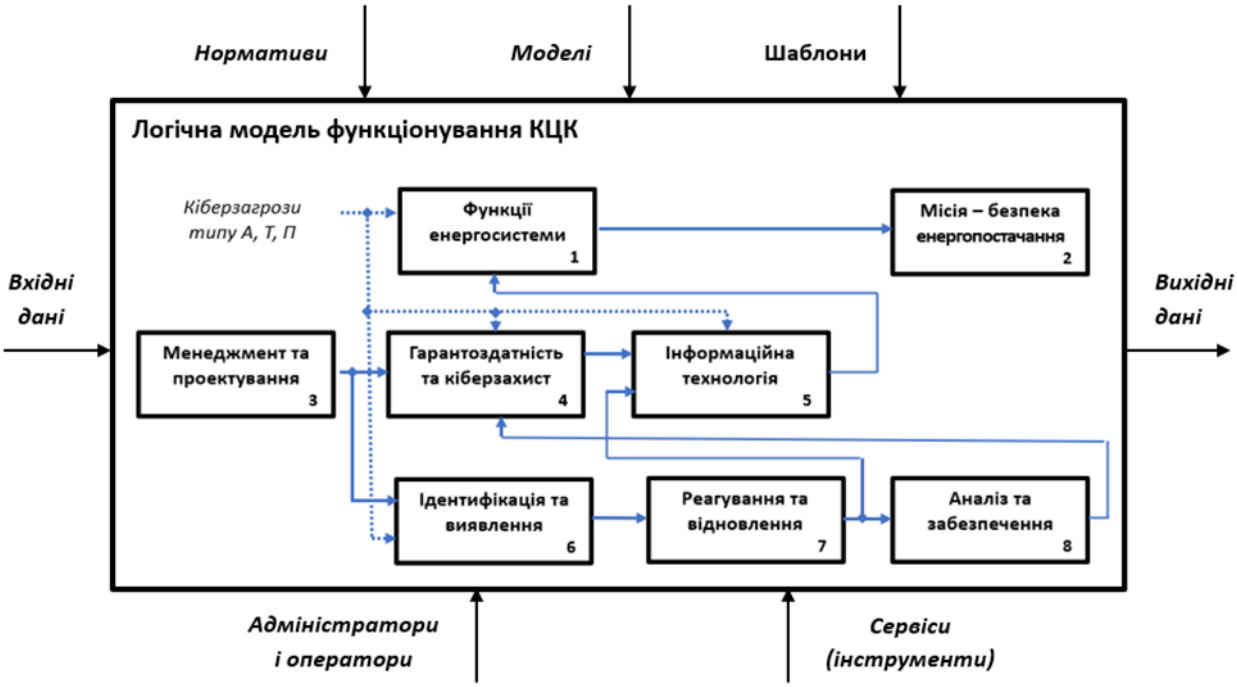

Рисунок 2.7 – Модель функціонування КЦК – CyberPlatform

Модель складається з двох взаємодіючих складових: логіки функціонування КЦК (бізнес-логіки) та поданої в нотації IDEF0 платформи виконання операцій з обробки інцидентів.

Платформа (CyberPlatform) виконання операцій з обробки інцидентів має забезпечувати підтримку всіх баз даних, включаючи нормативний довідник, базу моделей кіберінцидентів та базу даних шаблонів їх обробки.

CyberPlatform включає репозиторій сервісів (service repository), що відповідають визначеному в п. 2.1.2 обов'язкових інструментів кібербезпеки та зв'язуючу шину доступу до сервісів (service bus).

Фактично CyberPlatform – це централізована зона, де відбувається узгоджена агрегація сервісів та визначеної інформації. Така концентрація відбувається завдяки засобам моніторингу та детектування кіберпростору з метою подальшого використання для оперативного, систематичного та планового попередження учасників системи про кіберзагрози.

Відповідно до функцій КЦК платформа може управлятись одним центральним (або декількома) суб'єктом системи. CyberPlatform забезпечує функціонування централізованих кіберсервісів, як-от: захист від атак типу «відмова в обслуговуванні»; захист від дій шкідливих програм; захист вебдодатків та вебсервісів; захист e-mail додатків та служб, а також моніторинг та оцінку поточного стану кіберпростору тощо.

CyberPlatform має підтримувати функції централізованого моніторингу та детектування мережевих аномалій, попередження атак нової генерації, детектування та аналізу шкідливих кодів, управління захистом електронної пошти та інших функції.

CyberPlatform як центральна ланка системи кібербезпеки енергосистем та агрегатор відповідної інформації має підтримувати в межах визначених протоколів та процедур взаємодію з національними суб'єктами забезпечення кібербезпеки та з міжнародними галузевими системами збору та розповсюдження аналітичної та статистичної інформації щодо кіберзагроз (системи кібераналітики).

Співпраця із глобальними системами кібербезпеки надає значних переваг, насамперед, у випадках здійснення кібератак з-за кордону, коли їх швидке розпізнавання може бути ускладнене, а протидія лише локальними «силами» може виявитися не завжди ефективною.

Найважливішою функцією CyberPlatform, яка не передбачена багатьма проєктами побудови SOC, є підтримка процесів відновлення критичної інформаційної інфраструктури енергосистем після кібератак та забезпечення середовища для проведення професійного розслідування умов та обставин виникнення кіберінцидентів з метою їх попередження у майбутньому.

Організаційно-штатна структура корпоративної системи управління кібербезпекою енергетичного сектору, включати кадрову політику, діяльність із планування, розподіл відповідальності, практичне виконання завдань, процедури, процеси і ресурси, повинна визначатись відповідно до законодавства України.

2.2 Динамічна модель управління кібербезпекою і гарантоздатністю в ІКС-ЕС

2.2.1 Попередні результати теорії управління

Науково-практичній інтерес до побудови центрів кібербезпеки як невід’ємного компоненту захищених гарантоздатних систем постійно зростає, що обумовлено високими вимогами до надання інформаційних послуг загалом ОКІ та, зокрема, енергетичним системам.

Зауважимо, що концептуально принципи побудови та функціонування центрів кїбербезпеки, що призначені для подолання критичних подій в кіберпросторі, та ситуаційних центрів, які забезпечують скоординовані зусилля щодо ліквідації катастроф та аварії, співпадають та враховують кращі

рішення з обох боків. Зокрема, це стосується методів та технологій забезпечення їх кіберзахисту [111] та гарантоздатності [99].

Як будь-які організаційно-технічні системи працюють у гармонійному поєднанні віртуального простору інформаційних технологій та природнього інтелекту експертів, за якими залишається беззаперечне право формування, уточнення, корегування та відміни майже всіх управлінських рішень відповідно до компетенції.

Розв'язанню проблем раціонального управління такими системами сприяє та суттєво його покращує застосування таких сучасних інформаційних технологій та інструментів, як SIEM [101], Threat Intelligence [102], бази знань про кібератаки MITRE ATT&CK [103], технології атрибутизації кібератак [104] тощо.

Зручним інструментом управління забезпеченням кібербезпеки та гарантоздатності (КтГ), як і іншими виробничими процесами енергетичного сектору, можуть бути мережеві графіки, що є динамічними моделями відповідних процесів, що відображає технологічну залежність етапів комплексу робіт і послідовність їх виконання та відображає їх здійснення в часі.

Водночас комплексне забезпечення динамічного раціонального управління забезпеченням КтГ в АС є доволі складними процесом, запропонувати для якого ефективну методику є нетривіальною задачею.

Розв'язанню таких задач присвячено багато наукових публікацій, але пошуки нових рішень продовжуються. Основна складність завдання полягає в тому, що функції захисту в комп'ютерних системах переважно дискретні за визначенням, що повністю або частково унеможливлює застосування відомих математичних методів оптимізації управління.

Зокрема, в [105] відмічено, що на можливість застосування традиційних методів оптимального управління впливають особливості цих систем, тому для прийняття найкращого рішення щодо управляння об'єктами захисту

інформації досліджено застосування методів ситуаційного управління на основі сигнатурних моделей.

Погоджуючись в цілому з цією тезою, вважаємо за необхідне дещо уточнити сутність цих відмінностей, а саме це стосується: реалізації управління забезпечення КтГ системи в умовах невизначеності та негативного впливу на неї як з боку кіберпростору, так і внаслідок навмисних або випадковий дій її легальних користувачів; цілі і завдання управління можуть бути сформульовані як якісно, так і кількісно; опис об’єкта дуже складно піддається формалізації.

У [106, 107] методологія формалізації станів системи, що управляється, зазнала розвитку, але, на нашу думку, певним недоліком цих робіт, як і попереднього дослідження [105] цих авторів, є відсутність в роботах критеріїв досягнення визначеної мети, які б визначали стан захищеності інформації. Як наслідок, у [105] висновок анонсує лише можливість застосування алгоритмічного підходу до визначення повної множини ситуацій, створення бази знань, використання якої сприятиме підвищенню обґрунтованості управлінських рішень у разі застосування запропонованої методики використання сигнатурної моделі управління об'єктами системи захисту інформації.

У [108] запропоновано, як на основі експертних суджень побудувати математичну модель комплексної безпеки комп'ютерних систем (КС). Показано, що застосування модифікованого методу нестрогого ранжування дозволяє визначити ваги Фішберна для одного рівня ієрархії. В дослідженні застосовані показники рівня безпеки по деяким невизначеним критеріям. У [109] автором продовжено дослідження комплексної безпеки КС шляхом оцінки ймовірностей реалізації деяких загроз без посилання на конкретні критерії безпеки.

У [110] розглянуті концептуальні положення ряду дослідницьких ініціатив, пов’язаних з інноваційними технологіями для хмарних обчислень у сферах екологічної безпеки, забезпечення якості, складу послуг і управління

системою, а також без формалізації представлені технології виявлення вторгнень; проблеми безпеки клієнтів; експериментальна оцінка маршрутизації для грід і хмари; покращення симулятора для перевірки підходу до екологічних хмарних обчислень.

З початку зауважимо, що, відповідно до канонів філософської науки, захист інформації в загальному випадку слід характеризувати тими ж самими категоріями, як інші види продуктивної діяльності людини [111].

Це дає логічні підстави для використання кращих науково-практичних напрацювань у сфері ефективного менеджменту підприємницької діяльності (бізнеса) для формування загальних підходів до раціонального управління системою забезпечення КтГ, які мають бути доповнені методами і моделями, що специфічні для галузі, яка досліджується.

У класичній роботі Роберта Ентоні [112] для опису структури ефективного менеджменту підприємства запропоновано організаційну модель, що отримала назву трикутник Ентоні (рис. 2.8), яку згодом почали використовувати також для визначення завдань інформаційних систем [113].

У [112] пропонується розрізняти такі категорії (рівні) менеджменту:

1. **Стратегічне планування** (*strategic planning*) – це процес ухвалення рішень щодо цілей підприємства, змін у цих цілях, ресурсів, які використовуються для досягнення цих цілей, і політики, яка має керувати придбанням, використанням і розпорядженням цими ресурсами. Даній категорії відповідає стратегічний рівень управління.

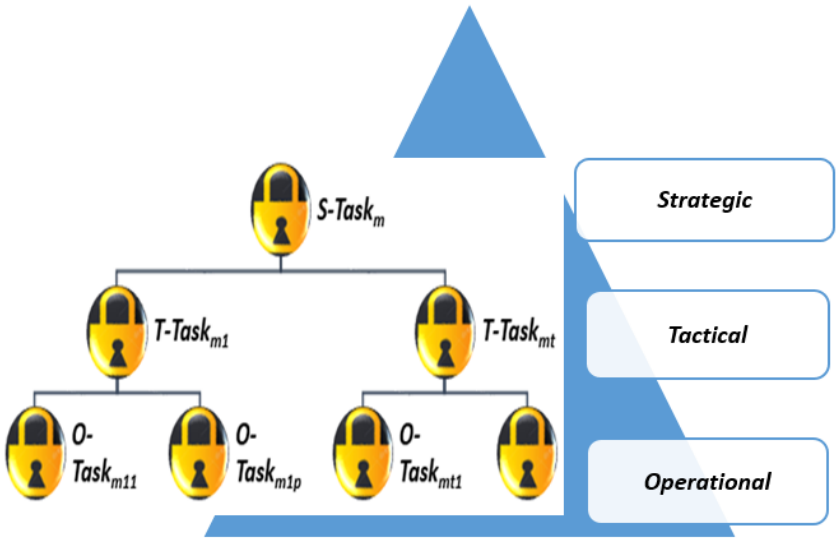

Рисунок 2.8 – Трикутник Ентоні (Anthony triangle)

2. **Управлінський контроль** (management control) – це процес, завдяки якому керівники переконуються, що ресурси використовуються ефективно та результативно для досягнення цілей організації. Даній категорії відповідає так званий тактичний рівень управління.

3. **Операційний контроль** (*operational control*) – це процес забезпечення ефективного та результативного виконання конкретних завдань. Він реалізується на операційному рівні управління.

Для кращого розуміння змісту поняття *Operational control* (англ.) звернемо увагу, що цьому поняттю в німецькій мові відповідає термін *Betriebskontrolle (нім.)* – виробничий контроль, тому в українському перекладі англомовному терміну надаємо перевагу поняттю «операційний» контроль (прикметник, пов'язаний із предметом контролю, – операціями) замість «оперативний» контроль (прикметник асоціюється з часом виконання контролю).

Загалом основна різниця між управлінським контролем і операційним контролем обумовлена [112] відмінністю між діяльністю, яку називають управлінням, і діями, пов’язаними з виконанням визначених завдань. Зокрема, можна стверджувати, що операційний контроль має відношення до технологій і процедур, тоді як управлінський контроль переважно стосується персоналу.

Крім того, операційний контроль не потребує прийняття значної кількості рішень, оскільки завдання, цілі та ресурси, потрібні для ефективного функціонування організації, мають бути детально визначені підчас стратегічного планування та управлінського контролю.

Модель трикутника Ентоні, зображена на рис. 2.8, відрізняється від поширених її зображень наявністю суттєвого, на нашу думку, доповнення, а саме: кожне завдання на рівні стратегічного управління $S\_Task_m,\ m = \overline{1, N_s}$ породжує на тактичному та операційному рівнях пов'язані з ним безлічі завдань $\{T\_Task_{m1},\ \ldots,\ T\_Task_{mp}\}$ та $\{O\_Task_{m11},\ \ldots,\ O\_Task_{mtq}\}$ відповідно.

Зважаючи на багаторічну всебічну апробацію моделі трикутника Ентоні, пропонується розглянути механізм її застосування у випадку управління заходами щодо забезпечення КтГ інформаційних систем критичної інфраструктури.

За аналогією з трикутником Ентоні з метою підвищення ефективності управлінської діяльності уявляється доцільним поділяти заходи щодо підтримки, розвитку, вдосконалення або відновлення рівня КтГ інформаційних систем на декілька рівнів (таблиця 2.1), виходячи з: характеристик вирішуваних задач, категорії та компетенцій персоналу, що безпосередньо відповідає та дбає про вирішення проблем КтГ, розміру фінансових, матеріальних і часових витрат на їх реалізацію.

Базові завдання різних рівнів управління в таблиці 2.1 визначені на основі підходів НАТО до кіберзахисту [114] і напрацювань попередніх розділів.

Таблиця 2.1 – Базові завдання різних рівнів управління безпекою

Рівень управління Керуючі особи	Базові завдання	Витрати	Термін
Стратегічний Власники АУІС	1. Схвалення політики безпеки, визначення її цілей і завдань, фінансових, матеріальних і людських ресурсів. 2. Нормативне регулювання кібербезпеки. 3. Виділення ресурсів для ліквідації наслідків кіберінцидентів. 4. Визначення порядку роботи у умовах надзвичайного стану. 5. Організація навчання і виховання персоналу, його мотивація. 6. Забезпечення фізичної безпеки	Великі (придбання основних засобів + навчання і утримання персоналу + роботи зовнішніх виконавців)	Тривалий
Тактичний Адміністратори безпеки	1. Моніторинг і оцінка поточного стану загроз для системи. 2. Організація оцінки і аудиту безпеки системи. 3. Визначення повноважень і управління системою розмежування доступу	Середні (утримання)	Середній

Продовження таблиці 2.1

	4. Моніторинг рівня підготовки та навчання операторів безпеки і користувачів системи. 5. Планування роботи в умовах надзвичайного стану. 6. Управління відновлювальними заходами		
Операційний Оператори безпеки	1. Керування, апаратними и програмними засобами захисту, включаючи їх інсталяцію, налаштування і обслуговування. 2. Проведення відновлювальних робіт після інцидентів	Середні (утримання+ витратні матеріали)	Короткий

2.2.2 Ключові показники ефективності управлінських дій щодо кібербезпеки

У загальному випадку, без орієнтації на конкретну сферу робіт організації, для оцінки ефективності управлінських дій, згідно з [115], мають бути сформувати ключові показники ефективності (key performance indicators – KPI), застосування яких дозволяє здійснити аналіз та вимірювання успішності обраних заходів на шляху досягнення очікуваного результату. Наявність надійних KPI має вирішальне значення для компаній, які впроваджують системи керування ефективністю.

В ролі KPI для систем управління КтГ пропонується обрати впорядковані функціональні профілі захищеності, які можуть динамічно змінюватися.

З початку для формалізації деяких процедур введемо оператор відношення на множині $\{K_1, \dots, K_M\}$ критеріїв захищеності комп'ютерних систем від несанкціонованого доступу [116].

Зауваження: далі вважаємо, що у разі незастосування деякого критерія K_j для опису захищеності конкретної АУІС його поточне значення дорівнює $\emptyset$ – «пустому» елементу, і це найнижчий рівень безпеки порівняно з будь-яким іншим значенням даного критерія.

Два значення $K_j(1)$ та $K_j(2)$ кількісного або якісного критерія K_j для $\forall\, j = \overline{1, M}$ будемо називати такими, що пов'язані співвідношенням «більшості»: $K_j(1) \prec K_j(2)$, якщо друге значення критерія відповідає вищому рівню безпеки. Наприклад, у випадку наведених у [117] прикладів профілів захищеності

$$K_1(1) = \{\text{КА} = 1\}, K_1(2) = \{\text{КА} = 3\} \text{ і } K_1(3) = \{\emptyset\}$$

має місце $K_1(3) \prec K_1(1), K_1(3) \prec K_1(2), K_1(1) \prec K_1(2)$.

Далі вважаємо, що функціональний профіль захищеності АУІС [118] є кортежем $\mathcal{K}(t) = \langle K_1(t_1), \dots, K_M(t_M) \rangle$, що включає всі критерії захищеності КС від несанкціонованого доступу з їх множині $\{K_1, \dots, K_M\}$.

Визначення 1. Будемо вважати, що два профіля захищеності пов'язані співвідношенням $\mathcal{K}(1) \prec \mathcal{K}(2)$, якщо має місце нерівність

$$\left|\left\{(\mu_1, \dots, \mu_p) \colon K_{\mu j}(2) \prec K_{\mu j}(1)\ \forall j = \overline{1, p}\right\}\right| < \left|\left\{(\nu_1, \dots, \nu_q) \colon K_{\nu j}(1) \prec K_{\nu j}(2)\ \forall j = \overline{1, q}\right\}\right|.$$

Визначення 2. Два профіля будемо називати такими, що практично не розрізняються ($\mathcal{K}(1) \cong \mathcal{K}(2)$), якщо має місце

$$\left|\left\{\left(\mu_1,\dots,\mu_p\right)\colon K_{\mu j}(2) \prec K_{\mu j}(1)\ \forall j=\overline{1,p}\right\}\right| = \left|\left\{\left(\nu_1,\dots,\nu_q\right)\colon K_{\nu j}(1) \prec K_{\nu j}(2)\ \forall j=\overline{1,q}\right\}\right|.$$

Побудоване у такий спосіб бінарне відношення не є відношенням еквівалентності [119], воно рефлексивно і симетрично, але не є транзитивним. Щодо невиконання властивості транзитивності достатньо розглянути такий приклад: нехай $\mathcal{K}(1)=\langle 1,2,1,2\rangle,\ \mathcal{K}(2)=\langle 2,1,2,1\rangle, \mathcal{K}(3)=\langle 1,3,2,1\rangle$. Згідно з (2), маємо $\mathcal{K}(1)=\mathcal{K}(2),\ \mathcal{K}(2)=\mathcal{K}(3)$, водночас, згідно з визначенням 1, маємо $\mathcal{K}(1)\prec\mathcal{K}(3)$. Інтуїтивно зрозуміло, що в запропонованій трійці останній гіпотетичний профіль є в певному сенсі слушним.

Звернемо увагу, що з визначень 1 та 2 слідує, що $p=q$ та

$$p+q=2\cdot p=M-s,$$

де s – кількість критеріїв, які одночасно не використовуються в профілях захищеності $\mathcal{K}(1)$ та $\mathcal{K}(2)$.

2.2.3 Культура кібербезпеки організації як складова системи управління безпекою

Для побудови управління безпекою вбачається доречним здійснити аналіз вихідних даних для реалізації проєкту системи кіберзахисту та прийняття рішень щодо поточних дій у різних умовах.

Спочатку звернемо увагу на те, що, згідно з визначенням НД ТЗІ [120], комп’ютерна система є сукупністю програмно-апаратних засобів, подана для її оцінки (target of evaluation). Саме цей об’єкт оцінки після випробувань характеризується профілем захищеності.

Водночас необхідні підприємствам інформаційні сервіси надаються різновидами автоматизованих систем – інформаційними,

телекомунікаційними тощо, які обов’язково включають персонал цих систем. Зрозуміло, що виконання базових завдань КтГ на всіх рівнях управління (таблиця 2.1) потребує наявності у персоналу певних знань, умінь, навичок і якостей [121].

Відповідна сукупність характеристик у [122] визначена як культура кібербезпеки організації (Cyber Security Culture in organisations – CSC), яка стосується знань, переконань, уявлень, ставлень, припущень, норм і цінностей людей щодо кібербезпеки та того, як вони проявляються в людях. поводження з інформаційними технологіями. Зазначимо, що високий рівень безпеки, заданий профілем захисту, не гарантує безпеки реальної АУІС, якщо рівень CSC є низьким [123].

Отже, в рамках комплексного підходу до забезпечення ГіК АС реалізація ефективного управління потребує врахування на стратегічному та тактичному рівнях поточного стану та динаміки змін рівня CSC.

Сформулювати інтегральну характеристику CSC у загальному випадку дуже складно, тому пропонується використати евристичний підхід щодо оцінки досягнення необхідного рівня CSC на основі ідеї тесту Тюрінга [124], що теоретично застосовний для відрізнення штучного інтелекту від природного.

Згаданий тест можна інтерпретувати таким чином: експерт взаємодіє з комп'ютером та людиною. Використовуючи відповіді на запитання, експерт повинен встановити, з ким або з чим він контактує, завдання штучного інтелекту створити у експерта враження спілкування з природним інтелектом.

У досліджуваній ситуації маємо зворотний випадок: діяльність людини (оператора безпеки, користувача) в типових ситуаціях має повністю відповідати вимогам затверджених інструкцій, ризик помилкових дії має бути мінімальним. Виходячи з цього, ключовим завданням оперативного та тактичного рівнів управління вбачається підвищення та підтримання CSC в організації на рівні, що адекватний ступеню надійності застосованих

інформаційних технологій і виключає можливість прояву в АУІС такого явища, яке отримало назву «людський фактор» [125].

Підвищенню рівня CSC має сприяти проведення на тактичному рівні навчань, тренінгів та поточного контролю набутих навичок [126, 127]. При цьому ефективним інструментом для рейтингового контролю знань та умінь особи, що навчається, має бути шкала оцінювання Європейської кредитно-трансферної системи – ECTS [128].

Нагадаємо, що ця шкала оцінювання включає п’ять позитивних рівнів якості підготовки майбутнього фахівця, а саме: найвищий – A (незначна кількість помилок), середній – B, C, задовільний – D, найнижчий – E (задовольняє мінімальним критеріям), а також негативний – F та FX.

На прикладі моделі необхідного рівня CSC в організації (таблиця 2.2) можливо з’ясувати, як можна керувати безпекою персоналу організації, використовуючи визначення категорії критичності ОКІ [129], індикатор, що характеризує вірогідність реалізації кібератак, та середню оцінку рівня культури кібербезпеки в організації.

Таблиця 2.2 – Модель достатності рівня CSC для різних категорій критичності ОКІ

Категорії критичності ОКІ	M_{ects} середня оцінка рівня CSC для стану агресивності зовнішнього середовища S_{ex}			
	$S_{ex} = 0/T_{ex}\uparrow$	$S_{ex} = 1/T_{ex}\uparrow$	$S_{ex} = 2/T_{ex}\uparrow$	$S_{ex} = 3/T_{ex}\uparrow$
IV – необхідні об’єкти	E	D	C	B
III – важливі об’єкти	D	C	B	A

Продовження таблиці 2.2

II – життєво важливі об'єкти	C/B	B/A	A	A
I – особливо важливі об'єкти	B/A	A	A	A

У таблиці 2.2 застосовані такі позначення:

S_{ex} – індикатор, що характеризує вірогідність реалізації кібератак щодо об'єкта інформаційної діяльності, який доречно називати станом агресивності зовнішнього середовища. В [110] у рамках аналізу мотивів, цілей і завдань вторгнень із різних позицій відмічено, що знання цих факторів покращує ситуацію із запобіганням можливим наслідкам.

У нашому випадку, з точки зору впровадження запобіжних заходів, акцент управлінської реакції дещо інший. Постає питання: чим поточна ситуація в кіберпросторі відрізняється від звичайного становища та як, використовуючи людський потенціал, підвищити резистентність АУІС.

Зрозуміло, що визначення відповідних станів потребує глобального аналізу політичних, військових, економічних та інших цілей і прагнень окремих держав і їх альянсів, або злочинних угруповань. Це питання становить окремий науковий інтерес і потребує окремого опрацювання, а в рамках цього дослідження виділяємо такі ситуації:

– звичайний стан зовнішнього середовища ($S_{ex} = 0$);

– підвищений рівень небезпеки ($S_{ex} = 1$);

– високий рівень небезпеки ($S_{ex} = 2$);

– дуже високий рівень небезпеки ($S_{ex} = 3$).

Зазначимо, що характеристика S_{ex} пов'язана з величиною T_{ex} – трендом кількості кібератак, що спостерігаються в кіберпросторі за визначений проміжок часу: якщо кількість кібератак зростає, то маємо $T_{ex} > 0$, у випадку

не збільшення кількості кібератак $T_{ex} \leq 0$. При цьому $|T_{ex}|$ – абсолютна величина тренду є різницею кількості кібератак в зовнішньому середовищі для двох послідовних проміжків часу (тиждень, декада, місяць).

Суттєве зростання цього тренду $(T_{ex}\uparrow)$ протягом певного часу може свідчити про необхідність визнання нового стану агресивності середовища. І навпаки, суттєве падіння кількості кібератак, що спостерігаються, може бути підставою для повернення в визначення характеристики CSC до попереднього стану S_{ex}.

Прийняття на стратегічному рівні управління рішення про встановлення вищого стану агресивності середовища S_{ex} повинно невідкладно активувати механізми підвищення рівня безпеки системи за допомогою організаційних заходів та додаткових програмно-технічних засобів (таблиця 2.1, колонка «Базові завдання», пп. 4, 5).

Зокрема, організаційні заходи можуть передбачати роботу посилених чергових змін, дострокову зміну ключів і паролів, звуження повноважень користувачів у системі розмежування доступу і, головне, – цілеспрямовану роботу з персоналом, що впливає на рівень КтГ системи в плані підвищення його професіоналізму і дисципліни (показники: M_{ects} – середня поточна рейтингова оцінка, T_{hr} – тренд показника CSC, що відображає зміни рівня професійної підготовки і дотримання норм (дисципліни) кібербезпеки).

Слід звернути увагу, що навіть в умовах звичайної обстановки показники M_{ects} та T_{hr} можуть суттєво погіршуватися внаслідок [111] значних змін у організаційній структурі підприємства, неефективної мотиваційної політики керівництва, прорахунків у кадровій роботі, плинності персоналу та впливу зовнішніх факторів. Тому важливим завданням тактичного рівня управління (таблиця 2.1, колонка «Базові завдання», пп. 4, 5) є моніторинг рівня підготовки та навчання персоналу.

В запропонованій моделі характеристика критичності конкретного об’єкта інформаційної діяльності, якщо він не підпадає під законодавчо встановлену класифікацію [129], має бути визначена апріорно з урахуванням

значущості сфери суспільного виробництва, можливої шкоди в разі зниження або втрати гарантоздатності системи (недоступності її сервісів), руйнування інформаційних ресурсів і програмних систем, втраченої вигоди та витрат на проведення відновлювальних робіт.

2.2.4 Динамічна модель управління безпекою АУІС

На підставі викладеного щодо зв'язку показників CSC із рівнем КтГ АУІС уявляється доцільним функціональний профіль захищеності, який перевірений підчас її оцінки та поданий в вигляді кортежу $\mathcal{K}(t) = \langle K_1(t), \dots, K_M(t) \rangle$, доповнити ще одним обов'язковим критерієм $K_{M+1}(t)$ – рівнем культури кібербезпеки персоналу CSC, який приймає значення з множини $\{E.D, C, B, A\}$, виходячи з моделі, заданої таблицею 2.2, та пояснень до неї.

У такий спосіб, додатковий критерій може приймати такі значення:

$$K_{M+1}(1) = \{CSC = E\}, K_{M+1}(2) = \{CSC = D\}, \dots, K_{M+1}(5) = \{CSC = A\},$$

при цьому $K_{M+1}(1) \prec K_{M+1}(2) \prec K_{M+1}(3) \prec K_{M+1}(4) \prec K_{M+1}(5)$.

Важлива умова: в профілі захищеності для АУІС цей критерій ніколи не може бути «пустим»:

$$K_{M+1} \neq \{\emptyset\}.$$

Це означає, що формування профілю захищеності АУІС організації має починатися з відповіді на питання: якому рівню CSC має відповідати персонал безпеки і користувачі системи?

Далі, використовуючи задану визначеннями 1 та 2 часткову впорядкованість на множині різних функціональних профілів захищеності та лексикографічний порядок, перенумеруємо всі можливі профілі захищеності в напряму їх підвищення вимог до захисту від 0 (для пустого профіля) до N_{max}, що відповідає найвищому рівню безпеки з максимальним рівнем гарантій.

До початку створення або модернізації системи безпеки мають бути визначені параметри категорії критичності (КК) об'єкта, тренд T_{ex}, стан агресивності середовища S_{ex}, необхідний рівень CSC в організації та, виходячи з наявних фінансових та матеріальних ресурсів, початковий профіль захищеності (в таблиці 2.3 профіль визначено умовно).

Виходячи з визначених параметрів, у процесі управління вживаються заходи щодо корегування профілю захисту та підвищення рівня CSC.

У інтервалі часу (T_0, T_3), виходячи з постійного зростання кількості кібератак ($T_{ex}\uparrow$), на систему корегуються параметри S_{ex}, M_{ects} та профіль захищеності, вживаються заходи щодо посилення безпеки, включаючи проведення інструктажів і тренінгів персоналу. На цьому здійснюється підрахунок поточних витрат на посилення КтГ, включаючи витрати на навчання і мотивацію персоналу безпеки.

Інтервал часу (T_3, T_4) в таблиці 2.3 і на діаграмі рис. 2.9 відповідає відновленню системи після кібератаки. Цей момент часу характеризується визначенням нанесених збитків, порівняння їх з попередніми витратами на покращення безпеки та прийняттям рішення щодо подальшого посилення заходів з безпеки. Зважаючи на те, що в цей період система є найбільш вразливою до нових уражень, за рішенням стратегічного рівня управлення категорію критичності організації доцільно тимчасово підвищувати на одну ступень.

Таблиця 2.3 – Динамічна модель управління безпекою АУІС

	ДИНАМІКА ПОДІЙ ЗА ЧАСОМ							
	до T_0	$T_0 \ldots T_1$	$T_1 \ldots T_2$	$T_2 \ldots T_3$	$T_3 \ldots T_4$	$T_4 \ldots T_5$	$T_5 \ldots T_6$	$T_6 \ldots T_\infty$
STRAT.	Завдання + забезпечення				Відновлення стану	Завдання + забезпечення		
TAKT.	Управління + навчання					Управління + навчання		
OPER.	Керування засобами					Керування засобами		
T_{ex}	=	↑	↑	↑	↑	=	=	=
S_{ex}	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**0**
KK	IV	IV	IV	IV	III	IV	IV	IV
M_{ects}	***E***	***E***	***E***	***D***	***D***	***D***	***D***	***D***
$K_1(T)$	**1**	**1**	**1**	**3**	**3**	**3**	**3**	**3**
$K_2(T)$	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**
$K_3(T)$	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**2**
$K_4(T)$	∅	**1**	**1**	**1**	**1**	**1**	**2**	**2**
$K_5(T)$	∅	∅	∅	∅	∅	∅	**1**	**1**

В інтервалі часу (T_4, T_6) реалізується прийняте рішення щодо подальшого посилення заходів з безпеки. Звернемо увагу, що на тактичному рівні управління менеджмент безпеки намагається підтримувати рівень CSS у рамках досягнутого значення параметра M_{ects}.

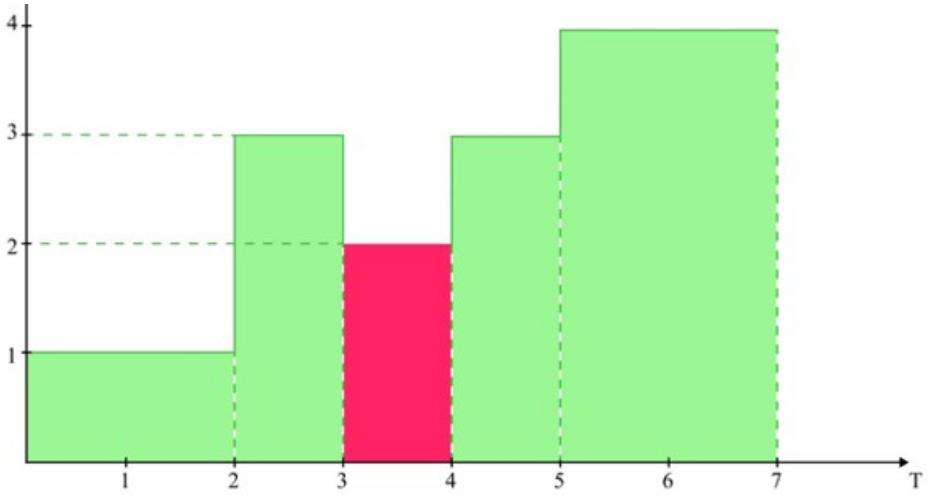

Рисунок 2.9 – Діаграма змін станів системи безпеки у часі

Співвідношення збитків що виникли внаслідок атак і сумарних витрат на покращення безпеки за суттю є показником ефективності обраних управлінських рішень. Виходячи з цього співвідношення, на підставі статистики за певною галуззю суспільної діяльності (промисловість, енергетика, охорона навколишнього середовища тощо) має бути визначений перший KPI_1 – ключовий показник ефективності управлінської діяльності організації в сфері забезпечення КтГ.

Як другого ключового показника KPI_2 доцільно обрати T_{hr} – тренд змін рівня CSC організації внаслідок реалізованих на оперативному та тактичному рівнях заходів з навчання, виховання і мотивування персоналу.

2.3. Побудова частково децентралізованої системи розмежування доступу в мережі КЦК

2.3.1 Проблеми ЦСРД і шлях їх розв’язання

Звернемо увагу, що в ролі об’єкта впровадження заходів з кіберзахисту та забезпечення гарантоздатності розглядається мережа корпоративного центру кібербезпеки ОКІ, яка поєднує декілька комерційних переважно

незалежних структур, фактично, рівноправних партнерів, метою співпраці яких в інформаційній сфері є формування виважених управлінських рішень, зокрема, для надійного постачання електроенергії [81, 130].

При цьому власники інформації відповідно до Закону [131] мають право визначати порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації, що може бути обумовлено специфікою способів отримання первинних відомостей та/або методів їх подальшої обробки, власним «ноу-хау» та/або авторським правом на деяку продукцію тощо.

Це потребує нового погляду на теорію і практику побудови систем розмежування доступом до процесів та ресурсів в мережі КЦК енергетичного сектору та загалом ОКІ.

Питанням побудови систем розмежування доступу (СРД) присвячено багато наукових досліджень, зокрема, в [132–134] наведено системний огляд і аналіз побудови існуючих та перспективних моделей, але аспекти їх ефективності щодо забезпечення конфіденційності інформації залишились по за увагою дослідників.

Для реалізації процедури оцінювання ефективності функціонування системи захисту інформації і кібербезпеки об'єктів критичної інформаційної інфраструктури в [135] запропоновані часткові показники ефективності.

В [136] досліджено розширення механізмів контроля доступу в певному класі чутливих інформаційних систем.

Слід зауважити, що вказані дослідження переважно базуються на централізованій системі управління доступом (ЦСРД), коли власник або розпорядник АУІС визначає порядок доступу до інформації та вимоги до архітектури СРД згідно з вимогами нормативних актів та стандартів [74, 137, 138].

На відміну від централізованого підходу до побудови СРД в [139, 140] запропонований інший підхід – децентралізований, що передбачає можливість

делегування частини повноважень від центрального рівня управління системою безпеки іншим її рівням.

При цьому у вказаних дослідженнях розглянуте питання щодо архітектури такої СРД та її побудови. Цей підхід полягає у винесенні складової, що відповідає за прийняття рішень про дозвіл або заборону доступу суб'єктів до об'єктів, поза робочою станцією, на якій проводиться розмежування доступу. Ця складова розміщується на іншій робочій станції і може використовуватися для розмежування доступу на кількох машинах. Такий підхід названо «децентралізацію системи розмежування доступу», зважаючи на те, що система поділяється на кілька складових, які встановлені на різних робочих станціях.

Нами пропонується інше рішення щодо побудови часткової децентралізації системи розмежування доступу, яке засноване на доказовому підході до гарантій інформаційної безпеки [140,141].

Як було вище зазначено, комплекси кіберзахисту сучасних інформаційних систем (ІС) переважно будуються за принципом централізованого управління безпекою, який передбачає наявність в системі єдиного менеджменту, що скеровується власником або розпорядником системи. Надалі згадуючи про власника системи будемо розуміти, що відповідні положення стосуються також її розпорядника. Відповідна онтологічна модель безпеки зображена на рис. 2.10.

Ця модель включає умовно єдиного адміністратора А, який формує та реалізує політику інформаційної безпеки (ПІБ), що затверджується керівництвом організації – власником системи, а також налаштовує компоненти системи кіберзахисту і контролює виконання заходів, які передбачені ПІБ, та іншими нормативними документами [74]. Користувачі інформаційної системи $U_1, U_2, \dots, U_N$, виконуючи правила, визначені ПІБ, взаємодіють з ІС для отримання доступу до інформаційних ресурсів $IR_1, IR_2, \dots, IR_M$, які необхідні для розв’язку певних задач. За звичаєм,

користувачі не беруть участі у формуванні ПІБ та налаштуванні засобів захисту, включаючи систему розмежування доступу.

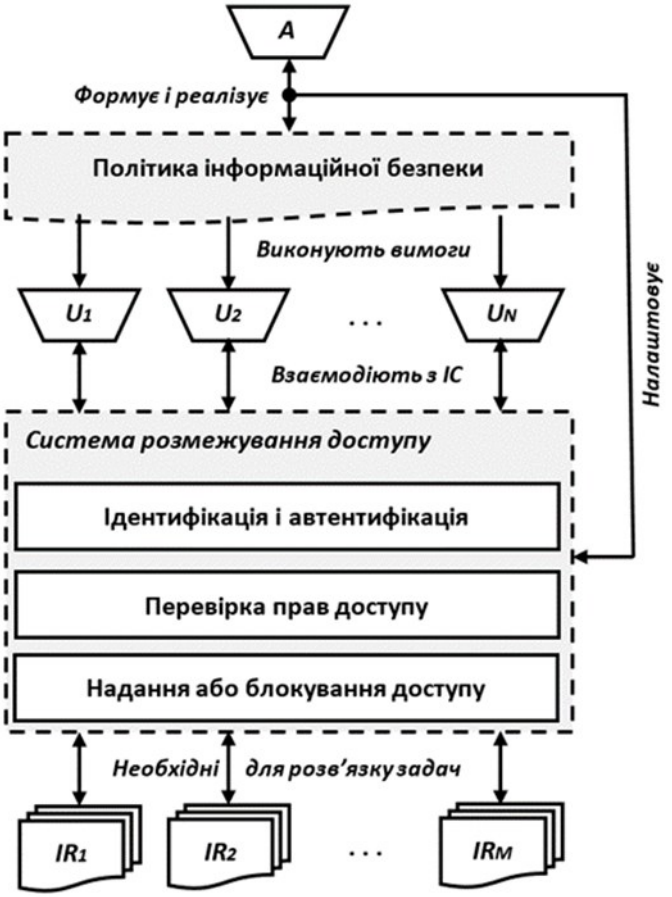

Рисунок 2.10 – Онтологічна модель централізованої системи безпеки в захищених ІС

Перевагами такого підходу до побудови системи управління інформаційною безпекою є:

– уніфікація вимог із захисту для всіх складових системи;

– зменшення ризику утворення відносно слабких ланок або вразливостей;

– єдина вертикаль управління і контролю розмежування доступу до ресурсів інформаційної системи.

Водночас цей підхід не вільний від деяких недоліків, а саме:

– потенційно адміністратор системи безпеки завдяки занадто великим повноваженням може особисто отримати доступ до змісту конфіденційних

інформаційних ресурсів або без достатніх підстав надати доступ певному користувачу системи;

– у випадку подолання захисних бар'єрів, наприклад, у разі нештатного функціонування системи захисту, атакуюча сторона може здійснити спробу несанкціонованого доступу до недостатньо захищеного ресурсу;

– існує потенційна небезпека копіювання та несанкціонованого поширення інсайдерами відкритих ресурсів, які створені за кошти власника та користувачів системи або є об'єктом авторського права.

Також слід зазначити що в інформаційних системах, що об'єднують декілька різних за підпорядкованістю корпоративних підсистем, у загальному випадку користувач (user) може виступати в одній або двох іпостасях: як власних (owner) інформаційного ресурсу і як споживач ресурсу (client / utilizer).

При цьому, зважаючи на, можливо, чутливий характер способу або методу отримання або збирання (отримання) первісних відомостей, що утворюють інформаційний ресурс, його власник (owner) може мати законні підстави для погодження або обмеження доступу споживачів (clients) до нього, а також може надавати пропозиції щодо ПІБ у системи в цілому та здійснювати адміністрування безпеки власного сегмента та контроль її стану.

Подібна ситуація, зокрема, може спостерігатися в мережі ситуаційних центрів державних органів, а також мережі КЦК енергетичного сектору.

Модель частково децентралізованої системи безпеки в захищеної ІС, яка враховує відповідні недоліки централізованої системи, зображена на рис. 2.11.

У наведеній моделі ключову роль в організації та забезпеченні безпеки, як і раніше, відіграє менеджмент центрального сегмента мережі, але на відміну від попереднього випадка власник (owner) U_i множини інформаційних ресурсів $\Omega_i = \{IR_{i1}, IR_{i2}, \dots, IR_{ip}\}$ набувають повноважень погоджувати доступ до них інших споживачів інформаційної системи та надавати пропозиції щодо формування ПІБ.

Вочевидь маємо

$$\cup\Omega_i = \{IR_1, IR_2, \dots, IR_M\}, \text{де } \Omega_i \cap \Omega_j = \emptyset \text{ для } i \neq j.$$

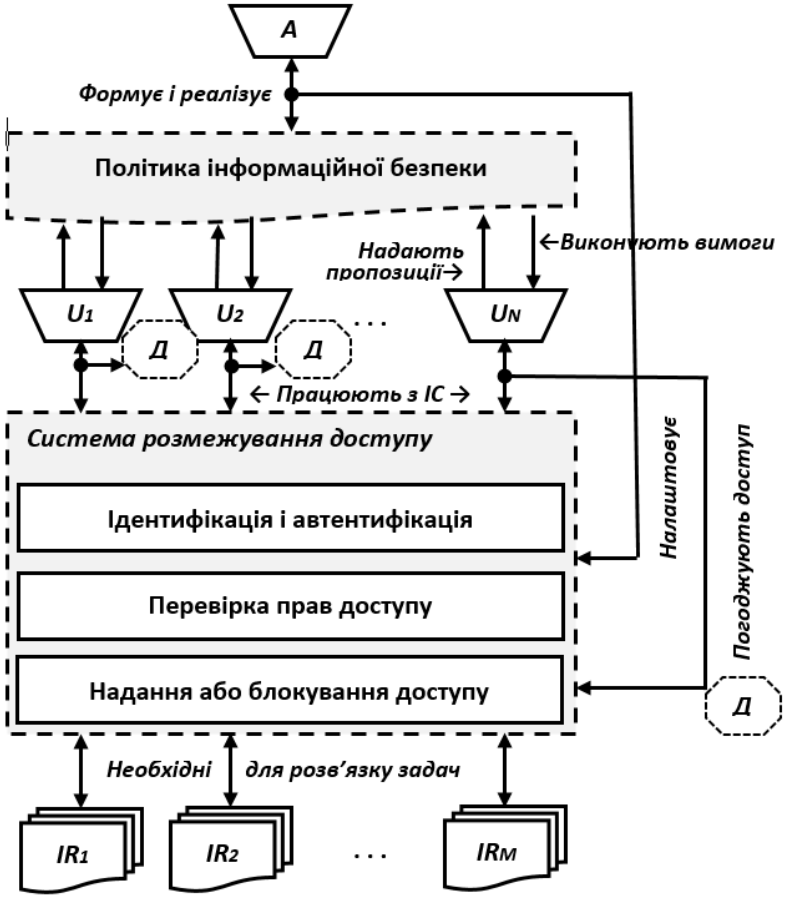

Рисунок 2.11 – Онтологічна модель частково децентралізованої СРД

Назвемо дескриптором приналежності даних їх власникам дворядкову таблицю, верхній рядок якої є унікальним номером користувача АУІС, а нижній рядок – множиною відповідних йому інформаційних ресурсів:

$$Ds = \begin{pmatrix} 1 & 2 & \dots & N \\ \Omega_1 & \Omega_2 & \dots & \Omega_N \end{pmatrix}.$$

На основі дескриптора належності менеджмент безпеки має формувати для комбінованої матрично-мандатної системи розмежування доступу матриці доступу та маркери володільців папок і файлів даних, що мають містити унікальні номери володільця ресурсу та код конфіденційності ресурсу – КК.

Наприклад, КК=0 може свідчити, що ресурс потенційно може бути доступним будь-якому ідентифікованому та автентифікованому користувачу системи, КК=1 може свідчити про певні обмеження щодо використання ресурсу тощо.

Ідея побудови механізму розмежування доступу базується на застосуванні криптографічних перетворень інформації. Для цього кожен файл, що передається в єдину базу даних інформаційної системи, шифрується за допомогою схваленого блокового криптографічного алгоритму $E_k(M)$ у режимі ECB (Electronic Codebook) [142] із використанням генерованого власником файлу ключем $\bar{k}$.

Ключ безпечно зберігається власником файлу і ніколи не циркулює в мережі у відкритому вигляді. Оскільки для розшифрування файлів потрібен ключ, тому необхідно побудувати процедура розподілу секрету [142, 143] між зацікавленими сторонами інформаційної системи так, щоб відновлення ключу було б можливим тільки за певних умов.

Далі розглянемо математичні основи запропонованого механізму розподілу секрету [200].

2.3.2 Математичні засади процедури розподілу секрету

Сформулюємо деякі математичні положення, які необхідні для обґрунтування пропонованої процедури розподілу секрету.

Твердження 1. Нехай задана система лінійних рівнянь

$$\begin{cases} \bar{\beta}_1 = \bar{k} \oplus \bar{\alpha}_1 \\ \quad \dots \dots \dots \\ \bar{\beta}_s = \bar{k} \oplus \bar{\alpha}_s \end{cases}, \tag{2.3}$$

де двійкові вектори $\bar{\alpha}_i, \bar{\beta}_i, \bar{k} \in V_2^n$, $i = \overline{1,s}$, V_2^n – векторний простір розмірності n над полем з двох елементів. Тут і далі операція $\oplus$ означає покоординатне додавання векторів за модулем 2 (виключне «або»). Якщо має місце рівність

$$\bar{\alpha}_1 \oplus \ldots \oplus \bar{\alpha}_s = \bar{0}\,, \tag{2.4}$$

де $\bar{0}$ – вектор, усі координати якого дорівнюють нулю та виконується умова

$$\bar{\alpha}_{i_1} \oplus \ldots \oplus \bar{\alpha}_{i_m} \neq \bar{0}\,, \tag{2.5}$$

де $m < s$ і елементи набора індексів $\{i_1, \ldots, i_m\}$ попарно не співпадають, тоді в разі непарного s вектор $\bar{k}$ однозначно обчислюється за виразом

$$\bar{k} = \bar{\beta}_1 \oplus \ldots \oplus \bar{\beta}_s. \tag{2.6}$$

У випадку парного s результат складання в (2.4) дорівнює $\bar{0}$.

Висновок твердження нескладно довести шляхом додавання рівнянь у системі (2.3).

Вектори з множини $\{\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_s\}$ будемо називати масками секретного параметра (ключа) $\bar{k}$.

Твердження 2. Якщо в системі рівнянь (2.3) компоненти векторів $\bar{\alpha}_i = (\alpha_{i1}, \ldots, \alpha_{in}), i = \overline{1,s}$ мають випадковий рівномірний розподіл, тобто

$$P(\alpha_{ij} = 1) = P(\alpha_{ij} = 0) = 0.5, \text{для } \forall\, i, j, \tag{2.7}$$

та не залежать від $\bar{k}$, то компоненти векторів $\bar{\beta}_i = (\beta_{i1}, \dots, \beta_{in}), i = \overline{1,s}$ також мають випадковий рівномірний розподіл

$$P(\beta_{ij} = 1) = P(\beta_{ij} = 0) = 0.5, \text{для } \forall\, i, j.$$

Дійсно, ймовірність того, що деяка компонента $\beta_{ij} = 1$ дорівнює

$$P(\beta_{ij} = 1) = 1 - P(\beta_{ij} = 0) = P(k_j \oplus \alpha_{ij}) = 1 =$$

$$P(\alpha_{ij} = 0) \cdot P(k_j = 1) + P(\alpha_{ij} = 1) \cdot P(k_j = 0) =$$

$$0.5 \cdot P(k_j = 1) + 0.5 \cdot P(k_j = 0) = 0.5 \cdot \Big(P(k_j = 1) + P(k_j = 0)\Big) = 0.5.$$

Твердження 3. Якщо в умовах тверджень 1 і 2 двійкові вектори $\{\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_s\}$ обираються рівноймовірно випадковим чином з векторного простору V_2^n, тобто

$$P(\bar{\alpha}_i = \bar{\gamma}) = 2^{-n} \text{ для } \forall\, \bar{\gamma} \in V_2^n,\ i = \overline{1,s}, \tag{2.8}$$

тоді кожне рівняння

$$\bar{\beta}_i = \bar{k} \oplus \bar{\alpha}_i, \text{для } \forall i = \overline{1,s} \tag{2.9}$$

задає досконалий шифр, а (2.3) визначає розподіл секретного ключа $\bar{k} \leftrightarrow \{\bar{\beta}_1, \bar{\beta}_2, \dots \bar{\beta}_s\}$ між спільнотою з s користувачів, а (2.6) встановлює правило відновлення секретного ключа.

Нагадаємо, що коли випадкові величини A, K, B приймають значення з V_2^n, а відображення $E(K, A) = B: V_2^n \times V_2^n \to V_2^n$ є бієктивним для будь-якого

фіксованого значення A, тоді $E(K,A)$ згідно з [140] називають досконалим шифром, якщо виконується рівність

$$P(K) = P\left({}^{K}/_{B}\right) \text{ для } \forall\, K.$$

Це означає, що угадування значення секретного K не залежить від того знаємо відповідне йому значення B чи ні.

Зауважимо, що за визначенням умовної ймовірності [144] має місце

$$P(K,B) = P(K)\cdot P\left({}^{B}/_{K}\right) = P(B)\cdot P\left({}^{K}/_{B}\right). \qquad (2.10)$$

Виходячи з (2.9) та (2.10) на підставі підходу, що запропонований у [145], маємо

$$P(K,B) = P(K)\cdot P\left({}^{B}/_{K}\right) = P(K)\cdot P(B \oplus K) = P(K)\cdot P(A) = P(K)\cdot 2^{-n}.$$

З останнього виразу та виходячи з (2.10),

$$P\left({}^{B}/_{K}\right) = {}^{P(K,B)}\Big/_{P(K)} = 2^{-n}.$$

За теоремою Байєса [17] маємо

$$P\left({}^{K}/_{B}\right) = \frac{P(K)\cdot P\left({}^{B}/_{K}\right)}{P(B)} = \frac{P(K)\cdot P\left({}^{B}/_{K}\right)}{\sum P\left(\bar{k}\right)\cdot P\left({}^{B}/_{\bar{k}}\right)} = \frac{P(K)\cdot 2^{-n}}{2^{-n}\cdot \sum P\left(\bar{k}\right)} = P(K).$$

В останньому виразі сума обчислюється за всіма можливими значеннями секретного параметра $\bar{k}$.

Отже, незалежно від розподілу ймовірностей випадкової величини *K* для досконалого шифру виконується умова Шеннона [140].

Водночас слід зазначити, що умова (2.4) певним чином вступає в протиріччя з вимогою незалежного вибору значень масок з генеральної сукупності, оскільки при цьому має місце

$$\bar{\alpha}_1 \oplus \ldots \oplus \bar{\alpha}_{s-1} = \bar{\alpha}_s.$$

Але ця ситуація має компенсуватись надійно безпечним збереженням повного набору масок $\{\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_s\}$.

Крім того, умова (2.5) дещо звужує множину припустимих різних наборів масок $\{\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_s\}$, що має несуттєве значення з точки зору безпеки в разі достатньо великого n. Нескладно бачити, що кількість перевірок N_p умови (2.5) оцінюється як

$$N_p = \sum_{m=2}^{s-1} C_s^m = \sum_{m=0}^{s} C_s^m - C_s^0 - C_s^1 - C_s^s = 2^s - s - 2.$$

Зокрема, для реально застосовних значень s у таблиці 2.4 наведені розрахункові значення N_p.

Таблиця 2.4 – Кількість перевірок N_p умови (2.5)

Покажчик	s=3	s=5	s=7	s=9	$s = 11$
N_p	3	25	119	501	2035
Сеансів ідентифікації	3	10	21	36	55

Зокрема, у випадку довжини $n = 128$ двійкового ключа $\bar{k}$ їх загальна кількість становить $2^{128} \approx 10^{37}$, водночас s=11 число $N_p = 2035 < 10^4$.

Також умову (2.5) можна дещо спростити, застосовуючи умову $\bar{\alpha}_i \neq \bar{0}$, для $\forall i = \overline{1,s}$.

Зауважимо, що в разі збільшення кількості сторін розподілу секрету s швидко зростає кількість сеансів ідентифікації сторін, що збільшує загальний час доступу споживача до необхідного інформаційного ресурсу, а це може суттєво впливати на оперативність реагування інформаційної системи в цілому на надзвичайні ситуації.

2.3.3 Побудова методики розмежування доступу на основі розподілу секрету

Зважаючи на те, що кількість учасників розподілу секрету s має бути непарним числом, з урахуванням складності комунікацій у перевантажених системах та на основі ролей учасників інформаційного обміну пропонується обрати значення $s = 3$.

Доцільно визначити такі ролі: адміністратор безпеки центрального сегмента мережі *A*, власник інформаційного ресурсу *B* та споживач ресурсу *C* (рис. 2.12).

За необхідності для деяких систем кількість різних ролей може бути збільшена до $s = 5$ у разі підключення в державних системах додаткових категорій контролю.

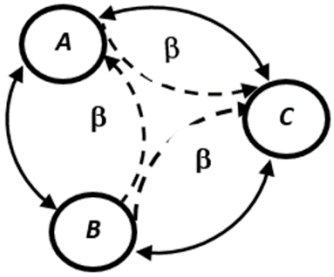

Рисунок 2.12 – Граф взаємодії «адміністратор (A) – власник (B) – споживач (C)»

У пропонованій процедурі для кожного коду конфіденційності $КК_j$ випадковим чином [146] генеруються окремий ключ шифрування файлів і відповідна множина масок ключа $\{\bar{\alpha}_{Aj}, \bar{\alpha}_{Bj}, \bar{\alpha}_{Cj}\}$, що відповідають умовам (2.4), (2.5), (2.7), (2.8).

Сформовані частини секрету $\bar{k}_j \to \{\bar{\beta}_{Aj}, \bar{\beta}_{Bj}, \bar{\beta}_{Cj}\}$ за допомогою стандартних криптографічних протоколів надсилаються власником адміністратору і споживачеві. На рис. 2.12 ця передача показана переривчастими лініями, суцільними лініями наведені запити – відповіді, що надсилаються учасниками інформаційного обміну один одному, зокрема, в рамках протоколів ідентифікації та автентифікації.

Після розподілу частин секрету потреба в їх повному наборі $\{\bar{\beta}_{Aj}, \bar{\beta}_{Bj}, \bar{\beta}_{Cj}\}$ фактично втрачається. З метою забезпечення безпеки запропонованої схеми цей набор необхідно знищити. У разі випадкової втрати окремої частини або підозри на її компрометацію необхідно генерувати та розсилати новий набір частин.

У таблиці 2.5 наведені основні кроки процедури розмежування доступу на основі розподілу секрету. В підсумку виконання процедури споживач отримує можливість відновити ключ $\{\bar{\beta}_{Aj}, \bar{\beta}_{Bj}, \bar{\beta}_{Cj}\} \to \bar{k}_j$ та розшифрувати потрібний ресурс, що відповідає коду конфіденційності $КК = j$.

У підсумку виконання відповідних процедур кожен з користувачів формує власну матрицю доступу $\|\bar{\beta}_{ij}\|$, розмір якої визначається кількістю користувачів в інформаційній системі та числом різних кодів конфіденційності.

Обов’язковою умовою безпеки пропонованої процедури розмежування є знищення у споживача відповідного ключа розшифрування $\bar{k}_j$ та розшифрованих файлів одразу після завершення сеансу обробки.

Зауважимо, що за процедурою адміністратор безпеки ніколи не отримує частини секрете споживача $\bar{\beta}_{Cj}$, що, згідно з (2.5), виключає його можливість розшифрувати відповідні файли та отримати доступ до їх змісту. Оскільки при

цьому шифруванню піддається лише змістовна частина файлів, а його атрибути не змінюються, це не впливає на процедури їх перезапису або архівування. Зазначена властивість пропонованого механізму розмежування доступу також вирішує проблему обстеження інформаційних систем із метою контролю за станом захисту інформації, оскільки особи, які здійснюють аудит системи, не отримують доступу до змісту інформаційних ресурсів.

У рамках виконання макетного проєкту побудови мережі ситуаційних центрів для створення частково децентралізованої СРД як блокового алгоритму шифрування даних було апробовано застосування надійних криптоалгоритмів, що визначені національним стандартом ДСТУ 7624:2014 [147] та міжнародним стандартом AES [148] у програмній реалізації криптографічних модулів із довжинами ключів 256 біт. Обидві реалізації мали достатню швидкодію.

Таблиця 2.5 – Покрокова процедура розмежування доступу

№№	**Дії згідно з ролями**		
	Адміністратор	**Власник**	**Споживач**
1	– Бере участь у процедурах ідентифікації і автентифікації. – Визначає унікальний номер кожного володільця даних.	– Бере участь у процедурах ідентифікації і автентифікації. – Формує реєстр файлів і надає адміністратору. – Визначає код конфіденційності для створюваних файлів. – Формує маркер володільця папок і файлів даних.	– Бере участь у процедурах ідентифікації і автентифікації. – Формує запит на доступ до конкретної категорії файлів власника

Продовження таблиці 2.5

	– Формує на основі реєстрів файлів дескриптор *Ds* – Формує матрицю доступу	– Погоджує запити та дескриптор – Генерує ключі в кількості різних кодів КК	
2	– Отримує частини секрету за допо-могою захищеного протоколу. – Здійснює кори-гування матриці доступу	– Шифрує та передає файли в ІС – Формує маски і частини секрету. – Надсилає частини секрету іншим ролям	– Отримує частини секрету за допомогою захищеного протоколу. – Отримує доступ до змісту зашифрованого ресурсу завдяки наданим частинам секрету
3	– Отримує звіти про знищення частини секрету	– Отримує звіти про знищення частини секрету. – Безпечно зберігає ключи та частини секрету	– Знищує розшиф-рований файл, ключ і частини секрету, що отримані від адміністратора і власника ресурсу. – Інформує про виконання знищення

2.3.4 Висновки до розділу 2

1. У другому розділі побудовано вдосконалену модель центру корпоративного захисту інформації в ІКС-ЕС, яка враховує особливості завдань і виконуваних функцій ОЕС-У та побудовану модель логічних ланцюгів впливу сучасних загроз на погіршення спроможності стійкого функціонування ЕС, які проаналізовані у попередньому розділі.

Модель центру корпоративного захисту складається із двох взаємодіючих складових: моделі логіки функціонування КЦК (бізнес-логіки), поданої в нотації IDEF0 платформи виконання операцій з обробки інцидентів та власно методики опрацювання кіберінцидентів.

Для вказаної моделі запропоновано інструментарій – несуперечливий перелік незалежних функцій, що мають бути реалізовані в сервіс-орієнтованій архітектурі КЦК з метою виконання завдань кібербезпеки та гарантоздатності інформаційної інфраструктури для забезпечення реалізації місії енергосистем – надійного безпечного енергопостачання.

Завдяки компоненті – динамічної моделі управління безпекою інформаційної інфраструктури – вдосконалена модель враховує фактор змін у ландшафті кіберзагроз та надає орієнтири у плані покращення рівня корпоративної кіберкультури.

2. З використанням доказового методу побудови систем захисту вперше запропонована модель децентралізованої системи розмежування доступу в мережі центру кібербезпеки, яка дозволяє безпечно керувати даними різних власників із різними рівнями обмеження доступу. Модель створена з застосуванням вперше запропонованої для цього методики розподілу секретів, що є ключем шифрування даних різних їх власників.

Застосування запропонованої методики дозволяє уникати ситуацій несанкціонованого ознайомлення адміністраторів безпеки з конфіденційними даними користувачів.

Основні результати розділу опубліковані автором у працях [1–6].

РОЗДІЛ 3
МЕТОДИКА РАЦІОНАЛЬНОГО СИНТЕЗУ ПІДСИСТЕМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ІКС-ЕС

3.1 Уразливості шифрування коротких повідомлень у мобільних ІКС ОКІ

3.1.1 Аналіз стану розробок безпеки мобільного доступу до АУІС

Інформаційний обмін в АУІС ОКІ, включаючи комплекси керування виконавчими пристроями і обладнанням енергетичного сектору, системи дистанційного обліку спожитих енергоресурсів, системи оповіщення про надзвичайні ситуації, промислові комп'ютеризовані системи пожежної безпеки, охорони і дистанційного контролю територій та об'єктів, інформаційно-діагностичні системи в технології IoT та інші, часто реалізується шляхом передачі, прийому і обробки відносно коротких повідомлень [66, 198].

Такі повідомлення можуть містити формалізовані команди управління і дані про поточний стан керованих об'єктів, сигнали оповіщення, відомості про підозрілу активність у комп'ютерних мережах або вихідні дані для формування спільних секретів (ключів) у системах кіберзахисту.

Можливо також звернути увагу, що під час виконання службових завдань виникають ситуації, коли критичні дані необхідно передавати та отримувати за допомогою мобільних пристроїв посадових осіб керівного складу підприємств. Переважно це в разі виникнення проблем із службовим зв'язком у місцях перебування топ-менеджменту. У цьому випадку персонал ОКІ буває вимушений для координації дій з ліквідації наслідків надзвичайних ситуацій використовувати незахищені комерційні системи телекомунікацій.

Трагічні події останнього часу на полях битв із окупантами та ліквідації їх варварських атак свідчать про необхідність вирішення подібних проблем із комунікаціями, також і для систем бойового управління силами та засобами,

хоча б на рівні підрозділів з ліквідації надзвичайних ситуацій в енергетиці, які не мають штатних засобів захищеного зв'язку.

Зазначимо, що на поточний час для швидкого обміну відносно короткими повідомленнями в мережах стільникового зв'язку широко використовуються служби коротких повідомлень (Short Message Service – SMS) [150, 151] або додатки на мобільних платформах – месенджери, включаючи поширені Viber, WhatsApp, Signal та інші [152].

Застосування цих механізмів (як позитив) не потребує швидкісних каналів зв'язку або оренди виділених IP-адрес, але (як негатив) стандартні механізми захисту для SMS не передбачені, а особливості технологій забезпечення безпеки месенджерів приховані за завісою комерційного «ноу-хау».

У такий спосіб, постає актуальне питання підвищення кіберзахисту мобільних пристроїв, що взаємодіють з АУІС ОКІ.

Зауважимо, що захищені мобільні інформаційні технології становлять інтерес також для персоналу і клієнтів енергосистем у плані захисту персональних даних, приватної інформації про особисте життя, реквізитів банківських карт тощо.

Актуальність цієї тези підтверджується результатами досліджень використання месенджера WhatsApp [153], на підставі якого можна зробити висновок, що близько 50 % користувачів використовують цей месенджер не для утворення великих чатів, а для спілкування «têt-à-têt».

У переважної більшості наведених випадків існують реальні загрози порушення конфіденційності чутливих даних або їх підробки, несанкціонованої модифікації з метою порушення сталого функціонування відповідних АУІС та нанесення значних збитків або шкоди власнику комп'ютерної системи і навіть державі. Тому існує нагальна потреба аналізу методів протидії загрозам та забезпечення безпеки коротких повідомлень та визначення шляхів її розв'язання.

В науково-практичних публікаціях для забезпечення конфіденційності та цілісності інформації в мережах мобільного доступу запропоновано декілька рішень, на яких зупинимося більш детально.

В рамках проєкту «Defense against cyberattacks using steganogaphy techniques» спеціалістами департаменту наукових досліджень національного університету оборони Кореї проаналізовано [154] побудову захищеної мережі на основі стеганографічного методу приховування інформації на платформах SNS (Social Network Service). Показано, що запропонована модель може бути реалізована в додатку Telegram SNS.

До недоліку методу слід віднести його неефективне витрачання пропускної здатності системи, зважаючи на те, що розмір контейнера має бути достатньо великим, оскільки у випадку його малого розміру порівняно з довжиною повідомлення факт приховування може ефективно виявлятися за допомогою методів математичної статистики.

В [155] запропоновано новий підхід для приховування факту відправлення коротких повідомлень на основі створення секретного IP-каналу. Замість шифрування повідомлення або його вбудовування в мультимедійний контейнер, як у класичній комп'ютерній стеганографії, для приховування секретного повідомлення обробляються всі повідомлення та генерується декілька IP-пакетів різних типів для переносу даних.

Зауважимо, що надійне приховування факту передачі унеможливлює атаку зловмисника, що спрямована на підробку повідомлення. Також відмітимо, що запропонований метод працює виключно у випадку форматів подання у мережах пакетної передачі даних. Сповіщення користувача, зашифровані за допомогою традиційного механізму шифрування, можуть бути передані через SMS, лише якщо зашифроване повідомлення закодовано у текстовій формі.

Згадана проблема узгодження методу захисту коротких повідомлень з форматом подання даних на рівні застосувань розглядається в [156] відносно

служби коротких повідомлень SMS, які використовуються в смарт-мережі енергетики.

Застосування методів симетричної криптографії, на відміну від стеганографічного захисту, дозволяє забезпечити конфіденційність повідомлень без збільшення навантаження на канал зв'язку, оскільки шифроване і відкрите повідомлення мають однакову довжину.

Зокрема, в [157, 158] наведений огляд криптографічних методів забезпечення безпеки SMS і порівняльний аналіз їх швидкодії, включаючи потоковий шифр RC4, стандарти блокового шифрування DES, 3DES і AES.

Зауважимо, що у випадку симетричного шифрування коротких повідомлень швидкість перетворень у певних межах не має суттєвого значення, більшої уваги потребують визначення та оцінка їх криптографічних якостей.

Зокрема, запропонований до використання в [159] алгоритм RC4 має вразливості, які підвищують загрози проведення ефективних криптоаналітичних атак на захищений інформаційний обмін [160].

Також, незважаючи на високий показник швидкодії практичної реалізації, не можна вважати перспективними для захисту коротких повідомлень алгоритм потокового шифрування A5/1, що слідує з результатів його криптоаналізу [161] та дослідження його модифікації [162, 163].

Відмітимо доволі вдалу модифікацію алгоритму A5/1 та високі криптографічні характеристики створеної його основі версії A5/1-128, яка призначена для забезпечення захисту комунікацій пристроїв IoT [164].

Стосовно якостей запропонованих у [165] алгоритмів 3DES і TEA блокового шифруваннях, що реалізують схему Файстеля [142], можливо зазначити, що їх криптографічна стійкість ще відповідає сучасним вимогам.

При цьому, з урахуванням перспектив зростання потужності комп'ютерних систем, які використовуються для реалізації криптоаналітичних атак, довжина ключу 128 біт в алгоритмі TEA викликає певний сумнів щодо доцільності застосування цих у сучасних системах захисту.

Сучасний алгоритм блокового шифрування AES має високі криптографічні якості і швидкодію [142, 148]. Водночас слід звернути увагу на те, що його застосування в режимах ECB (Electronic Code Book) або CBC (Cipher Block Chaining) довжини повідомлення має бути кратної 64 біт. У загальному випадку довільної довжини повідомлення воно потребує розширення,

Саме з метою уникнення вказаної проблеми в [166] запропонована модифікація стандартного AES – алгоритм AESw, що придатний для шифрування повідомлень довжини кратної 32-бітам без розширення даних.

З точки зору безпеки шифрування, в режимі ECB ця модифікація викликає сумнів, зважаючи на те, що максимальне значення порядку будь-якої точки векторного простору суттєво зменшується:

$$\left(AESw(\bar{x})\right)^n = \bar{x}, \qquad \bar{x} \in V_2^{32} \Rightarrow n \leq 2^{32},$$

$$\left(AES(\bar{x})\right)^n = \bar{x}, \qquad \bar{x} \in V_2^{64} \Rightarrow n \leq 2^{64}.$$

Запропонована в [167] для шифрування коротких повідомлень комбінація симетричного шифру Віжинера і криптосистеми з відкритими ключами RSA не містить обґрунтування щодо безпеки її застосування. Більш ефективним уявляється запропонована в [168] побудова шифру багато алфавітної заміни з псевдовипадковою управляючою послідовністю.

Слід мати на увазі, що підчас передачі по каналам зв’язку пакети даних можуть бути піддані атакам, внаслідок чого їх відхилить шифратор, а це може призведе до часткового блокування функцій АУІС. Для уникнення подібної ситуації в [169] запропоновано метод на основі кодів сімейства Ріда-Соломона, який забезпечить доставку коротких важливих повідомлень при дотриманні балансу швидкості обслуговування (speed of service – SOS) і пропускної здатності мережі.

При цьому для забезпечення доставки відповідно до вимог SOS додається мінімальна кількість надлишкових пакетів. За висновками цього дослідження зроблено висновок, що навіть в умовах кібератак важливі повідомлення, такі як сигнал тривоги постачаються своєчасно по захищеній завдяки шифруванню безпровідної мережі.

Асиметричні шифри (криптосистеми з відкритим ключем) використовуються для вирішення різних задач кіберзахисту, а саме: управління сеансовими ключами симетричних криптосистем, автентифікації, формування і перевірки цифрових підписів. При цьому слід згадати, що в асиметричних системах результат шифрування звичайно обчислюється по модулю деякого великого простого числа, тому запис результатів у двійковому вигляді може мати довжину бітового запису цього числа.

Це означає, що довжина результату зашифрування відносно короткого двійкового числа порядку 2^8 за допомогою асиметричної криптосистеми може досягати кількох тисяч бітів,. На практиці для класичних алгоритмів RSA або Диффі-Хеллмана довжина шифротексту може становити від 2048 біт і більше, що встановлює певні обмеження щодо застосування таких систем.

У [170] на основі криптосхеми ЄльГамаля з відкритим ключем запропоноване компактне асиметричне шифрування безпечне щодо атак з обраним шифрованим текстом [171].

Вказана схема шифрування працює в групі G простого порядка q с генератором $g \in G$. Для секретного навмання вибраного елемента $x \in \mathbb{Z}_q$ обчислюється відкритий ключ $y = g^x$. Якщо H – криптографічна стійка хеш-функція, тоді процедура шифрування відкритого повідомлення задається рівнянням

$$c = m \oplus H(y^r), r \in \mathbb{Z}_q.$$

Відмітимо, що в зазначеній схемі випадкове значення r використовується одноразово, після чого знищується, довжина відкритого і шифрованого

повідомлень визначається розміром дайджеста, що утворюється функцією хешування.

Також слід зазначити, що в сучасних умовах для уникнення реалізації в даній схемі атак за методом «грубої сили» порядок випадкового числа, що найменш, має бути

$$r \sim 2^{64} \approx 10^{19}.$$

Згідно з процедурою, отримувачу надсилається кортеж $\langle z, c \rangle$, де $z = g^r$, який розшифровується так:

$$m = c \oplus H(z^x), \text{тому що } z^x = g^{rx} = y^r.$$

Змістовна інформація щодо безпеки застосування асиметричних криптосистем для шифрування відносно коротких повідомлень, за суттю під якими маються на увазі сеансові ключі для симетричних шифрів, надана в [172, 173].

У загальному випадку для безпечного зашифрування будь-якого повідомлення за допомогою асиметричних криптосистем необхідно мати сертифікат відкритого ключа і відповідну організаційну структуру щодо його обслуговування.

Вирішенню вказаної проблеми може сприяти використання методу шифрування, що оснований на ідентифікації користувача [174] – IBE (Identity Based Broadcast Encryption). У [175] запропонована повнофункціональна схема *IBE*, в якій безпека зашифрованого повідомлення в моделі випадкового оракула заснована на обчислювальної складності в задачі Діффі-Хеллмана та використанні білінійних карт між групами. Прикладом такого відображення є спарювання Вейля на еліптичних кривих.

Інша проблема асиметричних шифрів, як відмічено в [176], полягає в площині можливого довготривалого застосування секретного (приватного)

ключа. У випадку компрометації цього ключа розшифрування всіх повідомлень, які зашифровані за допомогою відповідного відкритого ключа та перехоплені зловмисником раніше.

Це стосується також і майбутніх повідомлень, якщо не будуть вжиті заходи щодо зміни ключової пари. Саме тому для підвищення безпеки інформаційного обміну у вказаній статті запропонований протокол, що забезпечує можливість використання пар приватний, – публічний ключ протягом певного короткого терміну.

Загалом, підсумовуючи огляд систем кіберзахисту на мобільних пристроях можливо зробити висновок про недостатню увагу питанням уразливості відповідних криптосистем, що обумовлені особливостями інформаційних потоків. Тому метою цього розділу є дослідження можливості побудови атак на потенційно стійкі криптографічні системи в умовах шифрування коротких повідомлень

Для цього потрібно спочатку уточнити поняття коротке повідомлення.

3.1.2 Статистичний розподіл довжин повідомлень у чатах месенджерів

Поставимо питання: що вважати коротким повідомленням і у чому полягають особливості їхнього захисту в кіберпросторі? Зважаючи на певні обмеження в плані доступу до відомостей про обмін інформацією (трафік) і заходи щодо її захисту в приватних та державних комунікаційних системах, наше дослідження базується виключно на офіційних джерелах та науково-практичних публікаціях.

На поточний час соціальні мережі в Інтернеті дозволяють швидко обмінюватися текстом, зображеннями, аудіо- та відеофайлами.

В кіберпросторі поширюється використання месенджерів, зокрема, WhatsApp, Viber, Telegram, Signal, різними суспільними і професійними групами, включаючи чати підприємств, територіальних громад, державних і комунальних установ, професійних об’єднань тощо.

У чатах, у випадках, що не суперечать законодавству, відбувається голосування з різних питань, включаючи організаційні, фінансові, господарські тощо, а також приймаються певні рішення і надаються відповідні доручення.

За необхідності обмеження доступу до окремих питань доручення адресуються безпосередньо виконавцю. Перелічені факти свідчать про певний управлінський аспект застосування чатів у суспільстві. А це дає логічні підстави для застосування результатів досліджень таких систем в інтересах вирішення поставленої задачі – оцінки довжини таких повідомлень.

Зокрема, на підставі результатів оцінки довжини повідомлень у рамках демографічних досліджень, що отримані в [153, 177], створена діаграма (рис. 3.1), з якої неважко бачити, що з імовірністю більше 0,95 довжина повідомлень у досліджуваних чатах WhatsApp не перевищувала 100 символів (літер) англійської мови.

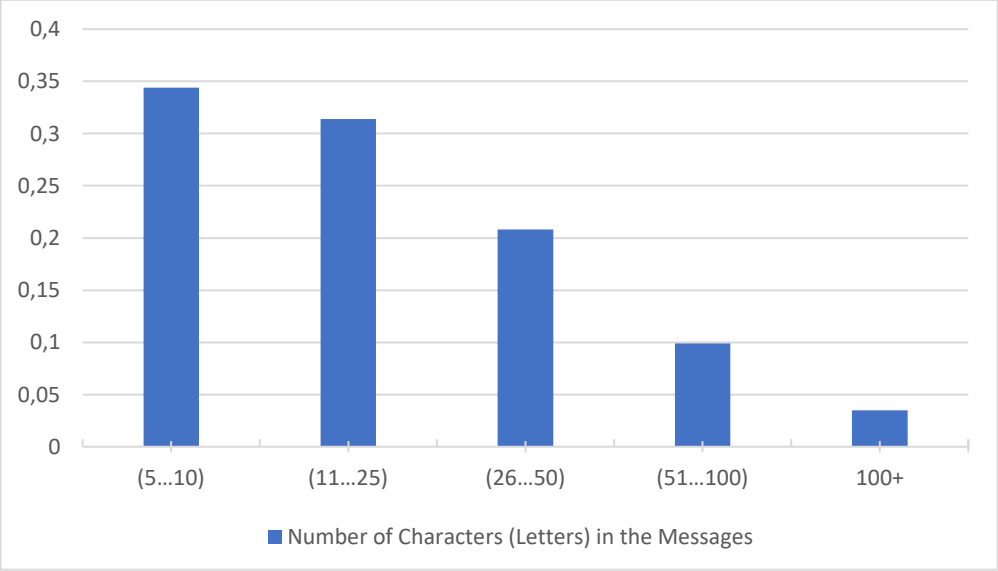

Рисунок 3.1 – Розподіл імовірностей довжин повідомлень англійської мови в чатах месенджера WhatsApp

Зазначимо, що в цьому випадку вихідні дані щодо розподілу довжин в чаті були наведені авторами досліджень у словах досліджуваної мови. Підчас перерахунку в діаграмі рис. 3.1 використана оцінка середньої довжини слова англійської мови в 5 букв [178]. Водночас відмітимо, що середня довжина слова української мові може сягати 6-7 букв, тобто різниця з англійською мовою становить порядку 20 %.

Виходячи з наведених у [179] даних про автоматизований переклад повідомлень у чатах (пост або коментар до нього) в мішаних кодах (мови хінді + англійська), можливо побудувати дещо іншу діаграму (рис. 3.2). При цьому використана типова процедура перетворення даних статистичного спостереження в гістограму [144].

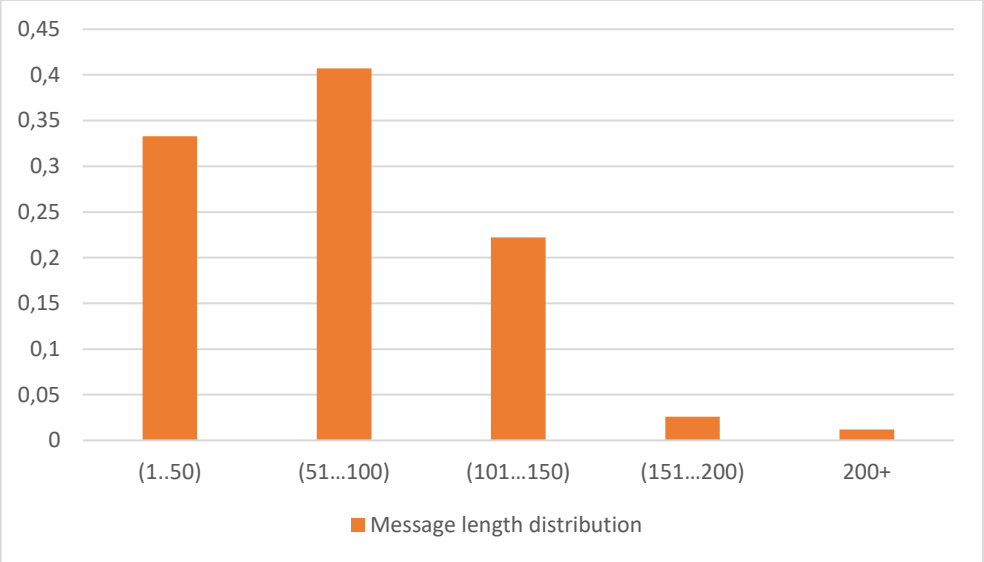

Рисунок 3.2 – Розподіл довжин повідомлень в індійських чатах

Коментуючи цю діаграму, слід відмітити, що можлива зміна мови і тематики досліджуваних постів і коментарів вплинула на їх розподіл довжин повідомлень. Зокрема, мода розподілу зсунулася вбік довжин з інтервалу (51,100), а також з ймовірністю більше 0,96 довжина навмання обраного повідомлення належить інтервалу (1,150). Інші довжини спостерігаються з ймовірністю меншою за 0,04.

Зауважимо, що в [179] наведені дані щодо розподілу довжин повідомлень (речень) після їх коректного перекладу на англійську мову, при цьому візуально суттєвої різниці не спостерігається. Надати математичну оцінку цьому факту не вдалося внаслідок різних інтервалів спостережень, а також відсутності точних числових даних спостереження та обсягу вибірки.

Слід звернути увагу, що результати двох незалежних досліджень [153, 177] та [179], які переслідували різні цілі в різних галузях знань, надали достатньо близькі за суттю результати.

Якщо в зазначених роботах вивчались виключно емпіричні результати, то в [180] і [181] були визначені гіпотези щодо розподілу довжин повідомлень, що становить окремий науковий інтерес. Зважаючи на те, що дослідження в [181] стосується невідомих нам характеристик інформаційного обміну в рамках Центру зарубіжних комунікаційних послуг (Бомбей, Індія), залишимо ці результати для вивчення й аналізу у подальшому.

Щодо результатів у [181] відмітимо, що авторами перевірено гіпотезу відносно розподілу довжин повідомлень у соціальних мережах згідно з логнормальним законом, а саме фактом, що функція розподілу має вигляд

$$f_{LN}(L) = \frac{1}{\sqrt{2\pi\sigma}}\frac{1}{L}exp(-(\ln(L) - \mu)^2/2\sigma^2),$$

де L – це довжина коментаря, а μ та σ – змінні параметри. Цей розподіл має моду $c = \exp(\mu - \sigma^2)$, середнє $\bar{f} = \exp(\mu + \frac{\sigma^2}{2})$ та медіану $m = \exp(\mu)$.

У підсумку дослідження відмічений хороший збіг теоретичних і практичних даних для відносно великих значень довжини повідомлень і дещо гірший результат отриманий для коротких повідомлень.

У нашому випадку становить інтерес саме питання відносно максимальних довжин, тому відмітимо, що максимальне значення функції розподілу довжин за даними в [180] для форуму BBC (British Broadcasting Corporation) і польських форумів досягається приблизно для 60 байт, але

внаслідок великого значення дисперсії σ^2 середня довжина повідомлення для форуму BBC і польського форуму ставлять 434 і 257 байтів відповідно. Якщо порівнювати ці результати з даними на діаграмах рис. 3.1 і рис. 3.2, можливо висунути гіпотезу, що збільшення довжин повідомлень у цьому випадку скоріш за все обумовлене політичною та культурологічною тематикою інформаційного обміну, яка потребує в чаті більш розгорнутого доведення власних думок учасників дискусій.

Крім того, в [180] для довжини повідомлень у вебресурсах YouTube та MySpace отримані оцінки середніх значень 104 і 124 байти відповідно.

Звернемо також увагу, що стандартна довжина інформаційної частини SMS становить 1120 біт [151], що надає можливість передати в одному повідомленні до 160 символів англомовного повідомлення, або до 70 символів у випадку використання як алфавіту кирилиці. SMS більшої довжини для передачі поділяються на частини.

Підсумовуючи вище викладене, в разі використання в службових цілях як інформаційно-комунікаційних платформ короткими доцільно вважати повідомлення довжиною до 150 байтів (до 1200 біт).

3.1.3 Атаки на захищений обмін з метою розпізнавання стану об’єкта та протидія ним

Нехай шифроване повідомлення $C = E(M, K)$ створене за допомогою криптографічного перетворення E з відкритого повідомлення M довжини $|M|$ допомогою ключа K. У загальному випадку метою проведення атак на криптографічну систему може бути часткове дешифрування повідомлення, безключове розкриття повідомлення або розкриття одночасно повідомлення і ключа. У випадку практично стійкого криптографічного перетворення,

безпечної реалізації та безпомилкового застосування засобу шифрування зазначені цілі недосяжні.

Водночас переважна більшість сучасних систем потокового і блокового шифрування, призначених для забезпечення конфіденційності даних в ІКС, не змінюють довжини файлів у результаті їх шифрування. Для таких систем $|C| = |M|$.

Несуттєвим доповненням довжини файлу можуть бути декілька байтів вектору ініціалізації або посилання на діючий комплект ключів шифрування. Внаслідок цього розподіл частот зустрічаємості довжин шифрованих повідомлень буде або повністю співпадати з відповідним розподілом відкритих повідомлень (рис. 3.1 і рис. 3.2), або несуттєво відрізнятися. Останній факт створює потенційну загрозу для реалізації атак на систему захисту.

Нехай H – деякий стан ОКІ, M – службове повідомлення. Якщо умовна ймовірність $P\left(H/_M\right) \neq P(H)$, то повідомлення M будемо називати характеристичним для стану H.

Нехай невідомі $M_{H1}, \dots, M_{Hk}$ є характеристичними повідомленнями для стану H, а серед множини шифрованих повідомлень $\mathcal{C} = \{C_i, i = 1,2, \dots\}$ є, зокрема, зашифровані характеристичні повідомлення. Якщо існує поліноміальний алгоритм $\mathcal{A}$, який дозволяє з використанням множини $\mathcal{C}$ оцінити умовну ймовірність $P\left(H/_{\mathcal{C}}\right)$ стану H, тоді будемо говорити про потенційну загрозу атаки на захищений обмін із метою розпізнавання стану об’єкта на основі зашифрованих повідомлень.

Звернемо увагу на те, що часткове дешифрування може розглядатись як загроза вказаної атаки.

Внаслідок специфіки інформаційного обміну в рамках окремих об’єктів, згідно зі змінами розподілу довжин повідомлень без застосування процедур криптоаналізу, можна виділити такі варіанти оцінювання змін станів:

1. Оцінювання різниці середньої довжини повідомлень у звичайному стані L_{mid} та середньої довжини повідомлень у стані H: L_{midH}, при цьому в разі незміни стану виконується нерівність Чебишова:

$$P(|L_{midH} - L_{mid}| \geq t) \leq \frac{\sigma^2}{t^2}.$$

Більш точна оцінка може бути отримана з використанням логнормального розподілу довжин повідомлень, що наведене у попередньому розділі.

2. Враховуючи, що внаслідок усереднення довжини може втрачатись суттєва інформація про застосування в ІКС характеристичних повідомлень, для розпізнавання зміни стану об'єкта може бути застосована статистика χ^2 узгодження Пірсона [144], а саме:

$$\chi^2 = \sum_{i=L_{min}}^{L_{max}} \frac{(\mu_{iH} - \mu_i)^2}{\mu_i},$$

де $\{\mu_i,\ i = \overline{L_{min}, L_{max}}\}$ – сукупність частот довжин повідомлень від мінімальної (L_{min}) до максимальної (L_{max}), $\{\mu_{iH},\ i = \overline{L_{min}, L_{max}}\}$ – сукупність частот довжин повідомлення відносно яких висувається гіпотеза про перехід досліджуваного об'єкта до стану H. Вказана гіпотеза відхиляється, якщо розраховане значення статистики перевищує значення квантиля з відповідним рівнем надійності.

Ефективними інструментами протидії реалізації зазначених атак, що дозволяють уникати аналізу довжин повідомлень, є такі заходи:

– зміни випадковим чином довжин відкритих повідомлень до початку їх шифрування шляхом їх дроблення на частини;

– надсилання випадковим чином фіктивних повідомлень із спеціально обраним розподілом їх довжин;
– обрання однакової (максимальної) довжини всіх повідомлень;
– використання надійно захищених VPN-з’єднань.

Кожен з варіантів має власні переваги та недоліки, тому доцільність їх застосування може бути визначена в конкретних умовах функціонування ІКС.

3.2 Методика декомпозиції складної інформаційної системи критичної інфраструктури

З’ясувавши аспекти безпеки криптографічного захисту в плані шифрування коротких повідомлень, уявляється доцільним визначити умови застосування підсистеми криптографічного захисту інформації (КЗІ) в складних інформаційних системах енергетичного сектору та загалом ОКІ для убезпечення інформації з обмеженим доступом та контролю її цілісності, а також у формуванні методики раціонального синтезу надійної підсистеми КЗІ.

Вище було запропоновано (підрозділ 1.1.2) описове визначення складної системи.

З урахуванням результатів дослідження об’єкта інформатизації, визначення його характеристик і властивостей, надалі сфокусуємося на таких аспектах складної інформаційної інфраструктури енергетичного сектору (підрозділ 1.1.2), як:

– 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 системи і ефективності її функціонування від 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. Припустимість використанням в окремих підсистемах мобільних пристроїв загального користування для реалізації дистанційного доступу до деяких ресурсів.

У 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.

Питання декомпозиції складних систем досліджено в [182–184], у нашому випадку проаналізуємо задачу декомпозиції складної інформаційної інфраструктури CS із метою убезпечення інформаційного обміну деякої множини взаємодіючих між собою підсистем, в яких обробляються інформаційні ресурси, вимоги захисту якої визначаються їх різними власниками.

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

$$G(V,A) = \langle V,A\rangle,\ V = \{v_1(r_1), v_2(r_2), \dots, v_n(r_n),\},\ A \subseteq V \times V, \qquad (3.1)$$

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).

Зазначимо, 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 у підсистемі CS, що є потенційним її споживачем, не менше рівня безпеки такої інформації в підсистемі, яка є утримувачем. При цьому можна вважати, що будь-який документ може бути переданий із 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 $r_i = r_j$. У 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 [119], тобто воно є відношенням еквівалентності відносно якого множина вершин може бути подана у вигляді прямої суми класів еквівалентних вершин:

$$V = \bar{V}_0 \dot{+} \bar{V}_1 \dot{+} \ldots \dot{+} \bar{V}_m, \ \bar{V}_i \cap \bar{V}_j = \emptyset, i \neq j \ . \tag{3.2}$$

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

$$\bar{V}_0 \longrightarrow \bar{V}_1 \longrightarrow \cdots \longrightarrow \bar{V}_m. \tag{3.3}$$

При цьому передача документи з будь-яким 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 зворотний 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 неявности 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 $\bar{V}_i$ у клас $\bar{V}_J, j < i$ з меншим рівнем захищеності є необхідність мінімізації ризику в разі реалізації загрози витоку інформації. Які спеціальні умови необхідно забезпечити для досягнення вказаної мети? Надалі перелічимо відповідні шість спеціальних умов, що позначені, як ***U***1 – ***U***6.

U1. Очевидно, передача інформації потребує, щоб рівні безпеки підсистеми отримувача та підсистеми відправника були максимально близькими. Це означає, зокрема, що умовна спрямована дуга може застосовуватися в (3) тільки між сусідніми еквівалентними класами, тобто умовні спрямовані дугі можуть з'єднувати тільки безпекові класи:

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

U2. 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).

U3. Довжина конфіденційного повідомлення, що передається в цих умовах, має бути максимально обмежена.

U4. Особи (суб'єкти), що можуть отримати доступ до відповідного конфіденційного повідомлення, мають бути погоджені (визначені) власником інформації.

U5. Інформація, що передається визначеним особам, має бути захищена за допомогою схвалених організаційно-технічних заходів.

U6. 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 спеціальних умов ***U***1 – ***U***6 початкова складна система (3.1) може бути подана у вигляді поєднання її підсистем, що більш пристосовані для забезпечення безпеки конфіденційності інформації в цій системі:

$$G(V,A) = \langle V,A \rangle \implies G(\bar{V}_0 \dot{+} \bar{V}_1 \dot{+} \ldots \dot{+} \bar{V}_m, A, U). \qquad (3.4)$$

Отриману декомпозицію CS ілюструє рис. 3.3.

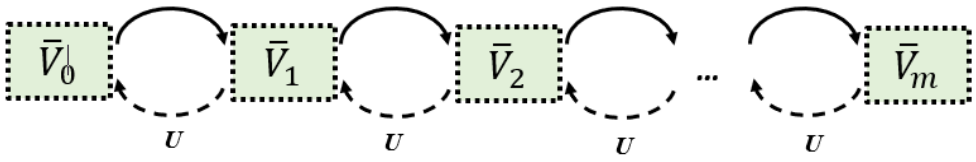

Рисунок 3.3 – Декомпозиція складної інформаційної системи

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

3.3 Вдосконалення моделі криптографічного захисту інформації

Серед спеціальних умов безпеки для передачі інформації з більш високими вимогами щодо її захисту в клас з нижчим рівнем захисту ***U***1 – ***U***6 найбільш важливим є фактор ***U***5, що передбачає реалізацію адекватних моделей та методів захисту.

В ряду 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 [185] суттєво знижується ймовірність вірусної атаки з боку глобальної мережі, оскільки спроба вбудувати злоякісний код в зашифрований потік або пакет даних із високим рівнем імовірності 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 [186, 187].

В умовах, коли зростання кількості та потужності кібератак на 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 [187, 188] для убезпечення ОКІ.

Зокрема, процедура вибору засобів криптографічного захисту інформації (КЗІ) повинна забезпечити визначення такої їх архітектури, що в комплексі забезпечує необхідний рівень конфіденційності та контроль цілісності даних в ІКС ОКІ, мінімізуючи при цьому вартість утримання.

Під архітектурою засобів КЗІ далі розуміємо сукупність їх криптографічних компонент, що доповнюють одна одну та сумісно реалізують повний комплекс необхідних функцій, включаючи модулі шифрування конфіденційної інформації, підсистему генерації та розподілу ключів, модуль контролю поточного стану та блокування помилок, 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 таких 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 [116] та відгуки експертів щодо результатів їх практичного застосування;

– оцінка вартості 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 [189] 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 [190, 191], 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 з діючими нормативними актами [190].

Друга група факторів включає, зокрема, такі функціональні характеристики:

1. Ступінь сумісності засобів КЗІ з вимогами запланованої до застосування транспортної інформаційної мережі (поширеними протоколами взаємодії).

2. Сумісність із 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. 3.4).

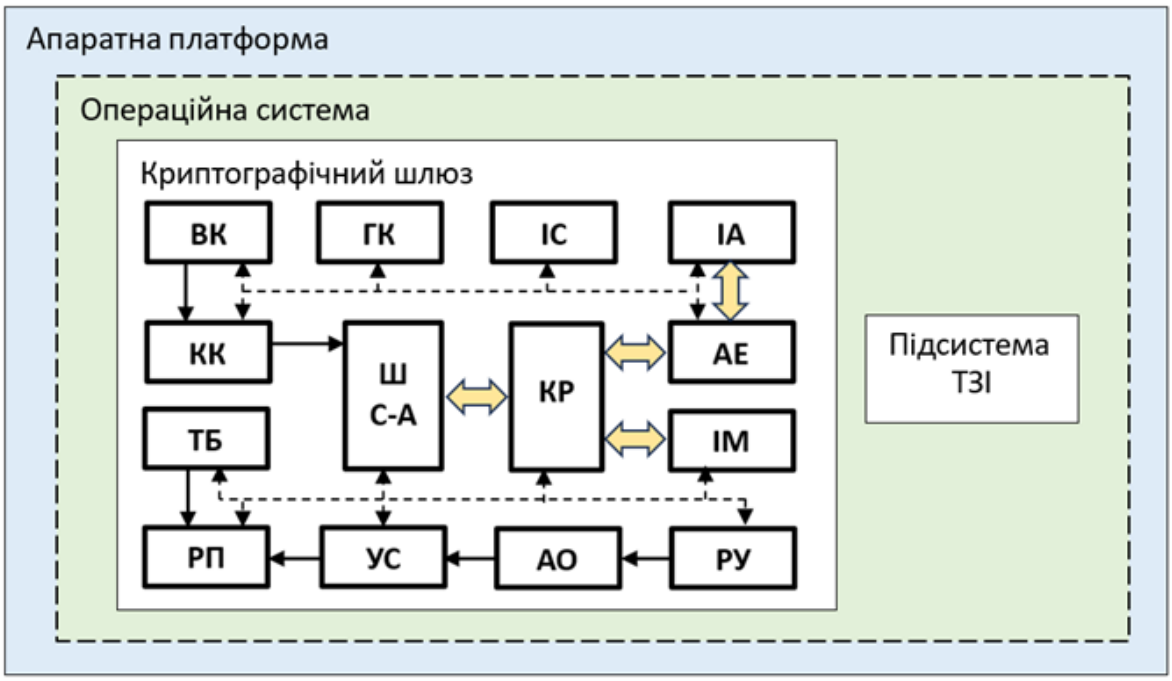

Рисунок 3.4 – Вдосконалена модель підсистеми КЗІ – шлюз безпеки

У вдосконаленій моделі використовуються модулі (вузли), які реалізують такі 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 рис. 3.4 показані сигнали управління та інформації про стан вузлів шлюзу. Суцільними лініями показана передача параметрів (символ →) та інформації, яка підлягає шифруванню (символ).

На відміну від прототипу [191] у вдосконаленої моделі засобу КЗІ передача даних 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 (МАС).

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

Відповідний МАС 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. У разі зміни документа, навіть часткової, МАС встановленим порядком формується на ново.

Для реалізації визначених функцій вдосконалена модель також має додаткові елементи. Головною відмінністю наведеної моделі порівняно з прототипом [191] є введення таких процедур, що відповідають необхідності виконання спеціальної умові ***U***5:

– контролю за наявністю відміток про погодження можливості передачі певного документа до іншої системи обробки даних вузла АЕ – автентифікації і екранування;

– реєстрації подій РП у 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;

– застосування 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 елементи мають бути убезпечені за допомогою підсистеми технічного захисту інформації, на яку, зокрема, покладаються завдання антивірусного захисту та розмежування доступу.

3.4 Характеристика показників підсистеми криптографічного захисту та їх раціональне визначення

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 [192].

При цьому показник ефективність може включати такі субпоказники, як імовірність виявлення та блокування небезпечної події, час, необхідний для однократної реалізації певної захисної функції, повернення інвестиційних коштів [192–194] 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 [29, 187], що базовим елементом методики раціонального вибору засобів КЗІ має бути побудова рейтингової шкали відображення цих показників у зіставні числові значення:

$$\bar{\alpha} \longmapsto \bar{x} = (x_1, \dots, x_n) \in \mathbb{R}^n, \tag{3.4}$$

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

Доволі простим варіантом реалізації шкали відображення в (3.4) 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 з [116].

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 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):

$$\mathcal{F}(x_1, x_2, \dots) = \frac{W}{M}\sum_j x_j\ , \tag{3.5}$$

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:

$$\mathcal{F} = \mathcal{F}_\text{C} + \mathcal{F}_I + \mathcal{F}_A + \mathcal{F}_O. \tag{3.6}$$

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

В таблиці 3.1 наведений приклад реальних даних щодо функціональних профілів двох засобів захисту інформації (ЗЗІ), лише деякі їх показники були змінені для наочності.

З таблиці 3.1 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 3.1).

Ненормована сума по всіх критеріях свідчить про перевагу на користь першого засобу (значення 7.37 проти 7.2). Але тут не враховано той факт, що кількість критеріїв у 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 3.1 наведені розрахунки за формулами (3.5) і (3.6) 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 такі 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:

$$\mathcal{F}_{i_1} \le \mathcal{F}_{i_2} \le \ \dots \ \le \mathcal{F}_{i_K}, \text{де } i_1, i_2, \dots, i_K \in \overline{1,K}, i_m \ne i_n, \text{де } m \ne n. \quad (3.7)$$

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 (3.7) набуває нової якості:

$$\mathcal{F}_{j_1}/_{C_{j_1}} \le \mathcal{F}_{j_2}/_{C_{j_2}} \le \dots \le \mathcal{F}_{j_K}/_{C_{j_K}}, \text{ де } j_1, j_2, \dots, j_K \in \overline{1,K}, j_m \ne j_n, \text{де } m \ne n. \quad (3.8)$$

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, які 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, з 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 3.1 – Приклад: функціональні профілі безпеки та зіставлені показники

№ №	Критерії безпеки	ЗЗІ - 1		ЗЗІ - 2		Краще?
		α_j	x_j	α_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	>

Продовження таблиці 3.1

Критерії спостереженості K_j^0						
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 такі відповідності «клас захищеності – рівень гарантій»: А (відмінно) – Г4, В (нормально) – Г3, С (непогано) – Г2.

3.5 Висновки до розділу 3

1. Проведений огляд наукових публікацій із захисту коротких повідомлень та узагальнення даних досліджень розподілу довжин коротких повідомлень у чатах сучасних комунікаційних додатків надалі, що дає можливість оцінити потенційну загрозу проведення зловмисником атак на мобільні захищені ІКС ОКІ з метою визначення стану цих об’єктів, а також сформулювати практичні рекомендації по протидії їх реалізації.

2. Досліджено методологію побудови підсистем захисту інформації в складних інформаційних систем ОКІ, окремо виділено питання забезпечення криптографічного захисту в цих системах. Відмічено, що складним системам притаманні такі властивості, як наявність значної кількості різнорідних елементів, що об’єднані в єдину систему для досягнення певної мети; існування складних, іноді, суперечливих зв’язків та впливів; потужні інформаційні потоки між складовими підсистемами.

Проведено аналіз характеристик складних інформаційних систем ОКІ, включаючи енергетичний сектор, які негативно впливають на побудову підсистем захисту інформації, визначено актуальність розв’язання завдань формування специфічних моделей та методик захисту в таких системах, особливо їх комплексного захисту.

У визначених умовах реалізації підсистем КЗІ для убезпечення інформації з обмеженим доступом та контролю її цілісності в складних системах вперше запропоновано методику декомпозиції складних систем одного виду та вдосконалено модель криптографічного захисту в них.

3. З метою підвищення ефективності процедур порівняння значної кількості якісних та кількісних показників підсистемах захисту інформації для визначення необхідних апаратно-програмних рішень запропоновано методику їх раціонального вибору на основі максимуму визначеної функції безпеки, що

використовує функціональні профілі захищеності та інші показники засобів захисту.

Основні результати розділу опубліковані автором у працях [1–6].

РОЗДІЛ 4
МЕТОДОЛОГІЧНІ АСПЕКТИ ПРОЄКТУВАННЯ СИСТЕМИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ В ІКС-ЕС

4.1 Вдосконалення методики побудови системи захисту на основі результатів дослідження

Виходячи з проведеного аналізу наукових публікацій, вивчення вимог нормативно-правових актів та нормативно-технічних документів, узагальнення досвіду практичних розробок систем ефективного забезпечення кіберзахисту та гарантоздатності інформаційної інфраструктури загалом ОКІ та, зокрема, енергетичного сектору можливо зробити висновок, що для успішного розвязання при цьому основних завдань та уникнення майбутніх проблем ключове значення має наукова проробка та постійне вдосконалення методологічного забезпечення відповідних процесів.

Діючі нормативно-правові акти та стандарти [28, 74] в цілому визначають концептуальні методологічні засади реалізації проєктів систем захисту. Зокрема, процесний підхід до управління інформаційною безпекою [74] пропонує модель, яка включає чотири фази життєвого циклу відповідної системи безпеки, а саме: планування (plan), реалізація (do), перевірка (check), застосування (act).

Деталізація процесів, що реалізуються в рамках вказаних етапів, фактично наведена в [28], при цьому відповідний перелік робіт у загальному випадку включає такі кроки (К1 – К9):

К1. Визначення категорій інформації, яка обробляється, здійснення оцінки інформаційних активів, що підлягають захисту.

К2. Прийняття рішення на адміністративному рівні управління щодо забезпечення захисту інформації (кіберзахисту), створення або призначення підрозділу (можливо, окремих посадових осіб), що відповідатиме за реалізацію на операційному рівні відповідних заходів.

К3. Проведення обстеження об’єкта інформатизації з метою визначення базових умов для побудови системи захисту, які включають вимоги до експлуатації автоматизованих систем та методів і технологій обробки технологічної інформації в ОЕС-У, застосовані при цьому конкретні програмні та апаратні платформи, впроваджені засоби захисту, оцінка стану нормативного забезпечення та характеристика середовища користувачів систем. Зібрані та впорядковані належним чином у вигляді актів обстеження дані використовуються на наступних кроках. Акти обстеження мають бути затверджені власниками відповідних підсистем ОЕС-У.

К4. Розроблення на основі даних попереднього кроку моделі загроз, моделі порушника та вихідних вимог до побудови системи інформаційної безпеки (кіберзахисту).

К5. Вибір кваліфікованого виконавця проєкту та розроблення технічного завдання на побудову системи інформаційної безпеки (кіберзахисту).

К6. Реалізація проєкту побудови системи інформаційної безпеки (кіберзахисту), розроблення пакету документації на систему захисту, включаючи настанови з питань її експлуатації та забезпечення безпеки.

К7. Проведення попередніх випробувань та дослідної експлуатації з метою виявлення та усунення помилок та невідповідності вимогам технічного завдання, а також відповідного корегування документації. Дослідна експлуатація також використовується для навчання обслуговуючого персоналу системи щодо дій в умовах наближених до реальної обстановки.

К8. Підготовка та проведення державної експертизи (сертифікації) створеної системи захисту з метою отримання атестату відповідності вимогам нормативних документів (сертифікату).

К9. Реалізація комплексу заходів з метою введення створеної системи захисту у промислову експлуатацію.

Перераховані етапи в рамках конкретних проєктів створення систем захисту можуть деталізуватися та частково перетинатися за окремими заходами.

Виходячи з результатів проведених досліджень та потреб практики щодо уникнення ситуацій з погіршенням спроможності стійкого функціонування електричних систем та неприпустимого зниження якості електричної енергії, пропонується таке методичне уточнення змісту виконуваних кроків (рис. 4.1), модифікація яких далі позначена, як $\widetilde{К}1, \widetilde{К}3, \widetilde{К}4, \widetilde{К}6, \widetilde{К}7$.

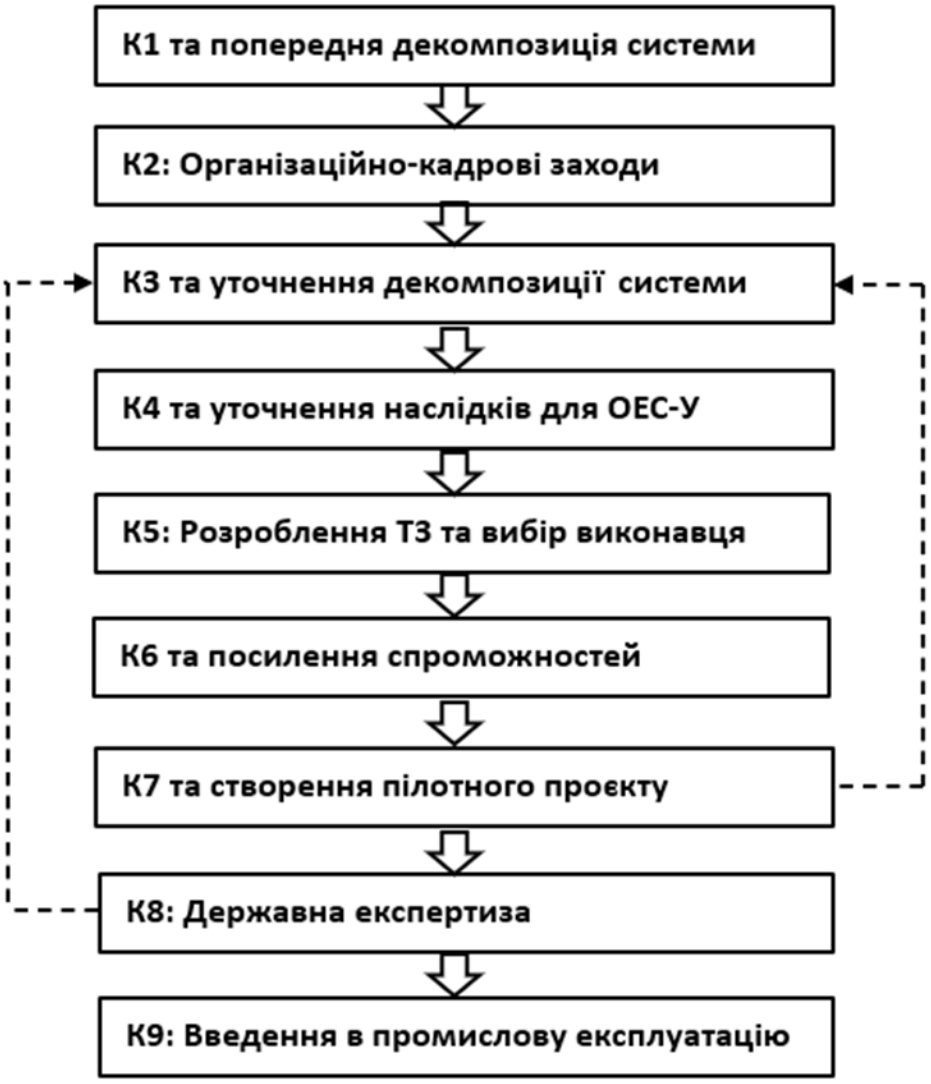

Рисунок 4.1 – Етапи побудови системи захисту з урахуванням пропонованих змін

$\widetilde{К}1$. На початку проведення аналізу умов забезпечення безпеки об’єктів критичної інфраструктури, зокрема, систем енергетичного сектору, доцільно

з’ясувати, чи є система, яка захищається інтегрованою складною системою? (див. п. 1.1.2).

У випадку позитивної відповіді на визначене питання для вказаної системи виконується попередня процедура декомпозиції згідно з п. 3.2 та визначаються умови передачі інформації з однієї підсистеми в іншу $\boldsymbol{U}1$ – $\boldsymbol{U}6$.

На підставі проведеного дослідження для забезпечення конфіденційності інформації, що передається з підсистеми з високим рівнем безпеки до підсистеми з низьким рівнем безпеки для певної посадової особи, практично відпрацьована процедура двоконтурного шифрування за допомогою мобільного пристрою отримувача.

Іншою особливістю реалізації модифікованого першого кроку створення системи забезпечення кібербезпеки та гарантоздатності стало уточнення категорій інформації, підлягають захисту та здійснення оцінки інформаційних активів. Пріоритетом визнано убезпечення критичної технологічної інформації, згідно із законом [195], за режимом доступу належить до інформації з обмеженим доступом та підлягає захисту.

$\widetilde{К}3$. На підставі зібраної та проаналізованої в рамках проведення обстеження підсистем об’єкта інформатизації має здійснюється уточнення попередньої схеми декомпозиції (див. крок $\widetilde{К}1$) та спеціальних умов передачі інформації між підсистемами з різними рівнями безпеки $\boldsymbol{U}1$ – $\boldsymbol{U}6$.

$\widetilde{К}4$. Під час відпрацювання на підставі результатів обстеження ОІД моделі загроз та моделі порушника для кожного виду критичної технологічної інформації відповідно до п. 1.4.2 детально визначаються потенційні наслідки порушення режиму їхньої безпеки.

$\widetilde{К}6$. На етапі технічного проєкту відповідно до пп. 2.1.2, 2.1.3, 2.2.2, 2.3.1 – 2.3.3 з метою посилення спроможностей до «кризового» реагування особлива увага приділяється аспектам побудови корпоративного центру кібербезпеки та підтримки гарантоздатності енергетичного сектору.

На цьому етапі, відповідно до п. 3.4, впроваджується вдосконалена криптосхема шлюзу безпеки та раціонально визначаються показники безпеки

засобів криптографічного захисту інформації. Для забезпечення безпеки шлюзу та підвищення його швидкодії бажаною є його програмно-апаратна реалізація.

К̃7. Обов’язкова реалізація пілотного проєкту для проведення дослідної експлуатації.

Слід заначити, що на етапах К̃7 та К8 (рис. 4.1) у необхідних випадках можуть бути прийняті рішення щодо уточнення декомпозиції системи.

Як було зазначено вище, для окремих категорій посадових осіб на їх мобільних пристроях пропонується програмна реалізація криптографічного додатку для реалізації процесів попереднього шифрування конфіденційної інформації, яка передається за допомогою обраних месенджерів. У наступному підрозділі наведені дані щодо відповідної практичної схеми.

4.2 Практична реалізація процедури двоконтурного шифрування на мобільних пристроях

Практика побудови та застосування сучасних корпоративних мереж свідчить про нагальну потребу створення підсистем та механізмів захищеного доступу мобільних абонентів до критичних ресурсів. Наявність відповідних підсистем диктується бізнес-логікою високо технологічних галузей промисловості та необхідністю топ менеджменту підприємств мати будь-де та будь-коли можливість дистанційного керування відповідними процесами.

Наслідком цього у останні роки сталося, з одного боку, у середовищі користувачів зростання кількості застосувань мобільних додатків на смартфонах для обміну повідомленнями та голосового зв'язку, з іншого боку, підвищення інтересу серед науковців та практиків до досліджень проблем, що пов'язані з безпеки застосування цих додатків у плані забезпечення конфіденційності чутливих даних.

Зокрема, в аналітичних матеріалах, імовірно, австралійського походження [196–197] наведено змістовний аналіз 15 поширених месенджерів та надані з технічними подробицями певні застереження щодо їх можливих вразливостей. При цьому в 10-ти з перерахованих месенджерів для шифрування даних за принципом “end-to-end” використовується стійкий блоковий алгоритм AES-256, але на головне питання: «чи рекомендується програма для захисту моїх повідомлень і вкладень?» огляд дає умовно позитивну відповідь лише для п’яти месенджерів.

Зважаючи на потенційну загрозу несанкціонованого доступу до інформації, що передається за допомогою месенджерів на мобільних пристроях та для забезпечення персонального отримання певних даних (спеціальна умова ***U***5), було практично реалізовано у вигляді додатка програмний шифратор на платформі Android.

До шифратора були визначені такі основні криптографічні вимоги:

– тип шифрування – попереднє;
– стійкість криптографічного перетворення щодо атаки повного перебору ключів – не гірше 2^{128};
– імітостійкий вузол накладання гами шифру;
– здатність працювати на платформах з обмеженими обчислювальними ресурсами для сумісності з пристроями IoT (Internet of Things) [80].

З урахуванням вказаних вимог, у ролі алгоритма шифрування було обрано перспективну розробку криптоалгоритму A5-128 [197]. Вихідний код створеного застосунку A5-128 на мові C# наведено у Додатку Б.

На рис. 4.2 зображені скріншоти екрана смартфону під час вибору файлу, що підлягає криптографічному захисту, введення пароля та вибору режиму зашифрування/розшифрування.

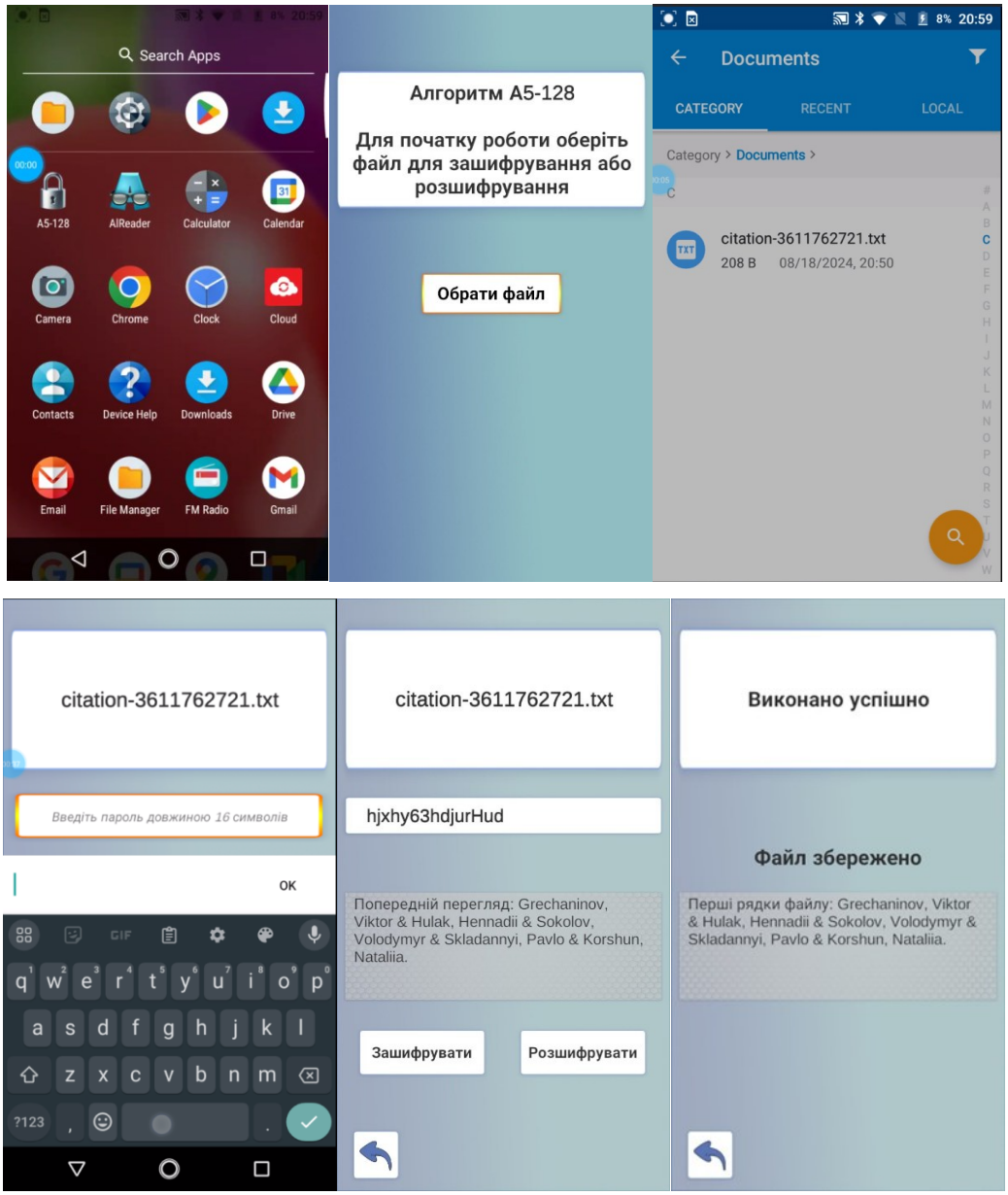

Рисунок 4.2 – Етапи роботи шифратора A5-128

Для захисту від несанкціонованого доступу при реалізації процедур зашифрування та розшифрування передбачено обов'язкове введення 16 символьного буквено-цифрового пароля.

Це дає достатньо високу складність щодо підбору пароля:

$$(26 + 10)^{16} \approx 2.8 \times 10^{12}.$$

На рис. 4.3 зображені заключні скріншоти екрана смартфону під час реалізації процедури шифрування.

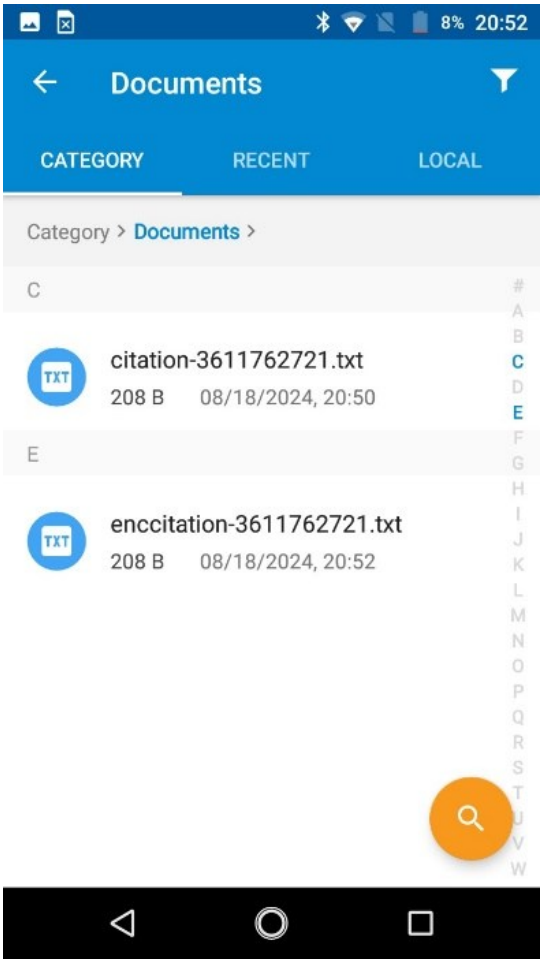

Рисунок 4.3 – Скріншот кінцевого результату процедури шифрування даних

За результатами тестових зашифрувань відкритих повідомлень на платформі чіпсет Mediatek MT6737 (28 нм), ЦП чотириядерний Cortex-A53 1,3 ГГц, оперативна пам'ять 2 Гб було отримано орієнтовний показник швидкодії, що перевищує 1 Мбайт\с (на 15–20% швидше, ніж стандартні алгоритми «легкої» криптографії [80]).

Зрозуміло, що досягнута швидкодія достатня для практичного застосування відносно коротких повідомлень, які передаються за допомогою месенджерів на сучасних мобільних пристроях.

Розподіл ключів для невеликої мережі мобільних пристроїв, що забезпечуватимуть захищений зв'язок, нескладно реалізувати шляхом завантаження необхідної кількості ключів під час початкової реєстрації пристроїв. При цьому ключі доцільно захищати шляхом зашифрування з використанням пароля користувача.

Для великої кількості користувачів може бути використана система розподілу на основі симетричних криптоалгоритмів із використанням транспортних ключів, що забезпечить високу швидкодію та дозволить уникнути обтяжливої процедури сертифікації відкритих ключів у разі застосування асиметричних криптосистем.

Саме в цьому напрямі уявляється доцільним продовжити прикладну частину подальших досліджень.

4.3 Висновки до розділу 4

1. Апробація результатів досліджень у рамках методологічного забезпечення етапів проєктування систем кіберзахисту та забезпечення гарантоздатності інформаційних систем енергетичного сектору свідчить про їх актуальність та практичну значущість для підвищення спроможності енергетики виконувати відповідні завдання в умовах складного ландшафту кіберзагроз.

2. Запропоновані рішення щодо моделей та методів на поточний час уже частково впроваджені та довели свою відповідність складним умовам функціонування енергетичного сектору в військовий час.

3. Подальші дослідження доцільно зосередити на аспектах управління ключами для запропонованих моделей та методів.

Основні результати розділу опубліковані автором у працях [1–6].

ВИСНОВКИ

У результаті дисертаційних досліджень, виконаних автором, вирішено актуальне наукове завдання, що полягає в розробці моделей та методів забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору на основі захисту інформаційних ресурсів та технологічної інформації від загроз конфіденційності, цілісності та доступності за рахунок реалізації концепції корпоративного кіберзахисту, розробки моделей і методів криптографічного захисту інформації, що збирається, передається та обробляється в ІКС-ЕС.

Вирішення цього наукового завдання має важливе значення для забезпечення кіберстійкості енергетичних систем як об’єктів критичної інфраструктури, що характеризуються специфічними властивостями та особливими умовами функціонування, а саме:

– вимогами реагування в реальному часі на будь-які зміни в умовах експлуатації, що означає суттєві обмеження часу на обробку та передачу даних та команд. Цей фактор обмежує умови застосування відомих рішень із кіберзахисту;

– ризиком прояву каскадних ефектів, внаслідок чого локальний збій управляючої системи та вимкнення електроенергії або погіршення її якості в одному регіоні може спровокувати відключення електроенергії або перебої в електропостачанні в інших регіонах та навіть загалом у державі (black out);

– проблемами поєднання застарілих технічних рішень із сучасними технологіями, що потребує відпрацювання адекватних заходів із безпеки організаційно-технічного характеру.

У дисертаційному дослідженні отримані такі основні результати:

1. Вперше на основі формування класів еквівалентності запропоновано методику декомпозиції складних систем, що підлягають кіберзахисту, яка

враховує можливість інформаційного обміну між підсистемами з різними вимогами до захисту інформації з обмеженим доступом.

2. Вдосконалено модель побудови корпоративного центру кібербезпеки енергетичного сектору на основі сервіс-орієнтованої архітектури з визначеною бізнес-логікою та відповідним набором функцій, що забезпечуватиме динамічне оброблення кіберінцидентів у реальному часі та відповідність сучасним викликам безпеці та специфіці реалізації завдань і функцій ОЕС-У.

3. Вдосконалено модель побудови децентралізованої системи розмежування доступу в мережі центру кібербезпеки на основі оригінальної методики розподілу секрету. Запропонована модель припускає її масштабування та мінімізує ризик несанкціонованого доступу до інформаційних ресурсів.

4. Подальшого розвитку набула модель побудови підсистеми криптографічного захисту інформації, що забезпечуватиме можливість двоконтурного шифрування для розмежування доступу в децентралізованій системі розмежування доступу до інформаційних ресурсів та підвищену безпеку коротких службових повідомлень.

5. Подальшого розвитку набула методика оцінки та раціонального визначення характеристик захисту криптографічної підсистеми.

6. Запропоновані рішення та отримані показники їх ефективності роблять результати дослідження актуальними та пріоритетними.

7. Отже, мета дослідження, яка полягає у забезпеченні гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору України для виконання місії енергосистем за рахунок розробки моделей і методів криптографічного захисту інформації в складних системах, досягнута та всі часткові завдання вирішено повністю.

8. Основні наукові результати дослідження:

– реалізовані у рамках виконання держаних програм науково-дослідної діяльності в Інституті проблем математичних машин і систем Національної академії наук України та були використані для удосконалення архітектури та

функціональності ситуаційних центрів об’єктів критичної інфраструктури, підвищення рівня кіберзахисту;

– прийняті до впровадження у науково-практичній діяльності Інституту проблем безпеки атомних електростанцій Національної академії наук України для покращення кібербезпеки інформаційної інфраструктури енергосистем;

– впроваджені в освітньому процесі Київського столичного університету імені Бориса Грінченка.

9. Напрями подальших досліджень у зазначеній галузі можуть ґрунтуватися на вдосконаленні процедур декомпозиції складних інформаційних систем із метою розробки заходів щодо підвищення стану їхньої кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Верховна Рада України. (2017). Закон України Про ринок електричної енергії. *Відомості Верховної Ради (ВВР)*, № 27-28, ст. 312.

2. European Commission. (2020, July 24). *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy* (COM(2020) 605 final). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52020DC0605.

3. European Commission. (2019, April 3). *Commission Recommendation (EU) 2019/553 on cybersecurity in the energy sector* (C(2019) 2400). URL: https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0553&qid=1710706056802.

4. European Commission. (2019, April 3). *Commission staff working document accompanying the document Commission Recommendation on cybersecurity in the energy sector* (SWD(2019) 1240 final). URL: https://circabc.europa.eu/ui/group/8f5f9424-a7ef-4dbf-b914-1af1d12ff5d2/library/0afed37a-e784-495d-b86b-69a41de76090/details?download=true.

5. Americas Cyber Defense Agency. (2015). *Energy Sector*. URL: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector.

6. Americas Cyber Defense Agency. (2015). *Energy Sector-Specific Plan*. URL: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.

7. Jewell, J. (2011). *The IEA Model of Short-term Energy Security (MOSES): Primary Energy Sources and Secondary Fuels*. IEA. URL: https://www.researchgate.net/publication/254439192_The_IEA_Model_of_Short-Term_Energy_Security_MOSES_Primary_Energy_Sources_and_Secondary_Fuel.

8. Nasibov, V., et al. (2018). Models of electric power industry security study for medium-term periods. *IFAC PapersOnLine, 51*(30), 405–409. DOI: https://doi.org/10.1016/j.ifacol.2018.11.342.

9. Кабінет Міністрів України. (2021, серпень 4). Про схвалення Стратегії енергетичної безпеки (№ 907-р). URL: https://zakon.rada.gov.ua/laws/show/907-2021-p#Text.

10. Кабінет Міністрів України. (2020, листопад 11). Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури (№ 1176). URL: https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text.

11. Президент України. (2021, серпень 26). Стратегія кібербезпеки України (Указ № 447/2021). URL: https://www.president.gov.ua/documents/4472021-40013.

12. Linkov, I., & Kott, A. (2018). Fundamental concepts of cyber resilience: Introduction and overview. In *Cyber resilience of systems and networks* (pp. 1-25). Springer International Publishing. DOI: https://doi.org/10.1007/978-3-319-77492-3_1.

13. Hollnagel, E., Woods, D. D., & Leveson, N. C. (2006). *Resilience engineering: Concepts and precepts*. Aldershot: Ashgate.

14. Hollnagel, E., Pariès, J., Woods, D. D., & Wreathall, J. (2011). *Resilience engineering perspectives. Volume 3: Resilience engineering in practice*. Ashgate.

15. Харченко, В. С. (2006). Гарантоздатність та гарантоздатні системи: елементи методології. *Радіоелектронні і комп'ютерні системи*, (5), 7–19.

16. Avizienis, A., et al. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing, 1*(1), 11–33.

17. IEC. (2002). *International Electrotechnical Vocabulary: Dependability and quality of service* (Ed. 1.0, Chapter 191). URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf.

18. Теслер, Г. С. (2006). Концепція побудови гарантоздатних обчислювальних систем. *Математичні машини і системи, 1*, 134–145.

19. Федухін, О. В., & Сеспедес Гарсия, Н. В. (2013). Атрибути і метрики гарантоздатних комп'ютерних систем. *Математичні машини і системи, 2*, 195-201.

20. Бондарук, А. Б., et al. (2008). Гарантоздатна інтегрована система навігації рухомих наземних об'єктів. *Вісник Національного університету "Львівська політехніка"*, (630), 24-30.

21. Ponochovniy, Y. L. (2019). Analysis of cyber security management concepts for distributed IT infrastructures. *Systems and Technologies, 2*(58), 87-101. DOI: https://doi.org/10.32836/2521-6643-2019-2-58-5.

22. Новиков, А. М., Родионов, А. Н., & Тимошенко, А. А. (2015). *Моделі та методи кібернетичного захисту інформаційно-комунікаційних систем на основі логіко-ймовірнісного підходу: Монографія*. НТУУ «КПІ», Політехніка.

23. Глухов, В. С. (2008). Оцінювання гарантоздатності криптографічних комп'ютерних систем. *Вісник Національного університету "Львівська політехніка"*, (616), 66-72.

24. Мінпаливенерго України. (2002). *Стійкість енергосистем. Керівні вказівки. ГКД 34.20.575-2002* (Наказ № 404).

25. Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг. (2018). *Про затвердження Кодексу системи передачі* (Постанова № 309). URL: https://zakon.rada.gov.ua/laws/show/v0309874-18#Text.

26. Міністерство енергетики України. (2022, грудень 15). *Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури* (Наказ № 417). URL: https://zakon.rada.gov.ua/laws/show/z0249-23#Text.

27. Zhang, S., Liu, X., & Wang, J. (2024). Research on the construction of a "full-chain" rapid response system for power emergencies. *Heliyon, 10*(4), e26501. DOI: https://doi.org/10.1016/j.heliyon.2024.e26501.

28. ДСТСЗІ СБ України. (2005). *НД ТЗІ 3.7-003 -2005 Порядок проведення робіт із створення комплексної системи захисту інформації*. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf.

29. Гулак, Є. Г. (2024). Методика раціонального синтезу підсистеми криптографічного захисту інформації в мережах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*, 4(24), С. 282-297. DOI: https://doi.org/10.28925/2663-4023.2024.24.282297.

30. Бусленко, Н. П. (1968). *Моделювання складних систем*. Видавництво «Наука».

31. Yang, K., et al. (2023). Complex systems and network science: A survey. *Journal of Systems Engineering and Electronics*, 34(3), 543-573. DOI: https://doi.org/10.23919/JSEE.2023.000080.

32. Ізраілов, К. Є., та ін. (2022). Оцінювання та прогнозування стану складних об'єктів: Застосування для інформаційної безпеки. *Питання кібербезпеки*, 6(52), 2-19.

33. Paulson, D., & Wand, Y. (1992). An Automated Approach to Information-Systems Decomposition. *IEEE Transactions on Software Engineering*, 18(3), 174-189. DOI: https://doi.org/10.1109/32.126767.

34. Chiriac, N., et al. (2011). Three approaches to complex system decomposition. In *Proceedings of the 13th International DSM Conference* (pp. 3-15). Cambridge, MA.

35. Pancerz, K., & Suraj, Z. (2013). A Rough Set Approach to Information Systems Decomposition. *Fundamenta Informaticae*, 127(1-4), 257-272.

36. International Renewable Energy Agency. (2022). *RE-organising power systems for the transition* (F. La Camera, Foreword). URL: https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2022/Jun/IRENA_Organising_Power_Systems_2022.pdf?rev=9c979df4adda4fe19cce18ab02f86e9c.

37. Міністерство енергетики та вугільної промисловості України. (2018). *Правила про безпеку постачання електричної енергії* (Наказ №448). URL: https://zakon.rada.gov.ua/laws/show/z1076-18#Text.

38. Міністерство палива та енергетики України. (2003). *Технічна експлуатація електричних станцій та мереж. Правила* (ГКД 34.20.507-2003).

39. Міністерство енергетики України. (2021). *Статут Приватного акціонерного товариства «Національна енергетична компанія Укренерго»*. URL: https://ua.energy/wp-content/uploads/2021/09/Statut-Minenergo-2021-1.pdf.

40. Chen, L., et al. (2024). Dynamics of cascading failure in cyber-physical power systems from cyberattack. *Physica Scripta*, 99(3). DOI: https://doi.org/10.1088/1402-4896/ad28e4.

41. Chu, X., et al. (2017). A security assessment scheme for interdependent cyber-physical power systems. In *Proceedings of the 8th IEEE International Conference on Software Engineering and Service Science* (pp. 816-819). DOI: https://doi.org/10.1109/ICSESS.2017.8343036.

42. Yohanandhan, R. V., et al. (2020). Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. *IEEE Access*, 8, 151019-151064. DOI: https://doi.org/10.1109/ACCESS.2020.3016826.

43. Voropai, N. (2020). Electric Power System Transformations: A Review of Main Prospects and Challenges. *Energies*, 13(21). DOI: https://doi.org/10.3390/en13215639.

44. Гнатюк, С., Сидоренко, В., & Сотніченко, Ю. (2020). Базові аспекти захисту конфіденційної інформації на об'єктах критичної інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка*, 1(9), С. 170–181. DOI: https://doi.org/10.28925/2663-4023.2020.9.170181.

45. ENISA. (2023). *Considerations on the Traffic Light Protocol*. URL: https://www.enisa.europa.eu/topics/incident-response/glossary/considerations-on-the-traffic-light-protocol.

46. GROUPSENSE. (2023). Understanding Traffic Light Protocol. URL: https://www.groupsense.io/resources/understanding-traffic-light-protocol.

47. ДЦК ДССЗЗІ України. (2021). *Загальні правила обміну інформацією про кіберінциденти. Протокол TLP*. URL:

https://cip.gov.ua/ua/news/zagalni-pravila-obminu-informaciyeyu-pro-kiberinciden ti-protokol-tlp.

48. FIRST. (n.d.). *Standards Definitions and Usage Guidance: Traffic Light Protocol V. 1.0*. URL: https://www.first.org/tlp/.

49. Служба безпеки України. (2023). *Положення про порядок обміну інформацією з використанням адаптованого програмного продукту «Malware Information Sharing Platform and Threat Sharing «Ukrainian Advantage» (MISP-UA)* (Наказ №503). URL: https://zakon.rada.gov.ua/laws/show/z2164-23#Text.

50. Вишневський, В. В., & Морозов, А. О. (2017). Ситуаційні центри як основа для стратегічного планування та управління державою. У *Збірник матеріалів VI Всеукраїнської науково-практичної конференції «Глушковські читання»*. С. 24-25.

51. Морозов, А. О., Гречанінов, В. Ф., & Бєгун, В. В. (2015). Управління безпекою в епоху інформаційного суспільства. *Вісник НАН України*, (10), С. 34-41.

52. Кабінет Міністрів України. (2019). *Питання Міністерства цифрової трансформації* (Постанова №856). URL: https://www.kmu.gov.ua/npas/pitannya-ministerstva-cifrovoyi-t180919.

53. Кононенко, Ж., Карнаухова, Г., & Балюк, О. (2023). Цифровізація підприємницької діяльності: значення та вплив. *Проблеми сучасних трансформацій: Серія економіка та управління*, Вересень. DOI: https://doi.org/10.54929/2786-5738-2023-9-04-08.

54. Majer, K., Cesky, L., & Janícek, F. (2018). Digitalization in Power Distribution Systems: Digital switchgear solution. In *Proceedings of the 14th International Scientific Conference on Energy Ecology Economy* (pp. 129-132).

55. Loukkalahti, M., et al. (2018). Digitalization in Power Distribution Systems: The Kalasatama Smart Grid Project. In *Proceedings of the CIGRE SESSION 2018, B5 Protection and Automation*. URL: https://www.researchgate.net/publication/329830322_Digitalization_in_Power_Di stribution_Systems_the_Kalasatama_Smart_Grid_Project.

56. Бойко, О., Парфененко, Ю., Івашова, Н., & Рикун, В. (2024). Мікросервіс підтримки прийняття рішень щодо режимів роботи енергетичної мікромережі з відновлюваними джерелами енергії. *Таврійський науковий вісник. Серія Технічні науки*, (1), 27-35. DOI: https://doi.org/10.32782/tnv-tech.2024.1.3.

57. Бунда, О., & Матюха, М. (2023). Цифровізація системи бухгалтерського обліку підприємства. *Журнал стратегічних економічних досліджень*, (6(17)). DOI: https://doi.org/10.30857/2786-5398.2023.6.14.

58. Безручук, С. Л., & Грабчук, І. Л. (2021). Основні концепції впливу цифровізації на якість бухгалтерського обліку. *Економіка, управління та адміністрування*, (4(98)), 69-74. DOI: https://doi.org/10.26642/ema-2021-4(98)-69-74.

59. Дія це. Держава, що допомагає, а не заважає. URL: https://plan2.diia.gov.ua.

60. Huang, L. D., Zhuang, W. J., Sun, M. Y., & Zhang, H. (2020). Research and application of microservice in power grid dispatching control system. In *Proceedings of the 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC 2020)* (pp. 1895-1899). DOI: https://doi.org/10.1109/ITNEC48623.2020.9084931.

61. Zimmermann, O. (2016). Microservices tenets: Agile approach to service development and deployment. *Computer Science – Research and Development*, 32, 301-310. DOI: https://doi.org/10.1007/s00450-016-0337-0.

62. Enge, A., Satybaldy, A., & Nowostawski, M. (2022). An offline mobile access control system based on self-sovereign identity standards. *Computer Networks*, 219, 109434. DOI: https://doi.org/10.1016/j.comnet.2022.109434.

63. Iskhakov, A., et al. (2022). Authentication model for mobile access subjects. *IFAC-PapersOnLine*, 55(9), 222-226. DOI: https://doi.org/10.1016/j.ifacol.2022.07.039.

64. Mühle, A., et al. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30, pp. 80-86. DOI: https://doi.org/10.1016/j.cosrev.2018.10.002.

65. Zheng, L., & Yao, J. G. (2016). The construction of power cloud integrated with heterogeneous application service systems. In *Proceedings of the 2016 International Conference on Communications, Information Management and Network Security* (Vol. 47, pp. 345-348). ISSN 2352-538X.

66. Гулак, Г., Жданова, Ю., Складанний, П., Гулак, Є., & Корнієць, В. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*, 1(17), С. 145-158. DOI: https://doi.org/10.28925/2663-4023.2022.17.145158.

67. Дереговський, В. В., Кафтанатіна, О. А., Кордюков, П. Л., Меньшенін, Є. А., & Гулак, Є. Г. (2021). Розробка математичної моделі впливу радіаційно небезпечних об'єктів на довкілля при пожежі. *Математичні машини і системи*, (4), 99-111. DOI: https://doi.org/10.34121/1028-9763-2021-4-99-111.

68. ДСТУ ISO/IEC 38500:2016 Інформаційні технології. Управління IT в організації (ISO/IEC 38500:2015, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=69054.

69. Чат-бот ДТЕК Київські регіональні електромережі — зручний сервіс передачі показів електролічильника. (2023). URL: https://www.dtek-krem.com.ua/ua/news/chat-bot-dtek-kijivski-regionalni-elektromerezhi-zruchniy-servis-peredachi-pokaziv-elektrolichilnika.

70. Підсумки року українсько-російської кібервійни — які правила слід винести бізнесу та як захистити дані. (2023). URL: https://gigatrans.ua/ua/news/itogi-goda-ukrainsko-rossiyskoy-kibervoynu-kakie-pravila-sleduet-vunesti-biznesu-i-kak-zash-itit-dannue.

71. Російські хакери координують дії з військовими та посилюють атаки напередодні зими. Як Україна протистоїть кібератакам на

енергосистему. (2023). URL: https://forbes.ua/ru/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energosistemu-08112023-17242.

72. Куваєв, В., та ін. (2024). Інтерфейс програмного супроводження складних інформаційно-керуючих систем автоматизації, критичних до режиму реального часу. *Information Technology Computer Science Software Engineering and Cyber Security*, (1), С. 41-49. DOI: https://doi.org/10.32782/IT/2024-1-6.

73. Адміністрація ДССЗЗІ України. (2007). *Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації* (Наказ №141).

74. ДСТУ ISO/IEC 27001:2015. (2016). Національний стандарт України. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. Київ: ДП «УкрНДНЦ».

75. Гончар, С. (2019). Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури. Київ: Альфа реклама.

76. Суходоля, О. М., та ін. (2023). *Енергетична безпека України: перспективна модель управління ризиками* (152 с.). НІСД. DOI: https://doi.org/10.53679/NISS-book.2023.01.

77. Zimmerman, C. (2014). *Ten strategies of a world-class cybersecurity operations center*. MITRE Corporate Communications and Public Affairs.

78. Bassey, C., et al. (2024). Building a scalable security operations center: A focus on open-source tools. *Journal of Engineering Research and Reports*, 26(7), 196-209. DOI: https://doi.org/10.9734/jerr/2024/v26i71203.

79. Falé, P., Reis, L., & Almeida, R. (2022). Cybersecurity – Security Operations Center. In *Proceedings of the Sixth International Scientific Conference ITEMA* (pp. 99-103). DOI: https://doi.org/10.31410/ITEMA.2022.99.

80. Черненко, Р. (2023). Оцінка продуктивності алгоритмів легкої криптографії на обмежених 8-бітних пристроях. *Кібербезпека: освіта, наука, техніка*, 1(21). DOI: https://doi.org/10.28925/2663-4023.2023.21.273285.

81. Гулак, Г. М., Скітер, І. С., & Гулак, Є. Г. (2021). Методологічні засади створення та функціонування центру кібербезпеки інформаційної інфраструктури об'єктів ядерної енергетики. *Кібербезпека: освіта, наука, техніка*, 4(12), 172–186. DOI: https://doi.org/10.28925/2663-4023.2021.12.172186.

82. Ayodeji, A., et al. (2023). Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors. *Progress in Nuclear Energy*, 161, 104738. DOI: https://doi.org/10.1016/j.pnucene.2023.104738.

83. Носовський, А. В. (2021). Науково-технічний супровід робіт з подолання наслідків чорнобильської катастрофи. *Вісник Національної академії наук України*, (7), 32–36.

84. International Atomic Energy Agency. (2016). *Conducting Computer Security Assessments at Nuclear Facilities* (p. 64). IAEA. ISBN 978-92-0-104616-1.

85. Park, J. K., Suh, Y. S., & Park, C. (2016). Implementation of cyber security for safety systems of nuclear facilities. *Progress in Nuclear Energy*, 88, pp. 88–94.

86. Jung, D., et al. (2023). Cyber Security Controls in Nuclear Power Plant by Technical Assessment Methodology. *IEEE Access*, 11, 15229–15241. DOI: https://doi.org/10.1109/ACCESS.2023.3244991.

87. Погосов, О. Ю., & Дерев'янко, О. В. (2017). Фізичний захист АЕС та інформаційна безпека як необхідні умови зниження ризиків ядерних і радіаційних аварій. *Ядерна та радіаційна безпека*, 3(75), 50–55.

88. Чумак, Д. В., & Клевцов, О. Л. (2015). Комп'ютерна безпека на ядерних об'єктах в Україні: області взаємодії між ядерною безпекою та захищеністю. *Ядерна та радіаційна безпека*, 3(67), 60–64.

89. International Electrotechnical Commission. (2009). *Nuclear power plants — Instrumentation and control important to safety — Classification of instrumentation and control functions* (IEC 61226).

90. International Electrotechnical Commission. (2014). *Nuclear power plants — Instrumentation and control systems — Requirements for security programmes for computer-based system* (IEC 62645).

91. Energy Expert Cyber Security Platform (EECSP). (2017). *Cyber Security in the Energy Sector. Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector (E03341).*

92. ДП «УкрНДНЦ». (2003). *ДСТУ ISO/TR 13335-2:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 2. Керування та планування безпеки IT.*

93. Turner, P. L., Adams, S. S., & Hendrickson, S. M. (2017). Enhancing power plant safety through simulated cyber events. In *American Nuclear Society's (ANS) 10th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies* (pp. 301–313).

94. ДП «УкрНДНЦ». (2018). *ДСТУ ISO/IEC 27032:2016. Національний стандарт України. Інформаційні технології. Методи захисту. Настанови щодо кіберзахисту.*

95. Fichtner, J., & Persy, C. (1992). Concept of a Security Control Center. *IFAC Proceedings Volumes*, 25(30), 267-271.

96. Overview of Security Operations Center Technologies. (2015). *SOC Conceptual Architecture*. Cisco Press. URL: https://www.ciscopress.com/articles/article.asp?p=2455014&seqNum=7.

97. Lowler, J. P., & Howell-Barber, H. (2019). *Service-Oriented Architecture: SOA Strategy, Methodology, and Technology*. CRC Press Taylor & Francis. ISBN 978-0-367-38823-2.

98. Morozov, A., Hrebennyk, A., Trunova, E., Skiter, I., & Hulak, E. (2021). Design of Industry Centers of Cyber Security of Facilities of Critical

Infrastructure. In *Cybersecurity Providing in Information and Telecommunication Systems CPITS-II-2021* (Vol. 3187, pp. 27–37). ISSN 1613-0073.

99. 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, pp. 107–117). ISSN 1613-0073.

100. Hulak, H., Skladannyi, P., Sokolov, V., Hulak, E., & Korniiets, V. (2022). Dynamic Model of Guarantee Capacity and Cyber Security Management in the Critical Automated System. In *2nd International Conference on Conflict Management in Global Information Networks* (Vol. 3530, pp. 102–111). ISSN 1613-0073.

101. Vielberth, M. (2021). Security Information and Event Management (SIEM). In *Encyclopedia of Cryptography, Security and Privacy*. Springer. DOI: https://doi.org/10.1007/978-3-642-27739-9_1681-1.

102. Жилін, А., Ніколаєнко, Б., & Бакалинський, О. (2021). Підвищення захищеності державних інформаційних ресурсів за рахунок застосування платформи Threat Intelligence. *Захист інформації*, 23(3), 136–146.

103. MITRE ATT&CK. (2021). URL: https://attack.mitre.org/.

104. Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *The Journal of Strategic Studies*, 38(1–2), 4–37.

105. Borzenkowa, S., et al. (2010). Upravlenie systemoju zastchity informacii na osnovi signaturnykh modeley. *Izvestiya TulGU, Tekhnichni nauky*, 2(2), 200–205.

106. Borzenkowa, S., & Chechuga, O. (2011). Koncepciya ispolzovaniya diskretnych sytuaciynych modeley v systemakh upravleniya zastchitoy informacii. *Izvestiya TulGU, Tekhnichni nauky*, 6(2), 328–336.

107. Borzenkowa, S., & Chechuga, O. (2013). Model prinyatiya resheniy pri upravlenii systemoyu zastchity informacii. *Izvestiya TulGU, Tekhnichni nauky*, 3, 471–478.

108. Azhmuchamedov, I. M. (2009). Matematicheskaya model kompleksnoy bezopasnosti komp'yuternykh system i setey na osnovi ekcpertnykh suzhdeniy. *Infokommunikacionnye tekhnologii*, 7(4), 103-107.

109. Azhmuchamedov, I. M. (2012). Dinamicheskay nechetkay kognitivnaya model ocenki urovnya bezopasnosti informacionnych aktivov VUZa. *Vestnik AGTU. Ser.: Upravlenie, vychislitelnay tekhnika I informatika*, (2), 137-141.

110. Westphall, C., et al. (2011). Management and Security for Grid, Cloud and Cognitive Networks. *Revista de Sistemas de Informação da FSM*, 8, 8-21.

111. Довгань, О. Д., та ін. (2012). Методологія захисту інформації. Наук.-ви. Центр НА СБ України.

112. Anthony, R. (1965). *Planning and Control Systems: A Framework for Analysis*. Division of Research, Graduate School of Business Administration, Harvard University.

113. Gorry, G. A., & Scott-Morton, M. S. (1971). A framework for management information systems. *Sloan Management Review*, 13, 21-36.

114. NATO Headquarters Supreme Allied Commander Transformation. (2016). Cybersecurity. A Generic Reference curriculum. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-curriculum.pdf.

115. Parmenter, D. (2019). *Key Performance Indicators – Developing, Implementing, and Using Winning KPIs* (4th ed.). John Wiley & Sons.

116. НД ТЗІ 2.5-004-99. (1999). Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf.

117. Гулак, Г. (2017). Механізми забезпечення безпеки програмних засобів захисту інформації. У *Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез*, 66-72.

118. НД ТЗІ 2.5-005-99. (1999). Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від

несанкціонованого доступу. URL: https://tzi.com.ua/downloads/2.5-005%20-99.pdf.

119. Akritas, A. G. (1989). *Elements of Computer Algebra With Applications* (1st ed.). Wiley-Interscience.

120. НД ТЗІ 1.1-003-99. (1999). Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.ua/assets/files/1.1_003_99.pdf.

121. Скітер, І. (2021). Модель оцінки рівня культури кібербезпеки в інформаційній системі. *Кібербезпека: освіта, наука, техніка*, 1(13), 158-169. DOI: https://doi.org/10.28925/2663-4023.2021.13.158169.

122. European Union Agency for Network and Information Security (ENISA). (2017). *Cyber Security Culture in Organisations*. URL: https://www.enisa.europa.eu.

123. Leenen, L., & van Vuuren. (2019). Framework for the Cultivation of a Military Cybersecurity Culture. *14th International Conference on Cyber Warfare and Security (ICCWS)*, 212-220.

124. Turing, A. (1950). Computing Machinery and Intelligence. *Mind*, 59(236), 433-460.

125. Salvendy, G., & Karwowski, W. (Eds.). (2021). *Handbook of Human Factors and Ergonomics* (5th ed.). Wiley.

126. Patrascu, P. (2019). Promoting Cybersecurity Culture through Education. *15th International Scientific Conference on eLearning and Software for Education (eLSE)*, 2, 273-279.

127. Stackpole, B. (2022). How to build a culture of cybersecurity. *MIT Sloan Management Review*. URL: https://mitsloan.mit.edu/ideas-made-to-matter/how-to-build-a-culture-cybersecurity.

128. European Commission, Directorate-General for Education, Youth, Sport and Culture. (2017). *ECTS Users' Guide 2015*. URL: https://data.europa.eu/doi/10.2766/87192.

129. Кабінет Міністрів України. (2020). Деякі питання об'єктів критичної інфраструктури. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text.

130. Grechaninov, V., et al. (2022). Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center. *Proceedings of the Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things*, 3149, 107-117.

131. Верховна Рада України. (1994). Закон України Про захист інформації в інформаційно-комунікаційних системах. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

132. Xiong, W., & Lagerstrom, R. (2019). Threat modeling - A systematic literature review. *Computers & Security*, 84, 53-69.

133. Xiong, W., et al. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, 21(2), 154-177. DOI: https://doi.org/10.1007/s10270-021-00898-7.

134. Abdunabi, R. (2013). An access control framework for mobile applications. Dissertation, Colorado State University. URL: https://mountainscholar.org/handle/10217/78814.

135. Хлапонін, Ю., та ін. (2022). Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка*, 3(15), 124-134. DOI: https://doi.org/10.28925/2663-4023.2022.15.1241341.

136. Al Kukhun, D. (2012). *Steps towards adaptive situation and context-aware access: A contribution to the extension of access control mechanisms within Pervasive Information Systems* (Doctoral thesis, Institut de Recherche en Informatique de Toulouse – UMR 5505 CNRS). URL: http://www.theses.fr/2012TOU30072.

137. National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity (version 1.1)*. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

138. American National Standards Institute. (2004). *American National Standard for Information Technology – Role Based Access Control (ANSI INCITS 359-2004)*. URL: https://www.cs.purdue.edu/homes/ninghui/readings/Access-Control/ANSI+INCITS+359-2004.pdf.

139. Chadov, A. (2018). Вироблення вимог до децентралізованої системи розмежування доступу. *Вопросы защиты информации*, (3), 13-16.

140. Chadov, A. (2020). Описание формальной модели децентрализованной системы разграничения доступа. У *Комплексная защита информации: материалы 25 научно-практической конференции, 15–17 сентября 2020* (с. 115-121). URL: https://www.okbsapr.ru/library/publications/opisanie-formalnoy-modeli-detsentralizovannoy-sistemy-razgranicheniya-dostupa1/.

141. Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal, 28*(4), 656-715. DOI: https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.

142. Grusho, A., & Timonina, E. (1996). *Теоретические основы защиты информации*. М.: «Яхтсмен».

143. Горбенко, І. Д., & Горбенко, Ю. І. (2012). *Прикладна криптологія: Теорія. Практика. Застосування* (Монографія). Харків: ФОРТ.

144. Harna, L., et al. (2016). Realizing secret sharing with general access structure. *Information Sciences, 367–368*, 209-220.

145. Cramér, H. (1999). *Mathematical Methods of Statistics*. Princeton University Press.

146. Fomichev, V. M. (2010). *Методы дискретной математики в криптологии*. М.: МИФИ.

147. Гулак, Г., & Ковальчук, Л. (2001). Різні підходи до визначення випадкових послідовностей. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, (3), 127-133.

148. Oliynykov, R., et al. (2015). A New Encryption Standard of Ukraine: The Kalyna Block Cipher. *IACR Cryptol ePrint Archive*. URL: https://eprint.iacr.org/2015/650.

149. Biryukov, A., & Khovratovich, D. (2009). Related-key Cryptanalysis of the Full AES-192 and AES-256. У *Advances in Cryptology – ASIACRYPT 2009* (Vol. 5912). URL: https://doi.org/10.1007/978-3-642-10366-7_1.

150. НД ТЗІ 3.7-003-2005. (2005). *Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі*. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf.

151. European Telecommunications Standards Institute (ETSI). (1994). *Digital cellular telecommunications system (Phase 2+); Alphabets and language-specific information (GSM 03.38)*. URL: https://www.etsi.org/deliver/etsi_300/628_300629/300628/01_60/.

152. European Telecommunications Standards Institute (ETSI). (1996). *European digital cellular telecommunication system (Phase 2); Technical realization of the Short Message Service (SMS) Point to Point (PP) (GSM 03.40)*.

153. Williams, M. (2020). *Secure Messaging Apps Comparison*. URL: https://www.securemessagingapps.com.

154. Rosenfeld, A., Sina, S., Sarne, D., Kraus, S., & Avidov, O. (2018). WhatsApp usage patterns and prediction of demographic characteristics without access to message content. *Demographic Research, 39*, 647-670. DOI: https://doi.org/10.4054/DemRes.2018.39.24.

155. Kwak, M., & Cho, Y. (2021). A novel video steganography-based botnet communication model in Telegram SNS messenger. *Symmetry, 13*(1), 84. DOI: https://doi.org/10.3390/sym13010084.

156. Trabelsi, Z., et al. (2006). Traceroute based IP channel for sending hidden short messages. У *Proceedings of the Advances in Information and Computer Security (IWSEC)* (с. 421-436).

157. Zhang, T., Sun, Z. X., & Jin, Y. C. (2015). A lightweight encoding mechanism for encrypted user notification on mobile device in power grid system. У *Proceedings of the International Conference on Computer Information Systems and Industrial Applications (CISIA)* (с. 513-515).

158. Karale, S. N., Pendke, K., & Dahiwale, P. (2015). The survey of various techniques & algorithms for SMS security. У *Proceedings of the International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)* (с. 1-6). IEEE. DOI: https://doi.org/10.1109/ICIIECS.2015.7192907.

159. Makala, R., Bezawada, V., & Ponnaboyina, R. (2017). A fast encryption and compression technique on SMS data. У *Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (с. 1213-1217). DOI: https://doi.org/10.1109/WiSPNET.2017.8299947.

160. Aung, T. M., Myint, K. H., & Ni Hla, N. (2019). A data confidentiality approach to SMS on Android. У *Proceedings of the 1st International Conference on Intelligent Computing and Optimization (ICO 2019)* (с. 505-514). DOI: https://doi.org/10.1007/978-3-030-36668-9_48.

161. Imperva. (2015). *Attacking SSL when using RC4*. URL: https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf.

162. Ekdahl, P., & Johanson, T. (2003). Another attack on A5/1. *IEEE Transactions on Information Theory, 49*(1), 284-289. DOI: https://doi.org/10.1109/TIT.2002.805078.

163. Pan, J., Ding, Q., & Qi, N. (2012). The research of chaos-based SMS encryption in mobile phones. У *Proceedings of the 2nd International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)* (с. 501-504). DOI: https://doi.org/10.1109/IMCCC.2012.137.

164. Pan, J., Qi, N., Xue, B. B., & Ding, Q. (2012). Field programmable gate array-based chaotic encryption system design and hardware realization of cell phone short message. *Acta Physica Sinica, 61*(18).

165. Корнієць, В., & Черненко, Р. (2023). Модифікація криптографічного алгоритму A5/1 для забезпечення комунікацій пристроїв IoT. *Кібербезпека: освіта, наука, техніка, 4*(20), 253-271. DOI: https://doi.org/10.28925/2663-4023.2023.20.253271.

166. Husein, M. S., Harahab, A. M., & Aisyah, S. (2018). SMS security system on mobile devices using tiny encryption algorithm. У *Proceedings of the International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT)* (с. 012037). *Journal of Physics: Conference Series, 1007*, 012037. DOI: https://doi.org/10.1088/1742-6596/1007/1/012037.

167. Lu, E. H., Huang, K. T., & Chiu, J. H. (2016). Word-based AES encryption without data expansion. *Journal of Information Science and Engineering, 32*(4), 849-861.

168. Ahamed, B. B., & Krishnamoorthy, M. (2020). SMS encryption and decryption using modified Vigenere cipher algorithm. *Journal of the Operations Research Society of China*. DOI: https://doi.org/10.1007/s40305-020-00320-x.

169. Гулак, Г. М., & Складанний, П. М. (2017). Забезпечення гарантоздатності автоматизованих систем управління та передачі даних безпілотних літальних апаратів. *Математичні машини та системи*, (3), 154–161.

170. Grushevsky, Y. L., Elmasry, G. F., Argentieri, S. R., & Lussier, R. (2006). Adaptive RS code for message delivery over encrypted military wireless networks. In *MILCOM IEEE Military Communications Conference* (pp. 1–5). DOI: https://doi.org/10.1109/MILCOM.2006.302323.

171. Asbullah, M. A., & Ariffin, M. K. (2012). A proposed CCA-secure encryption on an ElGamal variant. In *7th International Conference on Computing and Convergence Technology (ICCCT2012)* (pp. 499–503).

172. Гулак, Г. М., Мухачов, В. А., Хорошко, В. О., & Яремчук, Ю. Є. (2011). *Основи криптографічного захисту інформації.* Вінниця: Вид-во ВНТУ.

173. Bresson, E., Chevassut, O., & Pointcheval, D. (2004). New security results on encrypted key exchange. In *7th International Workshop on Theory and Practice in Public Key Cryptography 2004 | Public Key Cryptography - PKC 2004, Proceedings* (Vol. 2947, pp. 145–158).

174. IEEE. (2000). *IEEE Standard Specifications for Public-Key Cryptography* (IEEE Std 1363-2000).

175. Mishra, P., Renuka, & Verma, V. (2020). Identity-based broadcast encryption scheme with shorter decryption keys for open networks. *Wireless Personal Communications, 115*(2), 961–969.

176. Boneh, D., & Franklin, M. (2003). Identity-based encryption from the Weil pairing. *SIAM Journal of Computing, 32*(3), 586–615.

177. **.** Schneier, B., & Hall, C. (1997). An improved e-mail security protocol. In *13th Annual Computer Security Applications Conference Proceedings* (pp. 227–230).

178. Rosenfeld, A., Sina, S., Sarne, D., Avidov, O., & Kraus, S. WhatsApp usage patterns and prediction models. Retrieved from URL: https://www.researchgate.net/publication/299487660.

179. Yaglom, A. M., & Yaglom, I. M. (2007). *Probability and information* (512 p.). Москва.

180. Srivastava, V., & Singh, M. (2020). PHINC: A parallel Hinglish social media code-mixed corpus for machine translation. In *Proceedings of the Sixth Workshop on Noisy User-generated Text (W-NUT 2020)*. DOI: https://doi.org/10.18653/v1/2020.wnut-1.7.

181. Sobkowicz, P., Thelwall, M., Buckley, K., Paltoglou, G., & Sobkowicz, A. (2013). Lognormal distributions of user post lengths in Internet discussions – A consequence of the Weber-Fechner law? *EPJ Data Science, 2*(1). URL: https://www.researchgate.net/publication/257868097_Lognormal_distributions_of_user_post_lengths_in_Internet_discussions_-_a_consequence_of_the-Weber-Fechner_law.

182. Kekre, H. B., & Saxena, C. L. (1979). An estimate of the distribution of message lengths in overseas communications. *Computers & Electrical Engineering, 6*(2), 79–92.

183. Paulson, D., & Wand, Y. (1992). An automated approach to information-systems decomposition. *IEEE Transactions on Software Engineering, 18*(3), 174–189. DOI: https://doi.org/10.1109/32.126767.

184. Chiriac, N., et al. (2011). Three approaches to complex system decomposition. In *Proceedings of the 13th International DSM Conference* (pp. 3–15).

185. Pancerz, K., & Suraj, Z. (2013). A rough set approach to information systems decomposition. *Fundamenta Informaticae, 127*(1–4), 257–272.

186. Бурячок, В. Л., та ін. (2017). Швидкий алгоритм генерації підстановок багато алфавітної заміни. *Захист інформації, 2*, 173–177.

187. Корченко, О. Г. (2004). *Системи захисту інформації: Монографія.* Київ: НАУ.

188. 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 – 2024* (pp. 228–230). Київ.

189. 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.

190. Постанова КМ України від 21.10.2020 р. № 991 Про затвердження Технічного регламенту засобів криптографічного захисту інформації. URL: https://zakon.rada.gov.ua/laws/show/991-2020-п#Text.

191. Бурячок, В. Л., та ін. (2011). Метод оцінювання ефективності кібернетичного озброєння з подолання засобів криптографічного захисту

інформації. *Інформаційна безпека людини, суспільства, держави, 1*(8), 100–106.

192. Гулак, Г. М. (2018). Оцінка інженерно криптографічних якостей під час тематичних досліджень криптосистем. *Тези 13 Міжнар. наук.-практ. конференції «Математичне та імітаційне моделювання систем МОДС 2018»* (pp. 326–330). Чернігів: ЧНТУ.

193. Mpekoa, N. (2023). An analysis of cybersecurity architectures. In *Proceedings of the 19th International Conference on Cyber Warfare and Security (ICCWS 2024)* (pp. 200–207).

194. Hallman, R., et al. (2020). Return on cybersecurity investment in operational technology systems: Quantifying the value that cybersecurity technologies provide after integration. In *5th International Conference on Complexity, Future Information Systems and Risk*. DOI: https://doi.org/10.5220/0009416200430052.

195. 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. DOI: https://doi.org/10.4018/IJOCI.2021040105.

196. Закон України Про інформацію від 2 жовтня 1992 року № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12?find=1&text=критична#Text.

197. Secure Messaging Apps Comparison. URL: https://www.securemessagingapps.com.

198. Гулак, Г.М., Гулак, Є.Г., Корнієць, В.А. (2023). Безпека шифрування коротких повідомлень в інформаційно-комунікаційних системах об'єктів критичної інфраструктури. *Актуальні проблеми управління інформаційною безпекою держави*. Київ. 260–262.

199. Гулак, Г. М., Скітер, І. С., Гулак, Є. Г., Цирканюк, Д. А. (2023). Базові засади побудови центру кібербезпеки об`єктів ядерної енергетики.

Актуальні проблеми управління інформаційною безпекою держави. Київ, 2023. 262–266.

200. Hulak, H., Grechaninov, V., Hulak, E., Skladannyi, P., Sokolov, V. Decentralized Access Demarcation System Construction in Situational Center Network. *Cybersecurity Providing in Information and telecommunication Systems (CPITS-II-2021):* October 26, 2021, Kyiv, Ukraine, 2021. Vol. 3188. pp. 197–206. ISSN: 1613-0073.

ДОДАТКИ

Додаток А

Акти та довідки впровадження результатів дисертаційного дослідження

ЗАТВЕРДЖУЮ
В.о. директора ІПММС НАН України
д.ф.-м.н., професор

Віталій КЛИМЕНКО
«__» вересня 2024 року

АКТ
про впровадження результатів дисертаційного дослідження
ГУЛАКА Євгена Геннадійовича

Даним актом засвідчується, що нижченаведені наукові положення, а саме:

методика декомпозиції складної інформаційної системи критичної інфраструктури, оцінки характеристик підсистеми криптографічного захисту та їх раціонального визначення;

вдосконалена модель підсистеми криптографічного захисту інформації, що враховує можливість взаємодії інформаційних підсистем з різними рівнями щодо забезпечення безпеки інформації та запропоновано метод оцінки безпеки шифрування коротких повідомлень в мобільних компонентах мереж;

модель розмежування доступу в мережі на основі часткової децентралізації підсистеми управління доступом;

які розроблені Гулаком Є.Г., використані в Інституті проблем математичних машин і систем Національної академії наук України під час виконання науково-дослідних робіт шифр «Ситуаційне управління» (№ д.р. 0122Г201115), шифр «ІПММС-2021» (№ д.р. 0121U000107) в плані реалізації завдань підвищення рівня кіберзахисту та гарантоздатності державних об'єктів критичної інфраструктури.

Отримані Гулаком Є.Г. результати були використані на етапах проєктування для методологічного забезпечення процесів побудови систем кібербезпеки та гарантоздатності корпоративних мереж, обґрунтування технічних рішень, а також раціонального застосування засобів кіберзахисту та управління ними в контексті забезпечення конфіденційності та цілісності державних інформаційних ресурсів.

Запропоновані автором рішення дозволяють підвищити ефективність функціонування систем кібербезпеки в складних корпоративних мережах

Завідувач відділу № 220 ІПММС НАН України
к.т.н., с.д. Віктор ГРЕЧАНІНОВ

АКТ

про впровадження результатів дисертаційного дослідження
ГУЛАКА Євгена Геннадійовича

Даним актом засвідчується, що нижчеперелічені наукові положення, а саме:

методика декомпозиції складної інформаційної системи критичної інфраструктури, оцінки характеристик підсистеми криптографічного захисту та їх раціонального визначення;

вдосконалена модель підсистеми криптографічного захисту інформації, що враховує можливість взаємодії інформаційних підсистем з різними рівнями щодо забезпечення безпеки інформації та запропоновано метод оцінки безпеки шифрування коротких повідомлень в мобільних компонентах мереж;

модель розмежування доступу в мережі на основі часткової децентралізації підсистеми управління доступом,

що розроблені Гулаком Є.Г., будуть використані під час виконання робіт по підвищенню рівня кіберзахисту та кіберстійкості інформаційної інфраструктури Інституту проблем безпеки атомних електростанцій Національної Академії наук України.

Отримані Гулаком Є.Г. результати будуть використані для прийняття обґрунтованих технічних рішень та методологічного забезпечення побудови системи кібербезпеки корпоративної мережі, а також раціонального застосування засобів кіберзахисту та управління ними в контексті забезпечення конфіденційності та цілісності інформації, що циркулює в мережі в умовах кібератак та функціональної безпеки і живучості самої системи.

Запропоновані автором рішення дозволяють підвищити ефективність функціонування системи кібербезпеки корпоративної мережі Інституту проблем безпеки атомних електростанцій Національної Академії наук України.

В подальшому їх буде використано для вдосконалення кіберзахисту критичної інформаційної інфраструктури.

Т.в.о. зам. директора
Інституту проблем безпеки атомних
електростанцій
Національної Академії наук України Віктор Краснов

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА

ФАКУЛЬТЕТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
ТА МАТЕМАТИКИ
вул. Левка Лук'яненка, 13-Б, м. Київ, Україна, 04207
Тел.: +380 44 428-34-14
fitm.kubg.edu.ua, fitm@kubg.edu.ua

BORYS GRINCHENKO
KYIV METROPOLITAN UNIVERSITY

FACULTY
OF INFORMATION TECHNOLOGIES
AND MATHEMATICS
13-B Levka Lukianenka St, Kyiv, Ukraine, 04207
Tel.: +380 44 428-34-14
fitm.kubg.edu.ua, fitm@kubg.edu.ua

19.08.2024 № 18

АКТ

про впровадження результатів дисертаційного дослідження
Гулака Євгена Геннадійовича
на тему «Моделі та методи забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору», поданої на здобуття наукового ступеня доктора філософії зі спеціальності 122 Комп'ютерні науки

Цим Актом, ґрунтуючись на рішенні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка, засвідчуємо, що нижчеперелічені наукові положення, а саме:

- вперше на основі формування класів еквівалентності запропонована методика декомпозиції складних систем, що підлягають кіберзахисту, яка враховує можливість інформаційного обміну між підсистемами з різними вимогами до захисту інформації з обмеженим доступом.
- вдосконалена модель побудови корпоративного центру кібербезпеки енергетичного сектору на основі сервіс орієнтованої архітектури з визначеною бізнес логікою та відповідним набором функцій що забезпечуватиме динамічне оброблення кіберінцидентів у реальному часі. Вдосконалена модель відповідає сучасним викликам безпеці та ураховує специфіку завдань і функцій ОЕС-У.
- вдосконалена модель побудови децентралізованої системи розмежування доступу в мережі центру кібербезпеки на основі оригінальної методики розподілу секрету. Запропонована модель припускає її масштабування та мінімізує ризик несанкціонованого доступу до інформаційних ресурсів
- подальшого розвитку набула модель побудови підсистеми криптографічного захисту інформації, що забезпечуватиме можливість двоконтурного шифрування для розмежування доступу в децентралізованій системі розмежування доступу до інформаційних ресурсів, розроблені та обґрунтовані рекомендації, щодо підвищення безпеки криптографічного захисту інформації коротких службових повідомлень,

Розроблені особисто Гулаком Євгеном Геннадійовичем у ході проведення

ним дисертаційних досліджень та отримали високу оцінку при обговоренні на засіданнях кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.

Зазначені наукові результати:

по-перше, впроваджені в освітній процес кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка у робочих програмах навчальних дисциплін спеціальності 125 Кібербезпека за захист інформації першого (бакалаврського), другого (магістерського) та третього (освітньо-наукового) рівнів вищої освіти;

по-друге, впроваджені в програмно-апаратне забезпечення лабораторій безпеки інформаційних активів, антивірусного захисту інформації, систем технічного та криптографічного захисту інформації.

Дослідження Гулака Євгена Геннадійовича відповідає всім вимогам до організації наукового пошуку та дає позитивний результат у практичному застосуванні.

Декан
Факультету інформаційних технологій та математики
кандидат фізико-математичних наук,
старший науковий співробітник Оксана ЛИТВИН

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА * ЄДРПОУ 02807965 * ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА МАТЕМАТИКИ * УКРАЇНА *

Додаток Б

Вихідний код програмного шифратора A5-128 на мові C#

```
using System;
using System.Collections;
using System.Collections.Generic;
using System.IO;
using System.Text;
using UnityEngine;
using UnityEngine.UI;
using UnityEngine.Android;
using System.Linq;

public class A5m128 : MonoBehaviour
{
    private string path;
    public Text textToShow;
    public Text result;
    public InputField inputField;
    A5128LFSR a5;
    public ToggleGroup saveAs;
    static byte[] X = new byte[256] { 184,  222,   86,   80,  104,
31,   61,  146,  124,  100,  220,  120,  165,   11,
                137,  166,   15,  127, 72,  192,   42,   54,  205,
161,  157,  221,  129,   24,   23,  234,  253,   55,
                39,   52,   58,   75, 59,   28,  245,   92,    5,
2,  123,  206,  132,  145,  114,   40,   36,  110,
                136,    1,  144,  130, 190,   87,  180,  105,  209,
117,  201,  247,    6,  229,  178,  133,  147,  21,
                179,  174,  216,  171, 18,   56,  255,  202,   17,
22,  199,  189,  140,   45,  250,  215,   19,    7,
                176,   16,   76, 164, 115,   14,  243,   27,   43,
128,  228,  170,  175,  217,   64,    4,   93,  79,
                155,  102,  143,  235, 70,   81,  194,  134,   78,
32,   68,   74,   85,   95,  108,  232,   35,   82,
                156,   73,    3,   41, 238,  177,  214,  158,  241,
20,  242,  230,   13,   71,  150,  239,   83,   67,
                163,  48,  112,  113, 46,  237,   89,  154,  182,
60,  139,  66,  187,   51,  107,  227,   97,  109,
                50,  172,  248,   88, 8,  188,  168,  204,  249, 244,
236,   49,   10,  252,   77,  213,  0,  135,   69,
                116,  186,  101, 191,  208,   33,   62,  103,  153,
183,  122,  218,   47,   90,   98,  233,  251,   12,
                63,   44, 111, 224,   26,   29,  149,  151,  138,
254,   34,  125,   30,   25,  219,  173,  126,    9,
                131,   91,   65, 225,  106,  195,  207,  198, 118,
226,  141,  169,  142,  197,  203,  160,  181,  119,
                37,  223,  240, 196,  148,   57,   38,   96,   53,
167,  159,   94,  193,  231,  211,  121, 210,  200,
                152,  246,  162,   84, 212,   99,  185 };
    static byte[] reversX = new byte[256];
    // Start is called before the first frame update
    public void setPath(string p) {
        for (int i = 0; i < X.Length; i++)
        {
            reversX[X[i]] = (byte)i;
        }
        path = p;
    }
    public void setKey() {
        a5.setKey(inputField.text);
```

```
    }
    public void openRead() {
        try
        {
            string tUseRead = File.ReadAllText(path); //ReadAllBytes
            textToShow.text = tUseRead;
        }
        catch (Exception e)
        {
            Debug.Log("cant open");
            //throw;
        }
    }
    public void encrypt() {
        a5 = new A5128LFSR();
        setKey();
        byte[] M = File.ReadAllBytes(path);
        uint[] enc = new uint[(uint)Math.Ceiling((double)M.Length /
4)];
        if (enc.Length % 4 == 0)
        {
            for (int i = 0; i < enc.Length; i++)
            {
                enc[i] = (uint)((BitConverter.ToUInt32(M, i * 4) +
a5.getKeyWord()) % Math.Pow(2, 32));
            }
        }
        else{
            for (int i = 0; i < enc.Length-1; i++)
            {
                enc[i] = (uint)((BitConverter.ToUInt32(M, i * 4) +
a5.getKeyWord()) % Math.Pow(2, 32));
            }
            byte[] lastWord = new byte[4];
            for (int i = 0; i < lastWord.Length; i++)
            {
                if (i < enc.Length % 4)
                {
                    lastWord[i] = M[M.Length - 5 + i];
                }
                else {
                    lastWord[i] = 0;
                }
            }
            enc[enc.Length-1] =
(uint)((BitConverter.ToUInt32(lastWord, 0) + a5.getKeyWord()) %
Math.Pow(2, 32));
        }
        byte[] encBytes =
enc.SelectMany(BitConverter.GetBytes).ToArray();
        string tmp = BitConverter.ToString(encBytes);
        if (tmp.Length > 100)
        {
            textToShow.text = "Перші рядки файлу: " + tmp.Substring(0,
100);
        }
        else
        {
```

```
            textToShow.text = "Перші рядки файлу: " + tmp;
        }

this.gameObject.GetComponent<FipePickerSystem>().saveFile(encBytes,
"enc");
        inputField.text = "";
        result.text = "Файл збережено";

        //Debug.Log("_____________________________________");
    }
    public void decrypt()
    {
        a5 = new A5128LFSR();
        setKey();
        byte[] encBytes = File.ReadAllBytes(path);
        uint[] enc = new
uint[(uint)Math.Ceiling((double)encBytes.Length / 4)];
        uint[] dec = new uint[enc.Length];
        byte[] decBytes = new byte[encBytes.Length];
        for (int i = 0; i < enc.Length; i++)
        {
            dec[i] = (uint)((BitConverter.ToUInt32(encBytes, i * 4) -
a5.getKeyWord()) % Math.Pow(2, 32));
        }
        decBytes = dec.SelectMany(BitConverter.GetBytes).ToArray();
        string tmp2 = Encoding.ASCII.GetString(decBytes);
        if (tmp2.Length > 100)
        {
            textToShow.text = "Перші рядки файлу: " +
tmp2.Substring(0, 100);
        }
        else
        {
            textToShow.text = "Перші рядки файлу: " + tmp2;
        }


this.gameObject.GetComponent<FipePickerSystem>().saveFile(decBytes,
"dec");
        inputField.text = "";
        result.text = "Файл збережено";
    }
}
```

```
using System;
using System.Collections;
using System.Collections.Generic;
using System.Text;
using UnityEngine;

public class A5128LFSR// : MonoBehaviour
{
    private string key;

     byte[] reg1 = new byte[19];
     byte reg1_13 = 13;
     byte reg1_16 = 16;
     byte reg1_17 = 17;
     byte reg1_18 = 18;
     byte reg1Clock = 8;

     byte[] reg2 = new byte[22];
     byte reg2_20 = 20;
     byte reg2_21 = 21;
     byte reg2Clock = 10;

     byte[] reg3 = new byte[23];
     byte reg3_7 = 7;
     byte reg3_20 = 20;
     byte reg3_21 = 21;
     byte reg3_22 = 22;
     byte reg3Clock = 10;


    // Start is called before the first frame update
     void shiftReg1()
    {
        reg1[reg1_18] = (byte)((reg1[reg1_18] + reg1[reg1_17] +
reg1[reg1_16] + reg1[reg1_13]) % 256);
        if (--reg1_18 == 255) reg1_18 = 18;
        if (--reg1_13 == 255) reg1_13 = 18;
        if (--reg1_16 == 255) reg1_16 = 18;
        if (--reg1_17 == 255) reg1_17 = 18;
        if (--reg1Clock == 255) reg1Clock = 18;
        //byte newB = (byte)((reg1[18] + reg1[17] + reg1[16] +
reg1[13]) % 256);
        //Array.Copy(reg1, 0, reg1, 1, reg1.Length - 1);
        //reg1[0] = newB;
    }
     void shiftReg2()
    {
        reg2[reg2_21] = (byte)((reg2[reg2_21] + reg2[reg2_20]) % 256);
        if (--reg2_21 == 255) reg2_21 = 21;
        if (--reg2_20 == 255) reg2_20 = 21;
        if (--reg2Clock == 255) reg2Clock = 21;

        //byte newB = (byte)((reg2[21] + reg2[20]) % 256);
        //Array.Copy(reg2, 0, reg2, 1, reg2.Length - 1);
        //reg2[0] = newB;
    }
     void shiftReg3()
    {
```

```
        reg3[reg3_22] = (byte)((reg3[reg3_22] + reg3[reg3_21] +
reg3[reg3_20] + reg3[reg3_7]) % 256);
        if (--reg3_22 == 255) reg3_22 = 22;
        if (--reg3_21 == 255) reg3_21 = 22;
        if (--reg3_20 == 255) reg3_20 = 22;
        if (--reg3_7 == 255) reg3_7 = 22;
        if (--reg3Clock == 255) reg3Clock = 22;
        //byte newB = (byte)((reg3[22] + reg3[21] + reg3[20] +
reg3[7]) % 256);
        //Array.Copy(reg3, 0, reg3, 1, reg3.Length - 1);
        //reg3[0] = newB;
    }
    void majorityFunctionAndShift()
    {
        byte x = (byte)(reg1[reg1Clock] & 1);
        byte y = (byte)(reg2[reg2Clock] & 1);
        byte z = (byte)(reg3[reg3Clock] & 1);
        byte f = (byte)(x & y | x & z | y & z);
        if (x == f) { shiftReg1();  }
        if (y == f) { shiftReg2(); }
        if (z == f) { shiftReg3();}

    }
     void initA5(string keyS)
    {
        reg1 = new byte[19];
        reg2 = new byte[22];
        reg3 = new byte[23];
        byte[] key = Encoding.ASCII.GetBytes(keyS);
        byte[] syn = Encoding.ASCII.GetBytes("wzQYGqx8EfWLXhyD");
        Array.Copy(key, 0, reg1, 0, key.Length);
        Array.Copy(key, 0, reg2, 1, key.Length - 1);
        reg2[0] = key[key.Length - 1];
        Array.Copy(key, 0, reg3, 3, key.Length - 3);
        for (int i = 0; i < 3; i++)
        {
            reg3[i] = key[key.Length - 3 + i];
        }
        Array.Copy(syn, 0, reg1, 16, 3);
        Array.Copy(syn, 3, reg2, 16, 6);
        Array.Copy(syn, 9, reg3, 16, 7);
        for (int i = 0; i < 128; i++)
        {
            shiftReg1();
            shiftReg2();
            shiftReg3();
        }
    }
    public void setKey(string key) {
        initA5(key);
    }
    public byte getKeyByte()
    {
        majorityFunctionAndShift();
        return (byte)((reg1[reg1_18] + reg2[reg2_21] + reg3[reg3_22])
% 256);
    }
    public uint getKeyWord() {
```

```
    byte[] word = new byte[4];
    for (int i = 0; i < word.Length; i++)
    {
        word[i] = getKeyByte();
    }
    return BitConverter.ToUInt32(word, 0);
}
```

Додаток В

Список публікацій здобувача за темою дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Гулак Г. М., Скітер І. С., Гулак Є. Г. (2021) Методологічні засади створення та функціонування центру кібербезпеки інформаційної інфраструктури об'єктів ядерної енергетики. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2021. Т. 4, № 12. С. 172–186. DOI: https://doi.org/10.28925/2663-4023.2021.12.172186. *Бази: CrossRef, Google Scholar.*

2. Дереговський В.В., Кафтанатіна О.А., Кордюков П.Л., Меньшенін Є.А., Гулак Є.Г. (2021) Розробка математичної моделі впливу радіаційно небезпечних об’єктів на довкілля при пожежі. Математичні машини і системи. 2021. №4. С. 99–111. DOI: https://doi.org/10.34121/1028-9763-2021-4-99-111. *Бази: CrossRef, Google Scholar.*

3. Гулак Г., Жданова Ю., Складанний П., Гулак Є., Корнієць В. (2022). Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об’єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2022. №1 (17). С. 145–158. DOI: https://doi.org/10.28925/2663-4023.2022.17.145158. *Бази: CrossRef, Google Scholar.*

4. Hulak H., Skladannyi P., Sokolov V., Hulak E., Korniiets V., Dynamic Model of Guarantee Capacity and Cyber Security Management in the Critical Automated System, 2nd International Conference on Conflict Management in Global Information Networks: November 2022, Kyiv, Ukraine. 2022. Vol. 3530. P. 102–111. ISSN: 1613-0073. *Бази: Scopus, CrossRef, Google Scholar.*

5. Гулак Є. Г. (2024) Методика раціонального синтезу підсистеми криптографічного захисту інформації в мережах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».

2024. № 4(24). С. 282–297. DOI: https://doi.org/10.28925/2663-4023.2024.24.282297. *Бази: CrossRef, Google Scholar.*

Наукові праці, які засвідчують апробацію матеріалів дисертації:

6. Гулак Г.М., Гулак Є.Г., Корнієць В.А. (2023) Безпека шифрування коротких повідомлень в інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Актуальні проблеми управління інформаційною безпекою держави. Київ, 2023. С. 260–262.

7. Гулак Г. М., Скітер І. С., Гулак Є. Г., Цирканюк Д. А. (2023) Базові засади побудови центру кібербезпеки об`єктів ядерної енергетики. Актуальні проблеми управління інформаційною безпекою держави. Київ, 2023. С. 262–266.

Наукові праці, які додатково відображають наукові результати дисертації:

8. Morozov A., Hrebennyk A., Trunova E., Skiter I., Hulak E. Design of Industry Centers of Cyber Security of Facilities of Critical Infrastructure. Workshop on Cybersecurity Providing in Information and Telecommunication Systems CPITS-II-2021: October 26, 2021, Kyiv, Ukraine, 2021. Vol. 3187. P. 27–37. ISSN: 1613-0073. *Бази: Scopus, CrossRef, Google Scholar.*

9. Hulak H., Grechaninov V., Hulak E., Skladannyi P., Sokolov V. Decentralized Access Demarcation System Construction in Situational Center Network. Cybersecurity Providing in Information and telecommunication Systems (CPITS-II-2021): October 26, 2021, Kyiv, Ukraine, 2021. Vol. 3188. P. 197–206. ISSN: 1613-0073. *Бази: Scopus, CrossRef, Google Scholar.*