

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ І ГЛОБАЛЬНОГО
ІНФОРМАЦІЙНОГО ПРОСТОРУ

КУЗЬМЕНКО Лідія Володимирівна



УДК 681.5(042.3)

**ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДЛЯ СТВОРЕННЯ
ПЕРСПЕКТИВНИХ ГАРАНТОЗДАТНИХ АВТОМАТИЗОВАНИХ СИСТЕМ
УПРАВЛІННЯ ОБ'ЄКТАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ**

05.13.06 — «Інформаційні технології»

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2021

Дисертацією є рукопис.

Робота виконана в

Інституті телекомунікацій і глобального інформаційного простору Національної академії наук України

Науковий керівник: кандидат технічних наук, доцент
ГУЛАК Геннадій Миколайович,
завідувач лабораторії кібербезпеки Інституту проблем математичних машин і систем НАН України

Офіційні опоненти:

доктор технічних наук, доцент
СУБАЧ Ігор Юрійович,
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», завідувач спеціальної кафедри

доктор технічних наук, доцент
РАК Тарас Євгенович,
Приватний заклад вищої освіти «ІТ СТЕП Університет», м. Львів
Проректор з науково-педагогічної роботи,
професор кафедри інформаційних технологій

Захист відбудеться «11»березня 2021 р. о 13⁰⁰ на засіданні спеціалізованої вченої ради Д26.255.01 при Інституті телекомунікацій і глобального інформаційного простору НАН України за адресою:
03186, м. Київ, бул. Чоколівський, 13, ауд. 601.

З дисертацією можна ознайомитись у бібліотеці Інституту телекомунікацій і глобального інформаційного простору Національної академії наук України за адресою: 03186, м. Київ, бул. Чоколівський, 13

Автореферат розісланий «02» лютого 2021 р.

Учений секретар спеціалізованої вченої ради
к.т.н., ст.дослідник



О. Г. ЛЕБІДЬ

ВСТУП

Обґрунтування вибору теми дослідження. Ключовою тенденцією розвитку сучасної світової цивілізації є застосування цифрових технологій. Підтвердженням цьому слугує цифрова трансформація промисловості, логістики, системи продаж, сервісу тощо. Експерти фінансового ринку прогнозують, що дохід економіки від проявів цифрової трансформації сягне до 2025 року біля 30 трлн. USD. Разом з цим експерти стверджують, що такий стан справ вимагатиме суттєвої трансформації, власне, й інформаційно-телекомунікаційної індустрії. Більшою мірою це стосуватиметься автоматизованих систем (АС), включених в контури управління інформаційними та/або технологічними процесами (ІТП) об'єктів критичної інфраструктури (ОКІ), а також інформаційними ресурсами (ІР), які в умовах кібернетичних втручань і загроз забезпечують необхідні послуги та/або сервіси ОКІ. Негативними наслідками такої трансформації може бути виникнення нових ризиків для безпеки ІТП та ІР, що, як результат, й генерує потребу в побудові та впровадженні сучасних інформаційних технологій (ІТ) для створення перспективних гарантоздатних (ПГ) автоматизованих систем управління (АСУ), захищених від впливу антропогенних і техногенних загроз.

Незважаючи на нормативно-правову урегульованість питань щодо створення інформаційно-телекомунікаційних систем (ІТС) для потреб ОКІ та оцінювання стану їх захищеності від впливу шкідливих програм, фальшивого ПЗ і зловмисних шифруючих кодів, на сьогодні ще й досі спостерігається: дублювання інформаційних потоків та накопичення ОКІ надлишкового навантаження на засоби зберігання інформації; технологічна нерівність ОКІ у сфері інформаційних, телекомунікаційних та інших високих технологій; недостатність глибини наукових досліджень щодо створення для потреб ОКІ новітніх захищених АСУ, а також подекуди повна відсутність рішень щодо специфіки їх функціонування; недосконалість методів, моделей і методик вирішення відповідних завдань. Саме тому *наукова задача*, яка полягає в розробленні теоретичних і прикладних засад побудови інформаційної технології для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури, а також визначення впливу на процеси функціонування таких систем антропогенних і техногенних втручань та загроз *є актуальною і потребує розв'язку*.

Дослідженню проблеми побудови перспективних гарантоздатних АСУ та визначення впливу на процеси функціонування таких систем антропогенних і техногенних втручань та загроз присвячено роботи П.О.Балашова, М.М. Будько, В.Л.Бурячка, В.Б.Дудикевича, Н.Ф.Казакової, О.В.Копійка, Д.В.Ланде, М.І.Паламаря, Д.В. Стефанишина, І.Ю.Субача, О.М.Трофимчука, В.С.Харченка, W.Jansen, D.Catteddu, K.Stoddart та багатьох інших. За результатами їх досліджень встановлено, що особливістю вирішення зазначеного завдання є недостатність статистичної інформації, а також наявність невизначеностей та протиріч, викликаних:

- 1) відносно високим рівнем розвитку засобів автоматизації та низьким науково-методичним рівнем досліджень властивостей якості АСУ ОКІ;
- 2) рівнем відмовостійкості, закладеним у конструкцію АСУ ОКІ та її необхідним рівнем;
- 3) зростанням витрат на розробку, виробництво та експлуатацію АСУ ОКІ і реальними економічними можливостями замовника;
- 4) необхідним рівнем продуктивності та обмеженими можливостями промислової бази з виробництва якісної елементної бази і комплектуючих виробів, тощо.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота та отримані результати пов'язані з вирішенням науково-технічних задач, сформульованих в Стратегії національної безпеки України (Указ Президента України № 287/2015 від 26.05.2015 р.), «Порядку формування переліку ІТС об'єктів критичної інфраструктури держави» (Постанова

КМ України № 518 від 19.06.2019 р.), «Основних наукових напрямках та найважливіших проблемах фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014–2018 роки». Частину завдань дисертаційної роботи автором вирішено в рамках таких науково-дослідних робіт, як: «Розробка інформаційного інструментарію еколого-економічного прогнозування надзвичайних ситуацій техногенного та природного характеру з метою захисту об'єктів критичної інфраструктури» (№ д.р. 0116U000797), «Базис-Наука» (№ д.р. 0119U000042дс) та «Розробка науково-технічних пропозицій з організації віддаленого управління станціями оптико-електронних спостережень типу 1 та типу 2» (№ д.р. 0120U105420), які у 2020 році виконано відповідно в ІТГП НАН України, ІПММС НАН України і Національному центрі управління та випробувань космічних засобів України.

Мета і завдання дослідження. Метою дисертаційної роботи є побудова інформаційної технології для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури України, здатних гарантовано надавати абонентам необхідні послуги та/або сервіси, яким в заданих режимах і умовах застосування з урахуванням стану захищеності таких систем від загроз порушення цілісності, конфіденційності та доступності можливо виправдано довіряти.

Для досягнення поставленої мети в роботі необхідно розв'язати такі **завдання**:

- 1) дослідити можливі загрози та сформулювати їх актуальну множину, а також множину уразливостей безпеці функціонування АСУ ОКИ;
- 2) обґрунтувати та побудувати часткову модель загроз безпеці ПГ АСУ ОКИ;
- 3) розробити метод визначення впливу загроз на процеси функціонування ПГ АСУ ОКИ;
- 4) вдосконалити метод формування типового варіанту побудови ПГ АСУ ОКИ.

Зважаючи на таке, **об'єктом дослідження** в роботі є процеси створення перспективних гарантоздатних АСУ та процеси функціонування таких систем в умовах впливу антропогенних і техногенних втручань та загроз. **Предметом дослідження** – інформаційна технологія, спрямована на формування типового варіанту побудови ПГ АСУ, а також визначення впливу загроз порушення цілісності, конфіденційності та доступності (ЦКД) на процеси функціонування такої системи.

Методи дослідження. При вирішенні поставлених задач в дисертаційній роботі було використано класичні та похідні критерії вибору рішень в умовах невизначеності, «евристичні» (експертні) методи оцінювання – метод Дельфі, метод аналізу ієрархій (МАІ) та метод парних порівнянь, а також метод морфологічних карт, методи лінійного програмування, методи функціонально-вартісного (ФВА) та кластерного аналізу, тощо.

Наукова новизна отриманих результатів полягає в подальшому розвитку теоретичних і практичних методів та моделей побудови і визначення впливу загроз на процеси функціонування перспективних гарантоздатних АСУ ОКИ.

Новими результатами, отриманими в дисертаційній роботі, є:

- 1) вперше розроблений **метод визначення впливу загроз на процеси функціонування перспективних гарантоздатних АСУ ОКИ**, впровадження якого шляхом реалізації семантичної моделі протидії системі захисту ПГ АСУ ОКИ з атакуючою стороною, процедури детектування та відновлення даних та моделі оцінки стану захищеності такої системи від загроз порушення ЦКД дозволяє, на відміну від існуючих, відслідкувати вплив шкідливих програм, фальшивого ПЗ і злоякісних шифруючих кодів на ІТП в АСУ ОКИ, відшукати вразливості та/або істинні значення ключів, застосованих для шифрування даних в ПГ АСУ ОКИ, оцінити стан захищеності сформованого прототипу варіанту побудови ПГ АСУ ОКИ від впливу кібератак та убезпечити АСУ ОКИ від НСД до її ресурсів та інформації, що в ній циркулює;

2) удосконалений *метод формування типового варіанту побудови перспективної гарантоздатної АСУ*, впровадження якого за рахунок розробки процедури вибору прототипу топології мережевої інфраструктури, процедури вибору типового АРМ раціональної конфігурації, процедури раціонального вибору ПЗ ПР та процедури вибору типового варіанту побудови ПГ АСУ ОКІ дозволяє, на відміну від існуючих, організувати доступ до мережі та надання обчислювальних ресурсів і послуг абонентам для спільного використання ними власних і зовнішніх ІР, забезпечити доступ користувачам до таких ІР, керування їх обміном, передачею та машинною переробкою, автоматизувати процеси пошуку і збору інформації у зовнішніх і внутрішніх джерелах, її реєстрації, трансформації та функціональної обробки, а також процеси захисту ІР в АСУ від кібернетичних загроз.

Практичне значення отриманих наукових результатів полягає в тому, що вони за рахунок реалізації методу формування типового варіанту побудови такої системи та методу визначення впливу загроз на процеси її функціонування дозволили **розробити прикладні засади побудови інформаційної технології для створення ПГ АСУ ОКІ**, впровадження якої на відміну від існуючих забезпечує гарантоване надання абонентам необхідних послуг та/або сервісів, яким в заданих режимах і умовах застосування з урахуванням стану захищеності таких систем від загроз порушення ЦКД можливо виправдано довіряти. Разом з цим впровадження ІТ для створення ПГ АСУ ОКІ на прикладі НЕК «Укренерго» сприяє:

по-перше, підвищенню ефективності дій осіб, відповідальних за забезпечення безпеки ПГ АСУ ОКІ (за рахунок оперативного визначення найбільш значимих загроз та своєчасного реагування на стан захищеності АСУ від загроз порушення ЦКД) приблизно на 12%;

по-друге, скороченню часу на прийняття виважених управлінських рішень щодо побудови ПГ АСУ ОКІ з відповідним ПАЗ та їх впровадження приблизно на 18 - 20%.

Результати дисертаційного дослідження впроваджено в:

Інституті проблем математичних машин і систем НАН України при дослідженні проблеми побудови різномірних інформаційних систем ситуаційних центрів сектору безпеки і оборони та обміну даними між ними (Акт впровадження від 03.12.2020 р.);

Національному центрі управління та випробувань космічних засобів для оцінювання стійкості криптосистем та пошуку вразливостей або істинних значень ключів, застосованих при зловмисному шифруванні даних (Акт впровадження від 17.12.2020 р.);

НЕК «УкрЕнерго» під час виконання робіт зі створення та розгортання ІТС для потреб її структурних підрозділів, а також при налаштуванні SIEM систем, спрямованих на вирішення завдань захисту таких ІТС від сучасних кіберзагроз (Акт впровадження від 04.01.2021);

Азербайджанському Технічному Університеті при підготовці магістрантів спеціальності 050627 «Інженерія електроніки, телекомунікації та радіотехніки» за спеціалізацією «Інформаційна безпека телекомунікаційних систем» (Акт впровадження від 05.01.2021).

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться на захист, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [1] – результати експерименту щодо навантаження вбудованих апаратних платформ для IoT рішень при розгортання невеликих комерційних та наукових бездротових мереж; [2] – технологія захисту освітніх матеріалів та іншої інформації обмеженого доступу, а також ІТ-інфраструктури ЗВО від випадкових або спрямованих атак та шкідливого ПЗ; [3] – обґрунтування підходу до побудови та вибору раціональної топології комп'ютерних мереж сучасних АСУ ЗС України, що сприятиме підвищенню оперативності, стійкості, скритності, безперервності й ефективності управління військами; [4, 18] – алгоритм порівняльного оцінювання ПЗ однакового функціонального призначення (на прикладі СУБД та СЕДО), що спрямовані на розв'язання нагальних завдань інформаційної діяльності; [5] – обґрунтування

набору показників, які можуть бути використані для оцінювання якості та подальшого порівняльного аналізу ПЗ сучасних АС; [6] – алгоритм обґрунтованого вибору серед множини існуючих АРМ раціональної конфігурації; [7, 13] – алгоритм обґрунтованого вибору серед множини існуючих раціональної системи електронного документообігу; [8] – обґрунтування необхідності створення системи комплексної оцінки стану захисту інформації в розподілених корпоративних мережах; [9] – обґрунтування необхідності захисту критично-важливих сегментів та об'єктів економіки держав світу від загроз антропогенного і техногенного характеру; [10] – обґрунтування раціонального набору параметрів і функцій ПЗ спеціального призначення, спрямованих на розв'язання завдань інформаційної діяльності; [11] – алгоритм порівняльного аналізу автоматизованих ІС на підставі заздалегідь обраного набору ознак (властивостей) та комплексного показника якості системи; [12] – процедура формування системи детектування шкідливого ПЗ на базі застосування методів виділення значимих ознак в ІТ системах; [14, 19] – застосування методу кластеризації кількісних даних для вирішення задачі розпаралелювання операцій пошуку істинних значень застосованих ключів та визначенні місця соціальної інженерії в ході проведення розвідки ІТС; [15] – шляхи управління процедурою інвестування в ІТ з урахуванням їх багатофакторності та захисту інформації обмеженого доступу, а також ІТ-інфраструктури від випадкових або спрямованих атак та шкідливого ПЗ; [16] – технологія забезпечення інформаційної і кібербезпеки ЗВО України від стороннього кібернетичного впливу та захисту інформації обмеженого доступу, а також ІТ-інфраструктури ЗВО від випадкових або спрямованих атак та шкідливого ПЗ; [17] – технологія визначення наявності бездротових точок доступу та оцінки негативних наслідків витоку персональних даних під час їх обробки в АС; [20] – процедура виявлення та організації кіберзахисту об'єктів критичної інфраструктури України від впливу найбільш небезпечних векторів атак, зокрема від впливу шкідливого ПЗ; [21] – технологія захисту середовища ІоТ від випадкових або спрямованих атак та шкідливого ПЗ на етапах розробки та експлуатації.

Апробація результатів дисертації. Основні положення і результати досліджень доповідалися та обговорювалися на наукових конференціях та семінарах, серед яких: V-а НТК «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення» (м. Київ, ВІТІ НТУУ «КПІ» МО України, 2010), НТК «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (м. Київ, КНУ імені Т.Г. Шевченка, 2016 та 2018 р.р.), Регіональній конференції МСЕ для країн СНД та Грузії «Перспективи надання послуг на основі мереж пост-NGN, 4G и 5G. Організаційні і технічні рішення щодо їх побудови та захисту» ДУТ (м. Київ, ДУТ, 2017), VIII International conferece of students, PHD- students and young scientists «Engineer of XXI Century» (University of Belsko-Biala, Poland, 2018), X International conferece of students, PHD- students and young scientists «Engineer of XXI Century» (University of Belsko-Biala, Poland, 2020).

Публікації. Основні положення дисертаційної роботи опубліковано у 21 науковій праці, з яких: 2 публікації – розділ колективної монографії [1] та [2]; 12 – у вітчизняних фахових наукових виданнях, які входять до міжнародних наукометричних баз даних (*Index Copernicus*, *CORE*, *BASE*, *ResearchBib*, *PKP*, тощо) [3–14]; 3 – у міжнародних рецензованих виданнях, що входять до баз даних *Scopus* та *Web of Science* [15–17] та 4 тез доповідей [18–21]. Без співавторів опубліковано 1 наукову статтю і 1 тези доповідей.

Обсяг і структура дисертації. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, трьох розділів, загальних висновків, списків використаних джерел (в кінці кожного розділу) і 148 сторінок основного тексту, 48 рисунків, 38 таблиць. Список використаних джерел за трьома розділами містить 149 унікальних найменувань і займає 12 сторінок. Загальний обсяг дисертаційної роботи – 181 сторінка. Кількість сторінок додатку – 35.

ОСНОВНИЙ ЗМІСТ

У **вступі** показано актуальність наряду досліджень, відбито зв'язок дисертаційної роботи з науковими програмами, планами та темами, сформовано мету і завдання дослідження, наведено основні положення, які виносяться на захист, практичну цінність роботи та відомості про апробацію результатів їх впровадження.

У **першому розділі**:

1. Сформовано перелік об'єктів, які потенційно може бути віднесено до критичної інфраструктури.

2. Обґрунтовано, що під гарантоздатністю АСУ ОКІ слід розуміти їх комплексну властивість надавати необхідні послуги та/або сервіси, яким в заданих режимах і умовах застосування можна виправдано довіряти.

3. Досліджено множину загроз для АСУ ОКІ, а також уразливості програмно-апаратних засобів (ПАЗ) АСУ ОКІ, що впливають на її функціонування.

4. Проведено оцінку низки математичних моделей побудованих на розподілі Вейбулла, використання яких дозволяє ефективно проводити налаштування і випробування ПАЗ, оцінювати та прогнозувати надійність таких систем при їх проектуванні та експлуатації. Стисло розглянуто критерії, застосування яких дозволяє об'єктивно оцінити якість функціонування АСУ ОКІ в цілому.

5. Розглянуто програмно-апаратні методи захисту критичних засобів, втручання до яких створює передумови для порушення структури і функцій АСУ ОКІ.

6. Сформовано основні принципи забезпечення технологічної безпеки ПАЗ АСУ ОКІ на різних етапах їх життєвого циклу.

Це дозволило сформувати завдання і побудувати структурно-логічну схему дослідження (рис. 1).

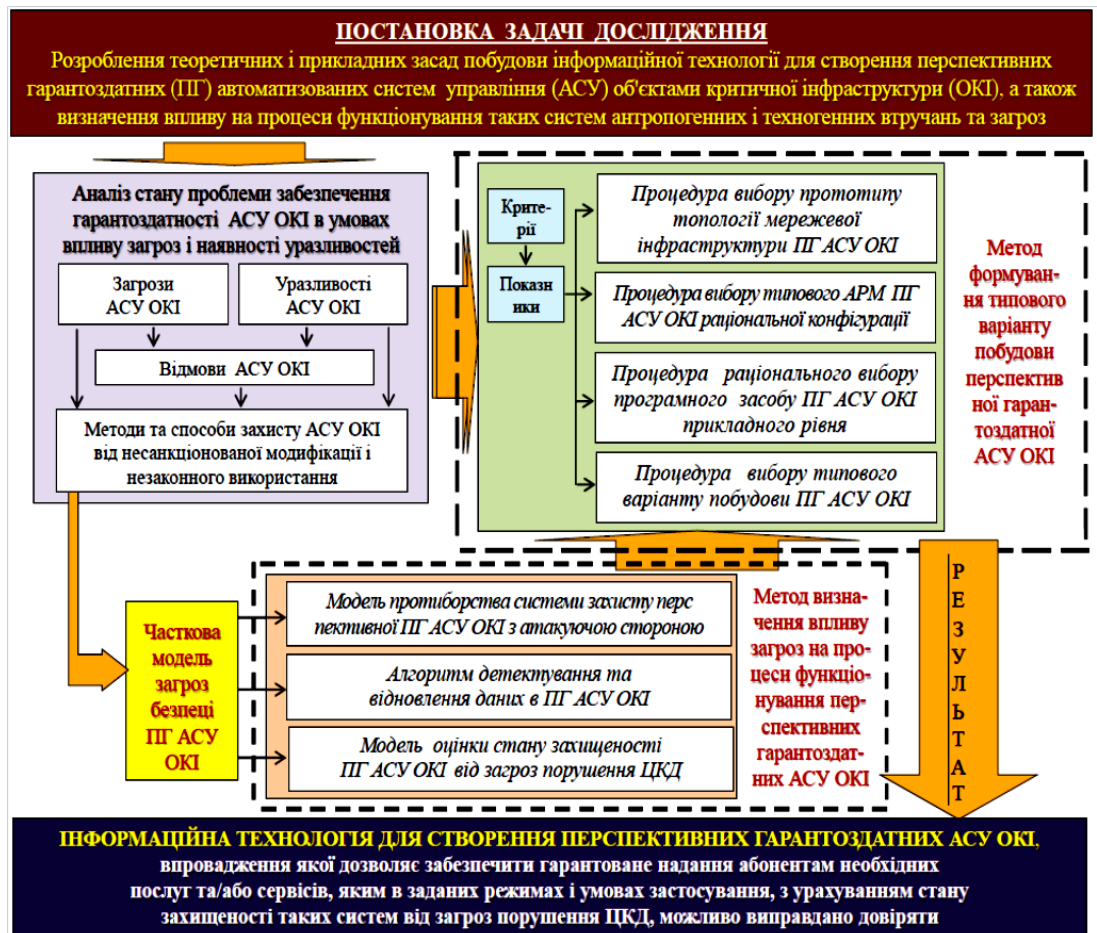


Рис. 1. Структурно-логічна схема проведення дослідження

В другому розділі описано метод формування типового варіанту побудови перспективної гарантоздатної АСУ ОКІ. Метод поєднує такі взаємодоповнюючі процедури, як вибір прототипу топології мережевої інфраструктури (МІ), вибір типового АРМ раціональної конфігурації, раціональний вибір ПЗ прикладного рівня та вибір типового варіанту побудови ПГ АСУ ОКІ, й виконується в чотири етапи.

Етап 1. Оскільки топологія МІ є однією з найважливіших характеристик будь-якого ОКІ,

то питання щодо вибору її прототипу серед низки можливих альтернатив Y_j , $j = \overline{1, n}$ ($n = 4$) вирішувалось в роботі одним із перших. Як критерії K_t , $t = \overline{1, k}$ ($k = 3$) для проведення порівняльної оцінки альтернативних варіантів було обрано (табл.1) вартість, функціональність та відповідність технічним вимогам, як підкритерії – показники R_i , $i = \overline{1, m}$ ($m = 10$).

Таблиця 1

Приклад порівняння класичних топологій побудови МІ в умовах невизначеності

Критерії оцінки МІ	Показники оцінки МІ	Позначення		Y_1		Y_2		Y_3		Y_4	
				R	b	R	b	R	b	R	b
Забезпечення дешевизни	Кабельна мережа	R_1	b_1	10	9	7	6	6	5	1	0
	Обладнання	R_2	b_2	9	6	8	5	7	4	3	0
	Монтаж	R_3	b_3	10	8	8	6	5	3	2	0
	Обслуговування	R_4	b_4	1	0	2	1	10	9	5	4
Забезпечення функціональності	Універсальність	R_5	b_5	1	0	3	2	10	9	1	0
	Діагностування	R_6	b_6	1	0	2	1	10	9	10	9
	Гнучкість	R_7	b_7	1	0	2	1	7	6	1	0
	Масштабованість	R_8	b_8	8	7	3	2	10	9	1	0
Забезпечення відповідності технічним вимогам	Швидкість роботи	R_9	b_9	3	0	5	2	8	5	10	7
	Захищеність від відмов	R_{10}	b_{10}	3	0	3	0	7	4	10	7
ВАЛЬДА		$\max_i \left(\min_j R_{ij} \right)$						+			
НАДЗВИЧАЙНОГО ОПТИМІЗМУ		$\max_i \left(\max_j R_{ij} \right)$		+				+		+	
СЕВІДЖА		$\min_j \left(\max_i b_{ij} \right)$					+				

Припустимо, що існує n класичних топологій побудови МІ (шинна - Y_1 , кільцева - Y_2 , зіркова - Y_3 та стільникова - Y_4), серед яких за визначеними критеріями і показниками (табл.1) необхідно обрати раціональну.

Спроба вирішити дану задачу за допомогою відомих критеріїв прийняття рішень в умовах невизначеності таких, як критерії Вальда, Севіджа та надзвичайного оптимізму не дозволила прийняти з цього питання однозначне рішення. Так, наприклад, згідно критерію Вальда найбільш перспективним може виявитися топологія Y_3 . За критерієм надзвичайного оптимізму такими можуть бути топології Y_1 , Y_3 та Y_4 . Критерій Севіджа взагалі пропонує зосередити увагу дослідника на топології Y_2 . Практичний же досвід створення мереж рекомендує зосередитись на прототипі Y_4 , оскільки топології Y_1 та Y_2 вважає застарілими і малонадійними.

Зважаючи на таке для подальшого порівняння обраних, як приклад, топологій в роботі було застосовано метод МАІ. Алгоритм його реалізації полягає в такому.

Крок 1.1. Структурування проблеми вибору прототипу топології МІ у вигляді ієрархії та виявлення найбільш важливих елементів, а саме множин: топологій Y_j , $j = \overline{1, n}$, серед яких необхідно вибрати найкращу; критеріїв K_t , $t = \overline{1, k}$, за якими обирається компромісне рішення та показників R_i , $i = \overline{1, m}$, що характеризуватимуть якість Y_j .

Крок 1.2. Проведення за спеціальною вербально-числовою шкалою попарного порівняння:

- 1) показників R_i ($i = \overline{1, m}$, $m = 10$) між собою;
- 2) показників R_i ($i = \overline{1, m}$, $m = 10$) за кожним із критеріїв K_t , $t = \overline{1, k}$ ($k = 3$)

та заповнення матриць, виду $A_l = \left\| \begin{matrix} a_{11}^{(l)} & a_{12}^{(l)} & \dots & a_{1j}^{(l)} \\ a_{21}^{(l)} & a_{22}^{(l)} & \dots & a_{2j}^{(l)} \\ \dots & \dots & \dots & \dots \\ a_{i1}^{(l)} & a_{i2}^{(l)} & \dots & a_{im}^{(l)} \end{matrix} \right\|$ (1)

де $a_{ij}^{(l)}$, $i = \overline{1, m}$, $j = \overline{1, m}$, $l = \overline{1, k}$ - результат порівняння l -м експертом i -го показника з j -м; k - число експертів; m - кількість показників.

Крок 1.3. Визначення власних значень кожної із сформованих матриць, їх максимальних

значень та відповідних цим значенням власних векторів.

Формування вектору власних значень матриць попарного порівняння показників R_i , $i = \overline{1, m}$ ($m = 10$) за кожним із критеріїв K_t , $t = \overline{1, k}$ ($k = 3$), тобто їх локальних пріоритетів та нормованої до одиниці матриці AB_{ji} , сформованої з власних векторів матриць попарних порівнянь топологій МІ за кожним із показників. Формування власного вектору локальних пріоритетів показників, що використовуються під час порівняння топологій МІ - XVB_i .

Крок 1.4. Обчислення глобальних пріоритетів досліджуваних топологій МІ, що дозволять визначити місце кожної з них серед порівнюваних:

$$AB_j^{glpr} = \sum_{i=1}^m (AB_{ji} - XVB_i). \quad (2)$$

Висновок. За сукупністю показників, перелічених у табл.1 та з врахуванням їх важливості на очікуваний результат, як прототип для побудови МІ перспективної АСУ ОКІ серед можливих j альтернативних варіантів доцільно обрати той, для якого AB_j^{glpr} буде максимальним.

Для подальших досліджень вводимо позначення та приймаємо, що $K_{MI}^{nad} = AB_{max}^{glpr}$.

Етап 2. Важливою складовою розвитку ОКІ є, як відомо, їх всебічне інформаційне (інформаційно-аналітичне) забезпечення. До нього пред'являються вимоги як за якістю та цілеспрямованістю, так й за точністю та вірогідністю. Останні є першорядними і неодмінними факторами надійного та ефективного функціонування ОКІ. Вони забезпечуються за рахунок впровадження АСУ, головною складовою яких є автоматизовані робочі місця (АРМ).

Вибір типового АРМ раціональної конфігурації для комплектування ПГ АСУ ОКІ в роботі пропонується здійснювати шляхом врахування продуктивності його програмного і апаратного забезпечення та, як наслідок, визначення рівня окупності капітальних вкладень на впровадження такого АРМ за такими кроками.

Крок 2.1. Формування моделі витрат на створення типового АРМ раціональної конфігурації

$$C_{tex+prog}^{APM} = \sum_{i=1}^n C_i^{TZ} + \sum_{j=1}^m C_j^{PZ} \quad (3)$$

де C^{TZ} - вартість технічних засобів (ТЗ), наприклад, монітору, системного блоку, функціонального пристрою, тощо; C^{PZ} - вартість програмних засобів (ПЗ), наприклад, загального (ОС) та спеціального програмного забезпечення.

Крок 2.2. Визначення продуктивності кожної складової ТЗ і ПЗ, як лінійної функції від витрат, що необхідні для їх придбання:

$$P_i^{prodykt} = K_i * C_i^{TZ}, \quad P_j^{prodykt} = K_j * C_j^{PZ} \quad (4)$$

де K_i , K_j - нормуючі коефіцієнти, які фактично визначатимуть споживчу ефективність i -х технічних та j -х програмних засобів АРМ, де $i = \overline{1, m}$, $j = \overline{1, n}$.

Крок 2.3. Формування матриці можливих конфігурацій для кожного i -го технічного та j -го програмного засобу АРМ, де $i = \overline{1, m}$, $j = \overline{1, n}$. Побудова за даними матриць графіків залежності показників продуктивності від значень ціни та визначення нормуючих коефіцієнтів K_i (K_j), як котангенсу кута нахилу апроксимуючої прямої до прямої показників продуктивності.

Крок 2.4. Формування цільової функції, яку необхідно мінімізувати

$$F(C_1^{TZ}, C_2^{TZ}, \dots, C_m^{TZ}, C_1^{PZ}, C_2^{PZ}, \dots, C_n^{PZ}) \xrightarrow{v} \min, \quad (5)$$

$$\text{за обмежень: } P_{dop}^{prodykt} \leq K_i * C_i^{TZ} \leq 100, \quad P_{dop}^{prodykt} \leq K_j * C_j^{PZ} \leq 100, \quad C_i^{TZ} > 0, \quad C_j^{PZ} > 0 \quad (6)$$

Вирази (5) та (6) відбивають класичне завдання лінійного програмування, де у якості

вхідних даних мають бути задані значення обчислених на кроці №2.2 нормуючих коефіцієнтів для всіх складових типового АРМ та гранично припустимі значення показників їх продуктивності ($P_{dop}^{produkt}$). В результаті отримаємо значення припустимих витрат на закупівлю кожного з i -х технічних та j -х програмних засобів АРМ, де $i = \overline{1, m}$ та $j = \overline{1, n}$, сума яких (3) становитиме частину від загальних капітальних вкладень на впровадження АРМ:

$$C_{вкл}^{капіт} = C_{тех+прогр}^{АРМ} + C_{трансп} + C_{нал} + C_{пуск}, \quad (7)$$

де $C_{трансп}$ - витрати на транспортування; $C_{нал}$ - витрати на налагодження; $C_{пуск}$ - витрати на запуск.

Крок 2.5. Оцінювання рівня окупності капітальних вкладень на впровадження АРМ раціональної конфігурації. Для цього скористаємось безрозмірним розрахунковим коефіцієнтом $K_P^{окупн}$, який дорівнює відношенню річної економії ($E_{рік}$) до витрат на впровадження АРМ ($C_{вкл}^{капіт}$) від початку й до кінця його життєвого циклу: $K_P^{окупн} = E_{рік} / C_{вкл}^{капіт}$. (8)

де $E_{рік} = E_{он} + E_{пр}$ - річної економії від впровадження АРМ;

$E_{он}$ - опосередкована ефективність (характеризує якісні зміни, що можуть статися в результаті впровадження АРМ такі, наприклад, як: підвищення оперативності отримання інформації; скорочення термінів прийняття управлінських рішень тощо). Для його розрахунку застосовують, як правило, методи експертних оцінок;

$E_{пр}$ - пряма ефективність. Може включати річний приріст прибутку, що викликаний, наприклад, зменшенням фонду заробітної плати його користувачів - керівників та виконавців:

$$E_{пр} = Z_{безАРМ}^{фондЗП} - Z_{зАРМ}^{фондЗП}; \quad (9)$$

$Z_{безАРМ}^{фондЗП}$ - річний фонд заробітної плати до впровадження АРМ;

$Z_{зАРМ}^{фондЗП}$ - річний фонд заробітної плати після впровадження АРМ.

Для того щоб впровадження АРМ давало відчутні результати, значення показника $E_{рік}$ має бути значно більшим від нуля: $E_{рік} \gg 0$. Це може бути досягнуто за умови, якщо:

$$\begin{cases} E_{он} \gg 0 & \text{при } E_{пр} \geq 0 \\ E_{пр} \gg 0 & \text{при } E_{он} \geq 0 \end{cases}$$

При $E_{пр} < 0$ обраний варіант впровадження АРМ вважається економічно недоцільним.

Крок 2.6. Порівняння розрахункового $K_P^{окупн}$ з нормативним $K_{норм}^{окупн}$. Нормативний коефіцієнт економічної ефективності (окупності) капітальних витрат $K_{норм}^{окупн}$ встановлюється власником системи для кожного об'єкту, на якому буде впроваджуватися АРМ.

Якщо $K_P^{окупн} \leq K_{норм}^{окупн}$ та коефіцієнт річної економії від впровадження АРМ $E_{ефф}^{екон} \geq 0$, то конфігурація типового АРМ, обраного для комплектування перспективної гарантоздатної АСУ ОКІ є раціональною і не потребує уточнення.

Для подальших досліджень вводимо позначення та приймаємо, що $K_{АРМ}^{ефф} = K_P^{окупн}$.

Етап 3. Підвищення ефективності інформаційного (інформаційно-аналітичного) забезпечення ОКІ залежить перш за все від ступеня автоматизації всіх процесів, що йому притаманні й, по-друге, від можливостей ринку ІТ – існуючих та новітніх ПЗ, які спрямовані на розв'язання завдань інформаційної діяльності. Раціональний вибір серед конкуруючого такого ПЗ ПР, яке б за параметрами та функціями відповідало вимогам користувача та відбиало усі його потреби, в роботі пропонується здійснювати шляхом врахування вимог щодо іконіки та інтерфейсу, підтримки сучасного меню та розвинуеного HELP, тощо, а також

ієрархічної декомпозиції проблеми при аналізі та прогнозуванні ситуацій з великою кількістю значимих факторів на більш прості компоненти. Процедура вибору реалізується при цьому методами МАІ та ФВА за такими кроками.

Крок 3.1. Формування доцільного набору факторів, критеріїв, метрик та оцінних елементів ПЗ ПР, що характеризують властивості цього ПЗ та необхідні для комплексного оцінювання його якості.

Таблиця 2

Приклад формування ієрархічної структури функцій та критеріїв ПЗ

Функції ПЗ		Критерії (варіанти реалізації функцій) ПЗ		
Назва функції	Ідентифікатор	Варіант	Назва коефіцієнту критерію	Ідентифікатор
Застосування моделі даних та забезпечення взаємодії ПЕОМ у мережі	F_1^2	а	застосування об'єктно-реляційної моделі даних	K_1^2
		б	застосування реляційної БД стандартного типу	K_2^2
Реалізації функціональних можливостей	F_2^2	а	реалізації процедури оптимізації запитів	K_3^2
		б	реалізації процедури підтримки мережних протоколів	K_4^2
		в	реалізації процедури розподіленої обробки даних	K_5^2
		г	реалізації процедури зберігання (обробки) мультимедійних і геопросторових даних	K_6^2
		д	реалізації процедури багатомірного аналізу інформації	K_7^2
Забезпечення надійної експлуатації	F_3^2	а	забезпечення відновлення після збоїв	K_8^2
		б	забезпечення резервного копіювання та відновлення змін	K_9^2
		в	забезпечення захисту від несанкціонованого доступу	K_{10}^2

множини критеріїв K_k^2 , $k = \overline{1, l}$ які характеризують властивості конкуруючих ПЗ _{i} та необхідні для комплексного оцінювання їх якості за кожною функцією.

Для обраних ПЗ _{i} , $i = \overline{1, n}$ (наприклад, $n = 3$) ґрунтуючись на гіпотезі Міллса про те, що експерт одночасно враховувати не більш ніж 7 ± 2 елементи, обмежимося 3 функціями ($m = 3$) та не більше ніж 5 критеріями для кожної з цих функцій (загалом $l = 10$).

Крок 3.3. Проведення за спеціальною вербально-числовою шкалою попарного порівняння (ПП) як самих ПЗ _{i} , так і притаманних ним функцій F_j^2 та критеріїв (варіантів реалізації кожної з цих функцій) K_k^2 , $k = \overline{1, l}$ ($l = 10$) шляхом заповнення матриць (1) та отримання: матриці ПП функцій F_j^2 , $j = \overline{1, m}$; матриць ПП критеріїв K_k^2 , $k = \overline{1, l}$ за кожною функцією окремо; матриці ПП усіх критеріїв K_k^2 , $k = \overline{1, l}$ між собою; матриці ПП ПЗ _{i} , $i = \overline{1, n}$ за кожним критерієм.

Визначення власних значень кожної із сформованих матриць, їх максимальних значень та відповідних цим значенням власних векторів.

Крок 3.4. Формування морфологічної карти альтернативних ПЗ _{i} , $i = \overline{1, n}$ та визначення як раціонального варіанту реалізації їх основних функцій та/або критеріїв, так й ПЗ ПР в якому цей варіант реалізовано найліпшим чином.

Крок 3.5. Формування позитивно-негативної матриці варіантів реалізації функцій ПЗ _{i} , $i = \overline{1, 3}$, обраних для порівняння (табл.3). Ті з варіантів, які мають суттєві недоліки або з різних причин не відповідають технічним умовам виключаються з подальшого розгляду. Інші підлягають техніко-економічному порівняльному оцінюванню.

Крок 3.6. Обрання потенційно можливих варіантів реалізації функцій на підставі їх порівняльного аналізу за перевагами і недоліками (табл. 3) та коефіцієнтами вагомості їх критеріїв - φ_k , $k = \overline{1, l}$ (наприклад, $l = 10$), сформованими у виді власного вектору матриці



ПП усіх критеріїв K_k^2 між собою, наприклад:

$$\begin{aligned} & 1) F_1^2 a + F_2^2 b + F_3^2 a; \quad 2) F_1^2 a + F_2^2 b + F_3^2 b; \\ & 3) F_1^2 a + F_2^2 b + F_3^2 c; \quad 4) F_1^2 a + F_2^2 c + F_3^2 a. \end{aligned} \quad (10)$$

Таблиця 3

Приклад формування позитивно-негативної матриці варіантів реалізації функцій ПЗ

Функції ПЗ	Варіанти реалізації функцій	Переваги	Недоліки
F_1^2	а	Простота доступу до інформації, мінімальний час звернення	Дублювання інформації при багатомашинному варіанті
	б	Унікальність інформації, менший об'єм пам'яті	Ускладнення доступу до інформації, збільшення часу звернення
F_2^2	а	Збільшення швидкості обробки інформації	Можливість втрати інформації при збоях
	б	Максимальна наочність інформації, що відображується	Зменшення швидкості обробки інформації
	в	Повне відображення інформації по одному об'єкту	Відсутність інформації по іншим об'єктам
	г	Зменшення імовірності втрати інформації при збоях	Складність реалізації
	д	Можливість порівняння інформації по декількох об'єктах	Часткове відображення інформації
F_3^2	а	Простота і зручність роботи з програмою	Збільшення об'єму програми
	б	Простота і швидкість навчання роботи з програмою	Збільшення об'єму програми
	в	Можливість використання в багатьох програмних комплексах	Збільшення необхідного об'єму оперативної пам'ятуючого пристрою

Крок 3.7. Обчислення коефіцієнтів рівня якості ПЗ ПР за кожним критерієм кожної функції

$$K_k^{ПЗ} = \sum_{k=1}^l \varphi_k \cdot B_{kj}, \quad j = \overline{1, m} \quad (\text{наприклад, } m = 3) \quad (11)$$

де l – кількість критеріїв конкуруючих ПЗ ПР, які прийняті для оцінювання, $l = 10$;

B_{kj} – бальна оцінка k -го критерію j -ї функції якості ПЗ ПР (визначається експертами).

Крок 3.8. Обчислення за формулами (10) узагальнюючих показників рівня якості ПЗ ПР для кожного k -го критерію (варіанту реалізації) j -ї функції окремо по кожній функції:

$$K_{ПЗ_j} = K_{kj}^{ПЗ} [F_{1k}] + K_{kj}^{ПЗ} [F_{2k}] + \dots + K_{kj}^{ПЗ} [F_{mk}], \quad (12)$$

де $j = \overline{1, m}$ (наприклад, $m = 3$), $k = \overline{1, l}$ (наприклад, $l = 10$).

Крок 3.9. Формування вектору власних значень матриць попарного порівняння критеріїв K_k^2 , $k = \overline{1, l}$ ($l = 10$) за кожною із функцій F_j^2 , $j = \overline{1, m}$ ($m = 10$), тобто їх локальних пріоритетів та матриці $ПЗ_{ik}$, сформованої з власних векторів матриць попарних порівнянь $ПЗ_i$, $i = \overline{1, n}$ ($n = 3$) за кожним із критеріїв K_k^2 , $k = \overline{1, l}$ ($l = 10$). Формування власного вектору локальних пріоритетів критеріїв, що використовуються під час порівняння ПЗ ПР - $ХПП_k$.

Крок 3.10. Обчислення глобальних пріоритетів $ПЗ_i$, $i = \overline{1, n}$, що дозволять визначити місце кожного з ПЗ ПР серед порівнюваних та визначення їх узагальнених показників якості:

$$\begin{aligned} ПЗ_i^{glpr} &= \sum_{k=1}^l (ПЗ_{ik} - ХПП_k) \cdot 100; \\ ПЗ_i^{\Sigma} &= ПЗ_i^{glpr} / \min(ПЗ^{glpr}) \end{aligned} \quad (13)$$

Висновок. За сукупністю функцій і критеріїв, перелічених у табл.2 та з врахуванням, як їх важливості на очікуваний результат, так й суджень абонентів щодо важливості критеріїв, кращим серед конкуруючого ПЗ ПР вважатиметься варіант для якого коефіцієнт функціональності $K_{ПЗ}^{fynkc} = \max_{1 \leq j < m} K_{ПЗ_j}$, а коефіцієнт раціональності $K_{ПЗ}^{racion} = \max_{1 \leq i < n} ПЗ_i^{\Sigma}$.

Етап 4. Комплексним рішенням щодо формування типового варіанту побудови ПГ АСУ

ОКІ є процедура, яка за рахунок застосування критеріїв, обчислених на попередніх етапах роботи та які найбільш повно характеризують конкретну АСУ ОКІ з точки зору її топології, архітектури (АРМ) та ПЗ, а також властивих для неї функцій, дозволяє серед низки альтернативних обрати найкращий (раціональний) варіант побудови АСУ. Найбільш ефективним при вирішенні цього завдання є метод Дельфі (рис.2).

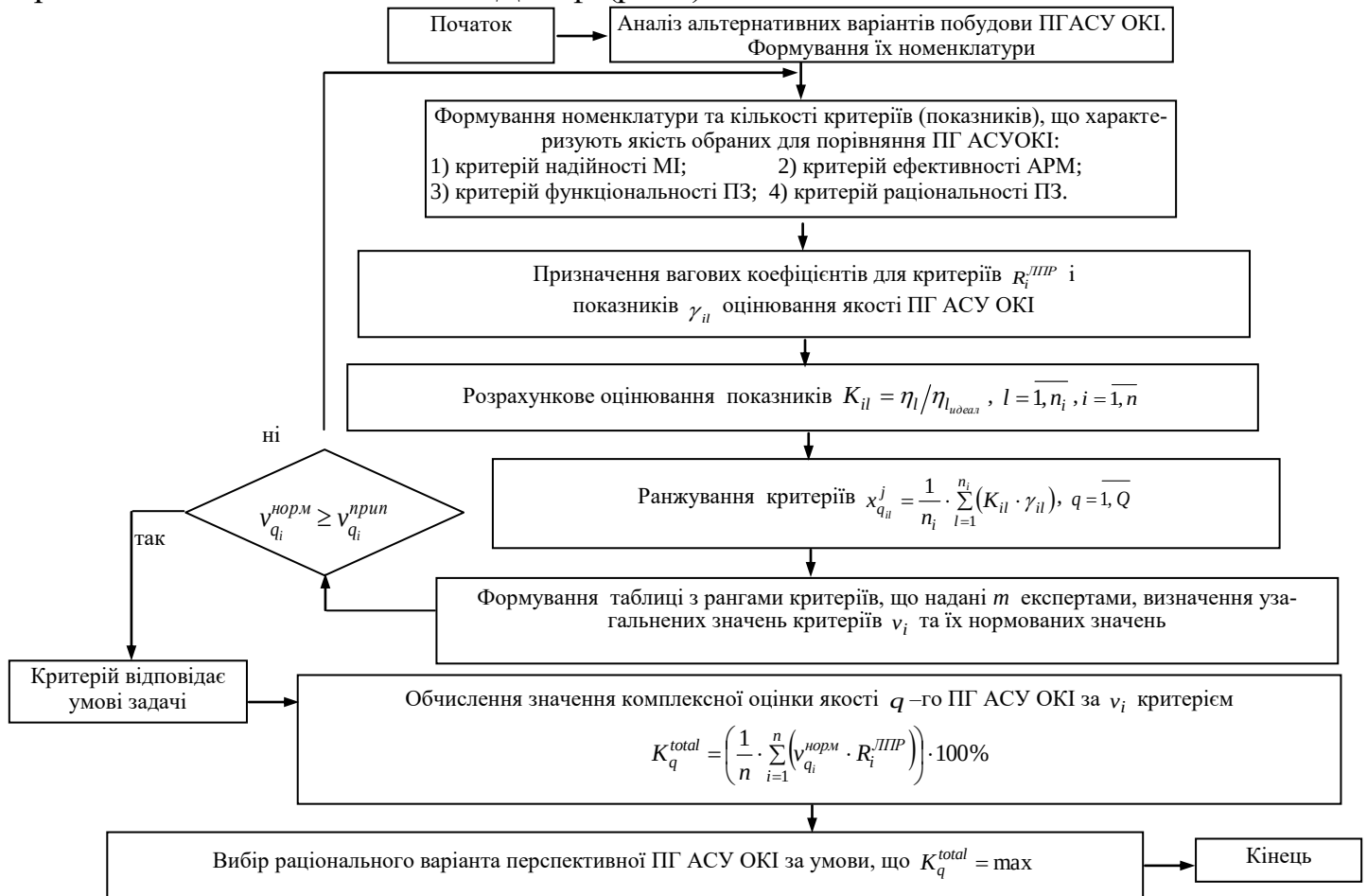


Рис. 2. Структурно-логічна схема алгоритму вибору типового варіанту побудови ПГ АСУ ОКІ

Крок 4.1. Структурування проблеми вибору раціонального варіанту для створення перспективної гарантоздатної АСУ ОКІ у вигляді ієрархії та виявлення її найбільш важливих елементів, а саме множин:

критеріїв R_j , $j = \overline{1, m}$ ($m = 4$) щодо надійності МІ (K_{MI}^{nad}), ефективності АРМ ($K_{АРМ}^{eff}$), функціональності ($K_{ПЗ}^{fynkc}$) та раціональності ($K_{ПЗ}^{racion}$) ПЗ серед яких необхідно вибрати найкращий;

показників Y_i , $i = \overline{1, n}$ ($n = 12$), що характеризуватимуть критерій Y_j (готовності, безперебійності, відновлюваності, доступності, змінюваності, змінюваності, вивчає мості, адаптованості, простоти інсталяції, відкритості, забезпечення єдиного ТК простору та захищеності).

Крок 4.2. Призначення за спеціальною вербально-числовою шкалою вагових коефіцієнтів важливості для γ_{il} - l -го показника i -го критерію і R_i -го критерію. При цьому слід враховувати, що вага найменш відповідальної ознаки має дорівнювати одиниці.

Крок 4.3. Оцінювання l -го показника i -го критерію - K_{il} з погляду повноти реалізації властивої йому функції за формулою: $K_{il} = \eta_l / \eta_{l_{ideal}}$, де $i = \overline{1, n}$, $l = \overline{1, n_i}$; $K_{il} \in [0, 1]$

де η_l – рахункова кількість одиниць l -го показника i -го критерію, що характеризують повноту реалізації тієї або іншої функції; $\eta_{l_{ideal}}$ – ідеальна кількість таких одиниць (повинна бути визначена в технічних умовах на створення МІ та відповідному технічному завданні); n – кількість критеріїв;

n_i – кількість показників i -го критерію.

Крок 4.4. Проведення комплексної оцінки i -го критерію. При цьому x_{qil}^j – ранг i -го критерію по альтернативному рішенню q , приписуваний j -м експертом обчислюється за формулою:

$$x_{qil}^j = \frac{1}{n_i} \cdot \sum_{l=1}^{n_i} (K_{il} \cdot \gamma_{il}) , \quad q = \overline{1, Q} , \quad j = \overline{1, m} \quad (15)$$

де γ_{il} – ваговий коефіцієнт важливості l -го показника i -го критерію; Q – кількість АСУ, що підлягають оцінюванню.

Крок 4.5.

- формування узагальненої таблиці з комплексних оцінок i -х критеріїв для досліджуваної АСУ, отриманих кожним з m експертів у ході виконання попередніх етапів роботи,

- сумарне ранжування $\sum_{j=1}^m x_{q_1}^j, \sum_{j=1}^m x_{q_2}^j, \dots$ за альтернативним рішенням q , де x – ранг i -го критерію по альтернативному рішенню q ($q = \overline{1, Q}$), приписуваного j -м експертом ($j = \overline{1, m}$).

- визначення коефіцієнта згоди W_q між існуючими думками фахівців та формування вектору ваг відповідальності критеріїв у процесі прийняття рішення - x_Σ ;

- визначення значення комплексної оцінки i -го критерію та їх ваги.

Крок 6. Обчислення комплексного показника якості досліджуваної АСУ K_q^{total} за кожним q -м альтернативним рішенням щодо її побудови за формулою:

$$K_q^{total} = \left(\frac{1}{n} \cdot \sum_{i=1}^n (v_{q_i}^{норм} \cdot R_i^{ОПР}) \right) \cdot 100\% \quad (16)$$

де $v_{q_i}^{норм}$ – нормована вага i -го критерію ($i = \overline{1, n}$); $R_i^{ОПР}$ – середнє значення вагового коефіцієнта важливості кожного критерію (властивості), визначене m незалежними експертами: $R_i^{ОПР} = \sum_{j=1}^m R_{ij}^{норм} / \sum_{j=1}^m \sum_{i=1}^n R_{ij}^{норм}$; $R_{ij}^{норм}$ – нормована вага i -го критерію (властивості) за q -м альтернативним рішенням побудови АСУ, приписувана j -м експертом $R_{ij}^{норм} = R_{ij} / \sum_{i=1}^n R_{ij}$ ($j = \overline{1, m}$).

Висновок. Якщо розгляду підлягає q альтернативних варіантів рішень побудови АСУ, то остаточний вибір серед них раціонального буде здійснюватися на підставі наступного правила: якщо $K_q^{total} \geq K_{q+1}^{total}$, то q -й варіант АСУ є більше якісним у порівнянні з $q+1$ та навпаки. За раціональний серед порівнюваних варіантів ОПР, шляхом урахування рівнів впливу кожного критерію на якість функціонування комплексу й чутливості комплексних показників якості, обирає в якості типового той варіант побудови ПГ АСУ ОКІ, якому відповідає $K_q^{total} = \max$.

Це дозволить ПГ АСУ ОКІ якісно задовольняти потреби користувачів у поданні повної і достовірної інформації та її ефективної обробки, а також гарантовано надавати необхідні послуги/сервіси та виконувати потрібні функції в заданих режимах і умовах застосування.

В третьому розділі описано **метод визначення впливу загроз на процеси функціонування ПГ АСУ ОКІ**. Метод поєднує в собі семантичну модель протидії системи захисту ПГ АСУ ОКІ з атакуючою стороною, процедуру детектування та відновлення даних в системі та модель оцінки стану захищеності системи від загроз порушення ЦКД, які ґрунтуються на частковій моделі загроз безпеці ПГ АСУ ОКІ.

Етап 5. Зважаючи на те, що інструментом реалізації загроз щодо АСУ ОКІ є атаки, які здійснюються, наприклад, з метою крадіжки інтелектуальної власності та гальмування інформаційних або технологічних процесів, тощо – ключовим елементом методу є семантична модель протидії системи захисту ПГ АСУ ОКІ з атакуючою стороною.

Найбільш поширеними, як відомо, останнім часом є DDoS-атаки, що формують сотні запитів різних типів, -

Таблиця 4

Семантична модель протидії захисту АСУ ОКІ та атакуючої сторони

Дія	Час початку	Етап	Методика дій захисту АСУ ОКІ
A_1	t_1	Вибір об'єкту атаки	Апріорна оцінка загрози
A_2	t_2	Пошук вразливості	Моніторинг портів та підключення пристроїв
A_3	t_3	Вбудовування Backdoor (лазівки), модифікація коду системи	Контроль несанкціонованих дій
A_4	t_4	Завантаження та запуск шкідливого коду	Контроль НСД, обчислення функції прийняття рішення
A_5	t_5	Активізація асиметричного перетворення, виклик стандартних функцій PRNG, CryptoAPI тощо	Контроль, перехоплення звернень, підміна фіктивної функцією
A_6	t_6	Активізація симетричного перетворення, виклик стандартних функцій PRNG, CryptoAPI тощо	Контроль, перехоплення звернень, підміна фіктивної функцією
A_7	t_7	Читання файлів за переліком форматів (розширень)	Контроль і управління доступом
A_8	t_8	Заміна розширення зашифрованого файлу на нестандартний формат	Контроль та блокування процесу
A_9	t_9	Знищення ключових даних шляхом звернення к відповідним функціям	Контроль та блокування процесу
A_{10}	t_{10}	Відправлення зашифрованих даних зловмиснику	Контроль та блокування процесу
A_{11}	t_{11}	Перезавантаження системи	Контроль та блокування процесу
		Закінчення атаки	Пошук ключів у ОЗП, RAM

якими атакується вузол-мішень. Це стосується й атак, що виявляються в криптографічних ПЗ реалізації атак та які не були виявлені під час їх проектування.

З врахуванням часткової моделі загроз безпеці ПГ АСУ ОКІ семантична модель протидії матиме вид, поданий в табл.4. Для її часових інтервалів характерні такі обмеження:

$$\begin{cases} t_{11} - t_1 \leq T_{\text{атаки, max}} \\ t_{i+1} - t_i \leq \Delta_i \end{cases},$$

де $T_{\text{атаки, max}}$ – загальна тривалість атаки, Δ_i – середній час між її етапами.

За цих умов на кожному етапі $\{A_i, i = \overline{1, 11}\}$ функції прийняття рішення про атаку:

$$\vartheta_i(A_1, \dots, A_i) = \begin{cases} 1, \text{ якщо приймається рішення про атаку} \\ 0, \text{ в іншому випадку} \end{cases} \quad (17)$$

При цьому вплив шкідливих програм на інформаційні процеси в гарантоздатних АСУ ОКІ може бути представлено наступною послідовністю кроків:

Крок 1. Перехоплення управління шляхом передачі помилкового запиту базового модулю ОС функцій на обслуговування переривань з виконання програм;

Крок 2. Відновлення початкового вигляду програми, в яку впроваджено шкідливі програми, фальшиве ПЗ та зловісні шифруючі коди;

Крок 3. Інфікування оперативної пам'яті комп'ютера;

Крок 4. Виконання шкідливих функцій з протиправного маніпулювання інформацією;

Крок 5. Повернення управління основній програмі.

Так як при виконанні даних кроків шкідливі програми (фальшиве ПЗ, зловісні шифруючі коди) реалізують системні функції, операції виявлення повинні проводитися тільки компонентами ОС під управлінням її базового модуля. При цьому еталонна послідовність контрольних точок також повинна бути надійно захищеною.

Висновок. Впровадження моделі дозволило відслідковувати вплив шкідливих програм, фальшивого ПЗ і зловісних шифруючих кодів на ІТП в АСУ ОКІ та обирати раціональні методи щодо відбиття нападу атакуючої сторони.

Етап 6. Питання щодо детектування та відновлення даних в ПГ АСУ ОКІ на відміну від відомої технології «грубої сили» в роботі вирішене за рахунок розпаралелювання операцій криптоаналізу шляхом кластеризації задачі відновлення зашифрованих даних на групи за методом «найближчого сусіда» так, щоб підзадачі усередині груп були подібні одна з одною, а підзадачі з різних груп суттєво відрізнялися. Вузловим моментом при цьому вважається вибір домінуючої задачі з визначеної вибірки R можливих задач відновлення зашифрованих даних, яка впливатиме на

остаточний варіант розбивки задачі на групи.

Алгоритм вирішення задачі полягає в послідовному виконанні наступних кроків.

Крок 6.1. Формування матриці, елементами якої можуть бути: або альтернативи-критерії C_{ik}^r , якщо використовується якісна шкала, де $k = \overline{1, Q}$ – кількість критеріїв/ознак, $i = \overline{1, N}$ – кількість альтернатив/під задач, або вихідна вибірка даних C_{ik}^r для r -ї задачі відновлення зашифрованих даних ($r = \overline{1, R}$) та p_k ознак по кожній з них, якщо використовується кількісна шкала.

Крок 6.2. Приведення матриці C_{ik}^r до нормального виду.

Крок 6.3. Формування матриці близькості $M^{blizk}(r_i, r_j)$, елементи якої (ρ_{ij}) будуть визначатися як між точкові відстані між пари альтернатив r_i та r_j : $\rho_{ij} = \sqrt{\frac{1}{Q} \sum_{k=1}^Q (C_{ik} - C_{jk})^2}$, $j = (i+1), N$. (18)

Крок 6.4. За матрицею близькості для пари альтернатив/підзадач r_i та r_j :

1) поділ множини з R задач на підвибірки (диполі) близько розташованих підзадач $A \cap B$;
2) довизначення (регуляризація) сформованих кластеризацій A і B шляхом додаткової перевірки та поділу множини підзадач на підмножини $C \cap D$;

3) обчислення міжточкових відстаней для підвибірок $A \cap B$ і $C \cap D$. Це триватиме до тих пір, поки всі задачі не увійдуть до множин $A \cap B$ та $C \cap D$.

Крок 6.5. Здійснення перебору гіпотез про число кластерів H_{AB} для підвибірок $A \cap B$ і H_{CD} для підвибірок $C \cap D$ та обчислюються індекси, що відповідають масивам узгодженості і неузгодженості: $H_{AB} = \frac{h - \Delta h}{h} \rightarrow \min$, $H_{CD} = \frac{h - \Delta h}{h} \rightarrow \min$, де h – кількість усіх кластерів, виділена на вибірках $A \cap B$ та $C \cap D$; Δh – кількість кластерів, що подібні один до одного;

Крок 6.6. Проведення перебору кластеризацій за сумарним критерієм несуперечності H_{Σ} та визначення порогів домінування шляхом порівняння індексів узгодженості – f_{ij}^{yzg} і неузгодженості – f_{ij}^{neyzg} з порогом кластеризації – ρ_{nop} : $H_{\Sigma} = \frac{1}{2}(H_{AB} + H_{CD}) \rightarrow \min$.

Оптимальній кластеризації відповідатиме випадок, коли $H_{\Sigma} \rightarrow 0$. Значення порога кластеризації – ρ_{nop} задається особою, що уповноважена приймати рішення.

Порівняння підзадач з оптимальної кластеризації здійснюється за правилом:

$$\text{якщо } f_{ij}^{yzg} > \rho_{nop} \text{ або } f_{ij}^{neyzg} < \rho_{nop}, \text{ то } r_i > r_j. \quad (19)$$

Висновок. Отриманий результат щодо раціонального розподілу множини з R задач на групи та формування деревоподібної ієрархічної структури з N підзадач в кожній суттєво залежатиме від таких факторів: відсутності однозначно найкращого критерію якості кластеризації; невизначеності щодо попередньої кількості кластерів відносно деякого критерію; залежності результату кластеризації від міри близькості задач щодо відновлення зашифрованих даних, вибір якої також суб'єктивний і визначається експертом.

Етап 7. Комплексним рішенням щодо визначення впливу загроз на процеси функціонування ПГ АСУ ОКІ є модель оцінки стану її захищеності від загроз порушення цілісності, конфіденційності та доступності (рис.3), яку реалізовано в роботі шляхом структуризації можливих загроз за потенційними наслідками та умовами подолання ними відповідних рубежів захисту. В моделі вирішуються дві групи задач:

по-перше, оцінювання стану захищеності обраного варіанту побудови перспективної гарантоздатної АСУ ОКІ від стороннього кібернетичного впливу;

по-друге, забезпечення АСУ ОКІ від НСД до її ресурсів та інформації, що в ній циркулює.

При цьому стан захищеності обраного варіанту побудови перспективної гарантоздатної АСУ ОКІ від стороннього кібернетичного впливу та загроз, що класифікуються за метою реалізації може бути, як результат, знайдений з наступного виразу:

$$P_{\text{стан.захищ.}}^{K_{\text{total}}} = 1 - (1 - P_{\text{поруш.}}^{\text{конфіден.}}) \cdot (1 - P_{\text{поруш.}}^{\text{цілісн.}}) \cdot (1 - P_{\text{поруш.}}^{\text{доступ.}}), \quad (20)$$

де $P_{\text{поруш.}}^{\text{доступ.}} = 1 - (1 - P_{\text{рес.}}^{\text{викор.}}) \cdot (1 - P_{\text{ссуд}})$ - ймовірність порушення доступності ресурсу;

$P_{\text{рес.}}^{\text{викор.}} = 1 - p_0 = 1 - \exp \left\{ -t_{\text{рес.}}^{\text{викор.}} \cdot \lambda_{\text{зп}} \right\}$ - ймовірність використання ресурсу;

$t_{\text{рес.}}^{\text{викор.}} = (T_{ki} - \Delta T_{ki}) / n_{io}$ - середній час використання ресурсу;

$T_{ki}, \Delta T_{ki}$ - періодичність і тривалість контролю цілісності;

n_{io} - кількість інформаційних об'єктів, що потребують використання на $(T_{ki} - \Delta T_{ki})$;

$\lambda_{\text{зп}}$ - загальна інтенсивність впливів;

$P_{\text{ссуд}} = 1 - P_{\text{нсд}}$ - ймовірності не подолання системи управління доступом;

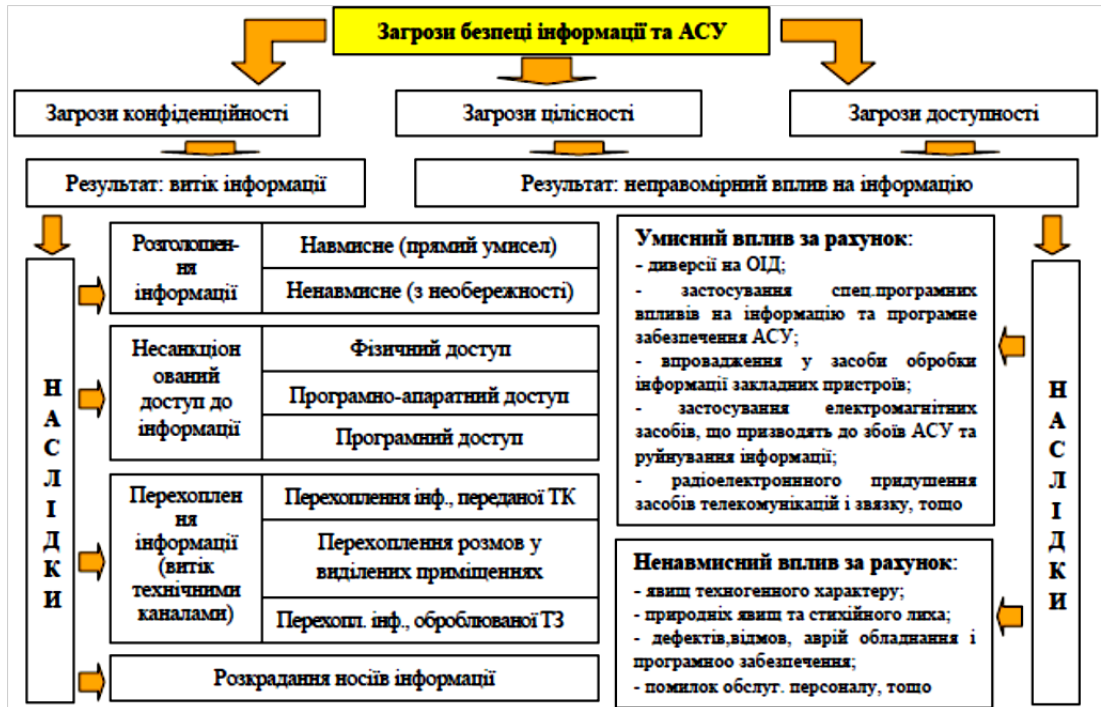


Рис.3. Загрози безпеці інформації в АСУ та їх можливі наслідки

$P_{\text{поруш.}}^{\text{цілісн.}} = P_{\text{кпці}} [1 - (1 - P_{\text{нсд}}) \cdot (1 - P_{\text{зсвтк}}) \cdot (1 - P_{\text{зцзмі}})]$ - ймовірність порушення цілісності інформації;

$P_{\text{зцзмі}}$ - ймовірність подолання засобів захисту від загроз мережевої інфраструктури;

$P_{\text{зсвтк}}$ - ймовірність подолання засобів захисту від спеціальних впливів ТК;

$P_{\text{нсд}}$ - ймовірність отримання порушником НСД до ресурсів АСУ та/або інформації за рахунок подолання засобів управління доступом: $P_{\text{нсд}} = P_{\text{пазуд}} \cdot [1 - (1 - P_{\text{озод}}) \cdot (1 - P_{\text{фзод}}) \cdot (1 - P_{\text{пзіак}})]$;

$P_{\text{пазуд}} = P_{\text{азуд}} \cdot P_{\text{пзад}}$ - ймовірність подолання порушником ПАЗ управління доступом;

$P_{\text{азуд}}$ - ймовірність подолання апаратних засобів управління доступом (брандмауерів);

$P_{\text{пзад}}$ - ймовірність подолання ПЗ адміністрування доступу на ресурсів АСУ;

$P_{\text{озод}}$ - ймовірність подолання організаційних заходів обмеження доступу до АСУ;

$P_{\text{фзод}}$ - ймовірність подолання фізичних заходів обмеження доступу до АСУ;

$P_{\text{пзіак}}$ - ймовірність подолання ПЗ ідентифікації та автентифікації користувачів;

$P_{\text{кпці}}$ - ймовірність подолання засобів контролю та поновлення цілісності інформації;

$P_{\text{поруш.}}^{\text{конфід.}} = 1 - (1 - P_{\text{нсд}}^{\text{кці}}) \cdot (1 - P_{\text{аззкв}}) \cdot (1 - P_{\text{пззга}})$ - ймовірність порушення конфіденційності інформації;

$P_{\text{нсд}}^{\text{кці}} = P_{\text{нсд}} \cdot P_{\text{кці}}$ - ймовірність отримання порушником НСД до ресурсів АСУ та/або інформації;

$P_{\text{кці}} = P_{\text{мова}} \cdot P_{\text{пзктп}} \cdot P_{\text{ключі}}$ - ймовірність подолання системи криптографічного захисту;

$P_{\text{мова}}$ - ймовірність того, що порушник знає мову, якою інформація подається;

$P_{\text{пзктп}}$ - ймовірність того, що порушник може застосовувати ПЗ або апаратуру криптоперетворення;

$P_{\text{ключі}}$ - ймовірність того, що порушник має ключі або ключові набори для криптоперетворення;

$P_{\text{аззкв}}$ - ймовірність того, що порушник знає апаратні засоби захисту каналів витоку інформації;

$p_{пзвга}$ - ймовірність того, що порушник знає ПЗ захисту від вірусних атак.

На підставі отриманих результатів особа, що приймає рішення зможе сформулювати рекомендації з вибору методів, заходів та механізмів забезпечення гарантоздатності АСУ ОКІ в сенсі забезпечення цілісності, конфіденційності та доступності (рис.4).

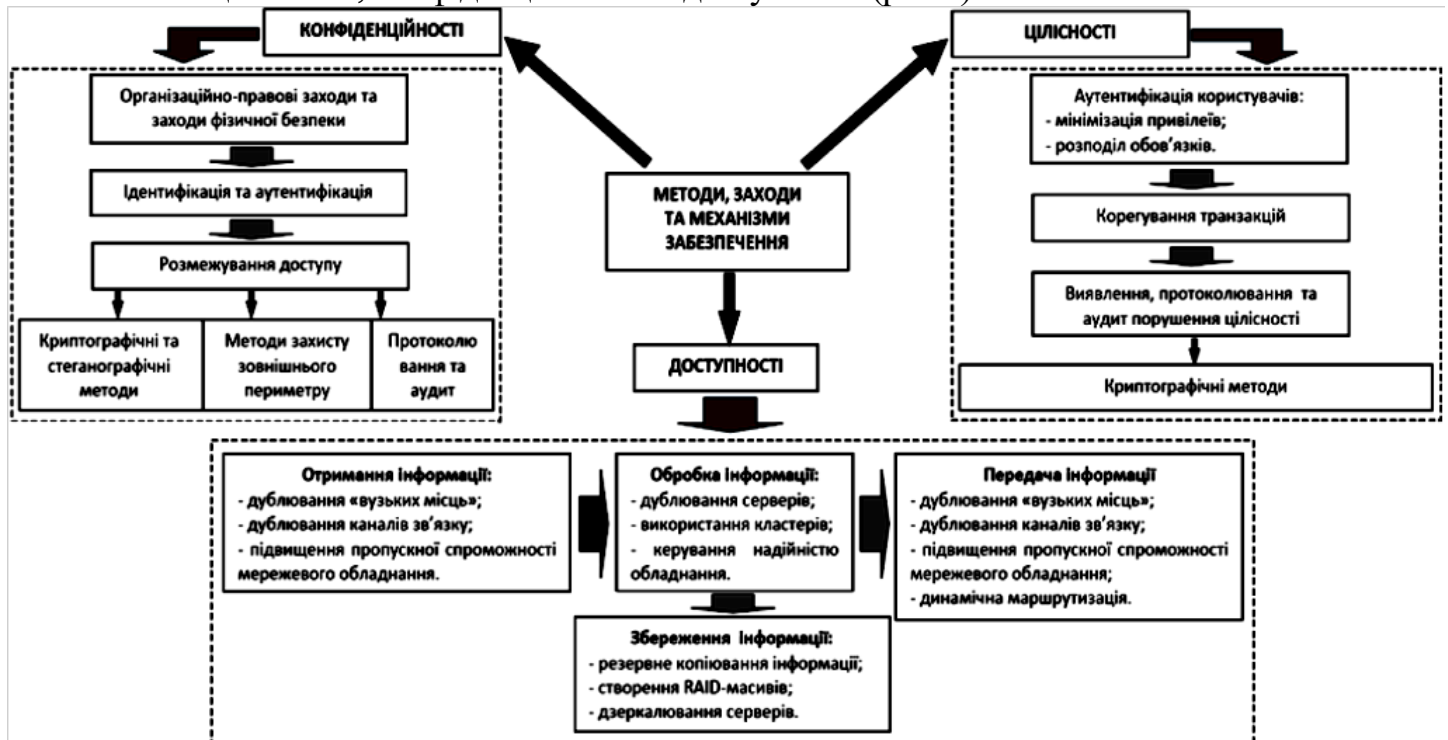


Рис.4. Методи, заходи та механізми забезпечення цілісності, конфіденційності та доступності в АСУ ОКІ

Висновок. Структуризація загроз порушення ЦКД за можливими наслідками та умовами подолання ними відповідних рубежів захисту, дозволила: створити передумови для ефективного оцінювання подій, які шляхом потенційно можливого впливу на АСУ прямо або опосередковано можуть завдати збитку її власникам і користувачам й, на відміну від існуючих, оцінити стан захищеності перспективної гарантоздатної АСУ ОКІ від стороннього кібернетичного впливу за комплексним показником $P_{стан.захищ}^{K_q^{total}}$ та убезпечити АСУ ОКІ від НСД до її ресурсів та інформації, що в ній циркулює.

Четвертий розділ присвячено дослідженню процедур, розроблених в процесі побудови інформаційної технології для створення ПГ АСУ ОКІ.

З метою вибору прототипу топології мережевої інфраструктури в роботі, як приклад, було проведено порівняльне оцінювання альтернативних топологій, а саме шинної, кільцевої, зіркової та стільникової. Результати експериментальних досліджень з вивчення процесів їх функціонування та результати обчислення їх глобальних пріоритетів, виконаних за формулою 2, – подано на рис.5.



Рис.5. Результати експериментальних досліджень з вивчення процесів функціонування можливих варіантів топологій МІ

За сукупністю показників (табл.1) та з урахуванням їх важливості на очікуваний результат серед альтернативних найбільш раціональним варіантом при створенні МІ перспективної гарантоздатної АСУ ОКІ є топологія типу «зірка». Її ваговий коефіцієнт становить: $K_{MI}^{nad} = AB_{glpr}^{max} = 3.864$. Це, як наслідок, підтверджує рішення, отримане в умовах невизначеності.

Процедуру вибору типового АРМ раціональної конфігурації для комплектування ПГ АСУ ОКІ в роботі було апробовано при оцінюванні можливих конфігурацій системного блоку (СБ), табл.5. Оцінювання СБ проводилось за тактовою частотою процесора (ГГц) та шини (МГц), обсягами ОП (Мб) та HDD (Гб), а також швидкістю HDD.

Таблиця 5
Параметри оцінювання системних блоків та їх значення

№	Тактова частота процесора, ГГц	Тактова частота шини, МГц	Обсяг ОП, Мб	Обсяг HDD, Гб	Швидкість HDD	Продуктивність, %	Ціна, \$
1	Athlon XP1 1800+	333	1 x 128 DIMM	40	7200	60	296
2	Athlon XP1 2400+	333	512 DDR	80	7200	95	320
3	Celeron 433	133	1 x 64 DIMM	10	5400	20	89
4	Celeron 633	133	1 x 128 DIMM	10	7200	30	145
5	Celeron 1000	233	1 x 128 DIMM	10	7200	40	159
6	Celeron 1700	333	1 x 256 DDR	80	7200	55	283
7	Celeron 2000	333	1 x 256 DDR	120	7200	60	296
8	Celeron 2400	333	1 x 256 DDR	80	7200	60	336
9	Celeron 2400	333	1 x 512 DDR	120	7200	70	490
10	P 4-1800	533	1 x 256 DDR	120	7200	92	395
11	P 4-2000	533	1 x 128 DDR	40	7200	95	318
12	P 4-2400	800	1 x 512 DDR	80	7200	100	510

Аналіз даних, наведених у табл.5, дозволив зробити висновок про те, що одною з кращих (серед оцінюваних) конфігурацій системного блоку є варіант під № 12 – P 4 - 2400. Показник його продуктивності $P_{max}^{produkt}$ було прийнято за 100% й відносно нього обчислено значення показників продуктивності інших конфігурацій СБ АРМ з табл. 5. Графік залежності показників продуктивності від відповідних ним значень ціни подано на рис. 6.



Рис. 6. Параметри оцінювання системних блоків та їх значення)

Прийняття рішення щодо вибору типового АРМ раціональної конфігурації здійснено в роботі за безрозмірним розрахунковим коефіцієнтом $K_{max}^{окупн} = 0.9$, що дозволяє оцінити рівень окупності капітальних вкладень на його впровадження, передусім програмних і технічних засобів. При цьому $K_{APM}^{eff} = K_{max}^{окупн}$.

Результатом експериментального вирішення задачі раціонального вибору, наприклад, серед конкуруючих СУБД такої, яка б за параметрами та функціями відповідала вимогам користувача, стало обчислення показників рівня якості варіантів реалізації їх основних функцій (табл.6) та їх глобальних пріоритетів (2), що подано на рис.7.

Функції ПЗ $j=1,3$	Критерії ПЗ $k=1,10$	Абсолютне значення j -ї функції, A_j	Бальна оцінка k -го критерію j -ї функції B_{kj}	Коефіцієнт вагомості k -го критерію, ϕ_k	Коефіцієнт рівня якості k -го критерію, $K_k^{ПЗ}$ нормований
F_1^2	а	4	7	0,165	0,114
	б	6,5	2	0,1	0,051
F_2^2	а	16	5	0,174	0,166
	б	0,1	5	0,098	0,091
	в	0,9	9	0,085	0,141
	г	1200	6,5	0,165	0,199
F_3^2	д	100	4	0,023	0,032
	а	1	8	0,034	0,091
	б	0,6	6	0,093	0,097
	в	1	9	0,063	0,018

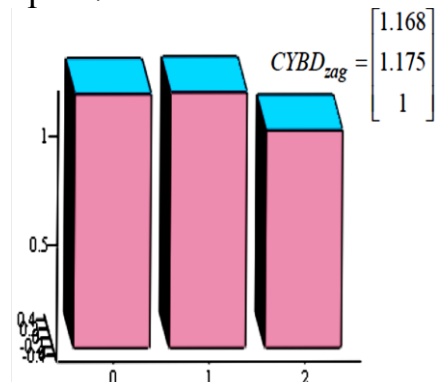


Рис.7. Результати експериментальних досліджень щодо визначення рівня якості критеріїв оцінювання ПЗ ПР на прикладі СУБД та значень їх глобальних пріоритетів

За сукупністю функцій і критеріїв, перелічених у табл.2 та з врахуванням як їх важливості на очікуваний результат, так й суджень абонентів щодо важливості критеріїв, кращим серед конкуруючих СУБД вважатиметься варіант для якого коефіцієнт функціональності $K_{ПЗ}^{func} = \max_{1 < j < m} K_{ПЗ_j} = 0.346$, а коефіцієнт раціональності $K_{ПЗ}^{racion} = \max_{1 < i < n} ПЗ_i^{\Sigma} = 1.175$.

Комплексна оцінка потенційно можливого варіанту побудови ПГ АСУ ОКІ в ході експерименту проводилась з урахуванням значень критеріїв, обчислених на попередніх етапах роботи та які найбільш повно характеризують конкретну АСУ ОКІ з точки зору її топології, архітектури та ПЗ, а також властивих для неї функцій (табл.6).

Таблиця 6

Розрахунок показників рівня якості варіантів реалізації основних властивостей АСУ ОКІ

Критерій оцінки АСУ	Вага критерію оцінки R_i	Показник критерію			Вага показника γ_{il}	Розрахункова оцінка показника			Комплексна оцінка критерію x_{qil}^j	Нормована вага критерію $R_{ij}^{нор}$
		Функція, що притаманна показнику	Міра виміру	Шкала виміру		Рахункова кількість η_l	ідеальна кількість $\eta_{l_{абст}}$	Значення K_{il}^j		
Надійність магістральної МП	$K_{МП}^{nad} = 3.864$	<i>Готовність:</i> готовність до роботи обл. лінійного тракту	імовірність	0.1-0.99	3.53	0.95	0.965	0.98	3.53	0.375
		<i>Безперебійність:</i> середній час між відмовами	год.	200-5000		270.1	277.78	0.97		
		<i>Відновлюваність:</i> середній час відновлення	год.	2-100		6	10	0.6		
Функціональність ПЗ	$K_{ПЗ}^{func} = 0.346$	<i>Доступність:</i> відносний час працездатного функціонування	імовірність	0.1-0.99	1.36	0.89	0.99	0.89	1.36	0.141
		<i>Змінюваність:</i> тривалість підготовки змін	год.	1-1000		100	150	0.67		
		<i>Замінюваність:</i> тривалість заміни компонентів ПЗ	год.	1-100		82	99	0.82		
Раціональність ПЗ	$K_{ПЗ}^{racion} = 1.175$	<i>Вивчаємість:</i> трудомісткість вивчення і застосування ПЗ	чол/год.	1-1000	1.65	100	150	0.67	1.65	0.173
		<i>Адаптованість:</i> трудомісткість адаптації	чол/год.	1-100		97	100	0.97		
		<i>Простота установки:</i> тривалість інсталяції ПЗ	чол/год.	1-100		88	100	0.88		
Ефективність АРМ	$K_{АРМ}^{eff} = 0.9$	<i>Відкритість:</i> можливість роботи у складі АСУ	порядкова	1-10	2.91	10	10	1.0	2.91	0.311
		<i>Забезпечення єдиного ТК простору:</i> внутрішньо системна інформ. зв'язність	порядкова	1-10	4	8	10	0.8		
		<i>Захищеність:</i> багаторівнева система захисту даних	порядкова	1-10	5	7	10	0.7		

Результат обчислення комплексного показника якості ПГ АСУ ОКІ для одного з множини варіантів її побудови подано в табл.7.

Таблиця 7

Параметри оцінювання системних блоків та їх значення)

Запропонований метод, як результат, шляхом урахування рівнів впливу кожного критерію на якість функціонування ПГ АСУ ОКІ та чутливості комплексних показників якості при

зміні суджень учасників експертної групи, дозволяє обрати серед множини альтернативних рішень раціональний варіант побудови системи, здатний гарантовано надавати необхідні послуги та виконувати потрібні функції в заданих режимах і умовах застосування.

Експериментальне дослідження процесу детектування та відновлення даних в ПГ АСУ ОКІ з використанням кластерного аналізу проводилось по вхідній вибірці даних для 11 об'єктів та 5 ознак. Після нормування вхідних даних, обчислення міжточкових відстаней між об'єктами, формування пар диполів, поділу диполів на дві підвибірки $A \cap B$ і $C \cap D$. та обчис-

Критерій (властивість) АСУ ОКІ	Параметри оцінювання системних блоків та їх значення)		Комплексний показник якості досліджуваної АСУ $K_q^{total}, q = 1$
	Нормована вага критерію (властивості) $v_q^{норм}$	Середнє значення вагового коефіцієнта важливості кожного критерію $R_i^{ОПР}$ ($R_i^{нор}$ у випадку безальтерн.варіанту)	
Надійність МП	0.163	0.375	5,61
Функціональність ПЗ	0.325	0.141	
Раціональність ПЗ	0.303	0.173	
Ефективність АРМ	0.209	0.311	

лювання міжточкових відстаней для них, в ході експерименту було побудовано дерева перебору гіпотез про число кластерів для підвбірок A і B та підвбірок C і D (рис.8).

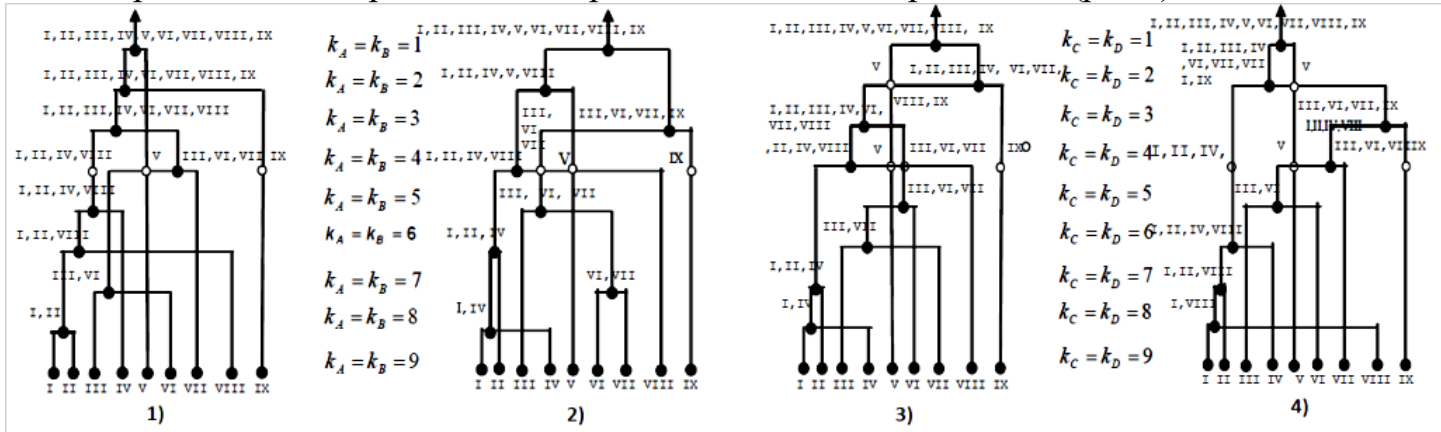


Рис.8. Ієрархічний перебір гіпотез про число кластерів:

1) - для підвбірки A , 2) – для підвбірки B , 3) - для підвбірки C , 4) – для підвбірки D

Результати оптимальної кластеризації подано в таблиці 8.

Таблиця 8

Адреса	Діполя	Об'єкти, об'єднані в кластер	Номер кластера
I II VIII IV	3-8 3-6 8-9 6-8	3,6,8,9	I
V	2-7	2,7	II
III VI VII	4-5 4-11 5-11	4,5,11	III
IX	1-10	1,10	IV

Розпаралелювання операцій криптоаналізу та проведення порівняльного аналізу поділених на групи зашифрованих даних з метою їх подальшого відновлення проводиться в подальшому за кількісними значеннями сумарного критерію несуперечності або індексами домінування. Це дозволило прийняти рішення щодо раціонального розподілу множини з R задач на групи та сформувати деревоподібну ієрархічну структуру з N підзадач в кожній.

Впровадження процедури в загальний процес визначення впливу загроз на процеси функціонування ПГ АСУ ОКІ створило передумови для пошуку вразливостей або істинних значень ключів, застосованих для шифрування даних, а також оцінювання стійкості криптосистем в умовах впливу шкідливих програм, фальшивого ПЗ і зловмисних шифруючих кодів на інформаційно-технологічні процеси в АСУ ОКІ.

ВИСНОВКИ

Результатом виконаної роботи є вирішення актуальної наукової задачі із **розроблення теоретичних і прикладних засад побудови інформаційної технології для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури**, а також визначення впливу на процеси функціонування таких систем антропогенних і техногенних втручань та загроз.

У процесі виконання дисертаційної роботи отримано такі наукові результати.

1. **Метод формування типового варіанту побудови перспективної гарантоздатної АСУ**, що поєднує в собі такі базові процедури, як:

процедура вибору прототипу топології мережевої інфраструктури;

процедура вибору типового АРМ раціональної конфігурації;

процедура раціонального вибору ПЗ прикладного рівня, - що в інтересах створення перспективної АСУ забезпечило доступ до мережі та надання обчислювальних ресурсів і послуг її абонентам для спільного використання ними власних і зовнішніх ІР, забезпечило доступ користувачам до таких ІР, керування їх обміном, передачею та машинною переробкою, дозволило автоматизувати процеси пошуку і збору інформації у зовнішніх і внутрішніх дже-

релах, її реєстрації, трансформації та функціональної обробки, а також процеси захисту ІР в АСУ від кібернетичних загроз.

Комплексним рішенням в межах даного методу, вхідними даними для якого є критерії, що найбільш повно характеризують конкретну АСУ ОКІ з точки зору її топології, архітектури та ПЗ, а також властивих для неї функцій й значення яких було отримано на попередніх етапах роботи, а прийняття рішення щодо вибору раціонального варіанту здійснюється при цьому за безрозмірним показником якості $K_q^{total} = \max$ - є *процедура вибору раціонального варіанту побудови ПГ АСУ ОКІ*. Її застосування дозволить ПГ АСУ ОКІ, як результат, якісно задовольняти потреби користувачів у поданні повної і достовірної інформації та її ефективної обробки, а також гарантовано надавати необхідні послуги/сервіси та виконувати потрібні функції в заданих режимах і умовах застосування.

2. Метод визначення впливу загроз на процеси функціонування перспективних гарантоздатних АСУ ОКІ, який ґрунтується на моделі загроз безпеці автоматизованих систем та поєднує в собі такі базові моделі та процедури, як:

семантична модель протистояння системи захисту АСУ ОКІ та атакуючої сторони;

процедура детектування та відновлення даних в АСУ ОКІ, - що в інтересах створення перспективної АСУ забезпечило відслідковування стороннього кібернетичного впливу на інформаційні і технологічні процеси ОКІ, а також пошуку вразливостей або істинних значень ключів шифрування даних та оцінювання стійкості криптосистем.

Комплексним рішенням в межах розробленого методу є *модель оцінки стану захищеності перспективної гарантоздатної АСУ ОКІ від загроз порушення цілісності, конфіденційності та доступності* яка, на відміну від подібних, дозволяє оцінювати події, що можуть впливати на інформаційно-технологічні процеси ОКІ та прямо або опосередковано завдати збитку її власникам і користувачам, приймати обґрунтовані рішення щодо стану захищеності АСУ ОКІ від впливу кібернетичних атак за комплексним безрозмірним показником $P_{стан.захищ.}^{K_q^{total}}$ та, як результат, убезпечити АСУ ОКІ від НСД до її ресурсів та інформації, що в ній циркулює.

3. Розроблено програмні додатки для проведення імітаційних експериментів.

Як наслідок, отримані в роботі наукові результати, утворюють у своїй сукупності **інформаційну технологію для створення перспективних гарантоздатних АСУ ОКІ**, впровадження якої, на відміну від існуючих, забезпечує гарантоване надання абонентам необхідних послуг та/або сервісів, яким в заданих режимах і умовах застосування з урахуванням стану захищеності таких систем від загроз порушення ЦКД можливо виправдано довіряти. Впровадження означеної ІТ для створення ПГ АСУ ОКІ на прикладі НЕК «Укренерго» окрім всього сприяє (Акт впровадження від 04.01.2021 року):

по-перше, підвищенню ефективності дій осіб, відповідальних за забезпечення безпеки ПГ АСУ ОКІ (за рахунок оперативного визначення найбільш значимих загроз та своєчасного реагування на стан захищеності АСУ від загроз порушення ЦКД) приблизно на 12%;

по-друге, скороченню часу на прийняття виважених управлінських рішень щодо побудови ПГ АСУ ОКІ з відповідним ПАЗ та її впровадженні приблизно на 18 - 20%.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Колективна монографія в іноземному науковому виданні:

1. Dreis Y. A tuple model for estimating the consequences of personal data leakage in automated systems. VIII International conferece of students, PHD-students and young scientists «Engineer of XXI Century». /Y.Dreis, I.Lofova, A.Biskupskyi, **L.Kuzmenko**, Ali .T. Al-Khwalde, A.Korchenko // Processing, transmission and security of information. – Bielsku-Białej:

NATH, 2018. Vol.2. – P. 41–50. ISBN: 978-83-65182-94-4.

2. Sokolov V. Development of low-budget spectrum analyzers for IOT and sensor networks. X International conference of students, PHD- students and young scientists «Engineer of XXI Century». / V. Sokolov, A. Platonenko, **L. Kuzmenko**, V. Buriachok // Projektowanie, badania i eksploatacja. – Bielsku-Białej: NATH, 2020. – P. 331–342. ISBN: 978-83-66249-54-7.

Публікації у наукових фахових виданнях України:

3. Рейш О.Е., Бурячок В.Л., Вертегел С.Г., **Бурячок Л.В.** Методика вибору раціональної топології комп'ютерної мережі перспективних автоматизованих систем управління військами. Труды Академії. – К.: НАО МО України, 2009. – № 2(89). – С. 81–90.

4. Бурячок В.Л., **Бурячок Л.В.** Алгоритм порівняльного оцінювання програмних засобів однакового функціонального призначення для розв'язання завдань інформаційної діяльності. Збірник наукових праць. – К.: НДІ ГУР МО України, 2010. Вип. 27. – С. 124–139.

5. Бурячок В.Л., **Бурячок Л.В.**, Костюк Т.Я. Формування набору показників для оцінювання якості програмного забезпечення сучасних автоматизованих систем. Збірник наукових праць. – К.: НДІ ГУР МО України, 2010. Вип. 28. – С. 111–124.

6. Бурячок В.Л., **Бурячок Л.В.**, Гулак Г.М. Алгоритм вибору АРМ раціональної конфігурації. Сучасний захист інформації. – К.: ДУІКТ, 2011. – № 2. – С. 85–94.

7. Бурячок В.Л., **Бурячок Л.В.**, Костюк Т.Я. Обґрунтування вибору раціональної системи електронного документообігу для державних структур спеціального призначення. Вісник воєнної розвідки. – № 24. – 2011. – С. 67–74.

8. Козачок В.А., Бурячок В.Л., **Бурячок Л.В.**, Складаний П.М. Пентестінг, як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах. Сучасний захист інформації. – К.: ДУТ, 2015. – № 3. – С. 4–12.

9. Бурячок В.Л., Невоїт Я.В., **Бурячок Л.В.** Вплив загроз антропогенного і техногенного характеру на стан безпеки ІТ-систем та соціальних інститутів провідних країн світу і України. Сучасний захист інформації. – К.: ДУТ, 2015. – № 4. – С. 29–43.

10. **Бурячок Л.В.** Стратегія обґрунтування раціонального набору параметрів і функцій програмних засобів спеціального призначення, спрямованих на розв'язання завдань інформаційної діяльності. Сучасний захист інформації. – К.: ДУТ, 2016. – № 3. – С. 3–9.

11. **Бурячок Л.В.**, Бурячок В.Л., Семко В.В. Технологія проведення порівняльного аналізу та оцінювання стану захищеності автоматизованих інформаційних систем. Сучасний захист інформації. – К.: ДУТ, 2016. – № 4. – С. 16–24.

12. Козачок В.А., Рой Я.В., **Бурячок Л.В.** Технології протидії шкідливим програмам та завідомо фальшивому програмному забезпеченню. Сучасний захист інформації. – К.: ДУТ, 2017. – № 2(30). – С. 30–34.

13. V.L.Buryachok, **Kuzmenko L.V.**, Kononenko O.V., Boskin O.O. Features of implementation of the information security policy in the creation of the rational system of electronic documentary cooperation for public and commercial structures of Ukraine. Збірник наукових праць «Системні технології» Національної металургійної академії України. Том 6 (113) 2017. – С. 43–61

14. Гулак Г.М., В.Л.Бурячок, Складаний П.М., **Кузьменко Л.В.** Криптовірологія: загрози безпеки гарантоздатним інформаційним системам і заходи протидії шифрувальним вірусам. Кібербезпека: освіта, наука, техніка. Том 2. №10 (2020). – С. 6 – 28. ISSN 2663 - 4023

Публікації у наукометричних базах Scopus i Web of Science:

15. V. Lakhno, V. Malyukov, N. Mazur, **L. Kuzmenko**, B. Akhmetov. Development of a model for decision support systems for managing the process of investing in information technology. Східно-Європейський журнал передових технологій. ТОМ 1, № 3 (103) (2020), с. 74 – 81. ISSN

(print) 1729-3774, ISSN (on-line) 1729-4061

16. Нашинець-Наумова А.Ю., В.Л. Бурячок, Н.В. Коршун, О.Б. Жильцов, П.М. Складанний, **Л.В. Кузьменко**. Технологія забезпечення інформаційної і кібербезпеки в закладах вищої освіти України. Електронне наукове фахове видання «Інформаційні технології і засоби навчання» Інституту інформаційних технологій і засобів навчання НАПН України. Том 77, № 4 (2020). – С. 337 – 354

17. Feodosiy Kipchuk, Volodymyr Sokolov, Volodymyr Buriachok, Pavlo Skladannyi, **Lidiia Kuzmenko**. Investigation of Availability of Wireless Access Points based on Embedded Systems. Proceedings of the VI International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T'2019), October 8–11, 2019: abstracts. – Kyiv: IEEE, 2019. – P. 246–250

Тези наукових доповідей:

18. Бурячок В.Л., **Бурячок Л.В.**, Боголій С.М. Порівняльне оцінювання програмних засобів однакового функціонального призначення. «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення». V-а НТК ВІТІ НТУУ «КПІ» МО України, 20–21.10.2010 рр. Доповіді та тези доповідей. – К.: ВІТІ НТУУ «КПІ», 2010. – С. 75–76.

19. **Бурячок Л.В.** Класифікація соціотехнічних систем за методом кластеризації кількісних даних. «Проблеми кібербезпеки інформаційно-телекомунікаційних систем». НТК Київського національного університету імені Тараса Шевченка, 10-11.03.2016. Збірник матеріалів доповідей та тез. – К.: НУ ТГШ, 2016. – С. 24–25.

20. Бурячок В.Л., **Бурячок Л.В.**, Гадичький М.Г. Цифрова стратегія безпеки критично важливих об'єктів державної інформаційно-комунікаційної інфраструктури. Матеріали Регіональної конференції МСЕ для країн СНД та Грузії «Перспективи надання послуг на основі мереж пост-NGN, 4G и 5G. Організаційні і технічні рішення щодо їх побудови та захисту», ДУТ, 7-9.06.2017. – К.: ДУТ, 2017. – С. 105–108 (електронний ресурс)

21. **Кузьменко Л.В.**, Бурячок В.Л. Тенденції розвитку та особливості забезпечення безпеки сучасних ІОТ-пристроїв. І міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем». Збірник матеріалів НПК Київського національного університету імені Тараса Шевченка, 05-06.04.2018. – К.: НУ ТГШ, 2018. – С. 264–268

АНОТАЦІЯ

Кузьменко Л.В. Методи і моделі створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 «Інформаційні технології». Інститут телекомунікацій і глобального інформаційного простору НАН України, Київ, 2021.

Дисертаційна робота присвячена вирішенню актуальної наукової задачі, що полягає в теоретичних і прикладних засадах побудови інформаційної технології для створення перспективних гарантоздатних (ПГ) автоматизованих систем управління (АСУ) об'єктів критичної інфраструктури (ОКІ), а також визначення впливу на процеси функціонування таких систем антропогенних і техногенних втручань та загроз.

У роботі розроблено нові та удосконалено існуючі моделі та процедури, що формують базис для двох методів – *методу формування типового варіанту побудови та методу визначення впливу загроз на процеси функціонування ПГ АСУ ОКІ*. В ході роботи над

ними було розроблено процедури вибору прототипу топології мережевої інфраструктури (МІ), вибору типового автоматизованого робочого місця (АРМ) раціональної конфігурації та раціонального вибору програмних засобів (ПЗ) прикладного рівня (ПР), а також семантичної моделі протистояння системи захисту ПГ АСУ ОКІ з атакуючою стороною, моделі оцінки стану захищеності системи від загроз порушення цілісності, конфіденційності і доступності та процедури детектування і відновлення даних в ПГ АСУ ОКІ.

У роботі проведено імітаційні дослідження щодо порівняльного оцінювання та вибору прототипу топології МІ, конфігурації АРМ та системи програмного забезпечення ПГ АСУ ОКІ прикладного рівня. У роботі досліджено можливості застосування кластерного аналізу для розпаралелювання процесів пошуку вразливостей або істинних значень ключів, застосованих для шифрування даних, а також оцінювання стійкості криптосистем від стороннього кібернетичного впливу та криптоперетворень.

Комплексним рішенням в рамках дисертаційного дослідження є інформаційна технологія для створення перспективних гарантоздатних АСУ ОКІ, впровадження якої, на відміну від існуючих: дозволяє оцінювати події, що можуть впливати на інформаційні і технологічні процеси на ОКІ та завдавати збитку як власникам, так і користувачам; забезпечує гарантоване надання абонентам необхідних послуг та/або сервісів, яким в заданих режимах і умовах застосування, з урахуванням стану захищеності таких систем від загроз порушення цілісності, конфіденційності і доступності, можливо виправдано довіряти. Впровадження означеної ІТ окрім всього сприяє: підвищенню, за рахунок оперативного визначення серед множини можливих найбільш значимих загроз, результативності дій осіб, відповідальних за забезпечення безпеки ПГ АСУ ОКІ; скороченню часу на прийняття виважених управлінських рішень щодо побудови ПГ АСУ ОКІ.

Ключові слова: гарантоздатність, критична інфраструктура, комп'ютерна мережа, автоматизоване робоче місце, програмне забезпечення, ефективність, надійність, доступність, цілісність, конфіденційність, інформаційна безпека, функціональна безпека.

ABSTRACT

Kuzmenko LV Methods and models for creating the advanced guaranteed automated systems for managing critical infrastructure. – Manuscript.

The dissertation for the degree of a candidate of technical sciences on the specialty 05.13.06 "Information technologies." Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Kyiv, 2021.

The dissertation is devoted to the solution of the actual scientific problem, which consists in theoretical and applied bases of construction of information technology for creation of perspective guaranteeable (GHG) automated control systems (ACS) of objects of critical infrastructure (CIF), and also definition of influence on processes of functioning of such systems and man-made interventions and threats.

The paper develops new and improved existing models, procedures and algorithms that form the basis for two methods - the method of forming a typical construction option and the method of determining the impact of threats on the operation of GHG ACS CIF. In the course of work on them, the procedures for selecting a prototype of network infrastructure topology (MI), selection of a typical automated workstation (AWP) of rational configuration and rational choice of software, as well as a semantic model of confrontation of ACS protection system were developed. CIF with the attacking side, models for assessing the state of protection of the system

from threats of integrity, confidentiality and availability and the algorithm for detecting and recovering data in the GHG ACS CIF.

The simulation experiments on the comparative evaluation and selection of the prototype of the MI topology, the configuration of the workstation and the software of the GHG ACS of the CIF of the applied level are carried out. The possibilities of application of cluster analysis for parallelization of processes of search of vulnerabilities or true values of keys used for data encryption, and also estimation of stability of cryptosystems from external cybernetic influence and cryptocurrencies are investigated in the work.

A comprehensive solution in the dissertation research is information technology to create promising guaranteed ACS CIF, the implementation of which, in contrast to existing: allows you to assess events that may affect the information and technological processes on the CIF and cause damage to both owners and users; provides guaranteed provision to subscribers of necessary services and / or services, which in the given modes and conditions of application, taking into account the state of protection of such systems from threats of violation of integrity, confidentiality and availability, may be reasonably trusted. The implementation of this IT also contributes to: increase, due to the prompt identification of the set of possible most significant threats, the effectiveness of the actions of persons responsible for ensuring the safety of GHG ACS CIF; reduction of time for making well-considered management decisions on the construction of GHG ACS CIF.

Keywords: warranty, critical infrastructure, computer network, automated workstation, software, efficiency, reliability, availability, integrity, confidentiality, information security, functional security.

Підписано до друку 22.01.2021. Папір офсетний. Ум.-др. арк. 0,9.
Формат 60×90/16. Наклад 110 прим. Замовлення №_____.

Суб'єкт видавничої діяльності занесено до державного реєстру №620049 від 13.10.2008
ПРІНТЦЕНТР, м. Київ, вул. Політехнічна, 16

