МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ПОГАСІЙ СЕРГІЙ СЕРГІЙОВИЧ

УДК 004. 056.53

МОДЕЛІ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В КІБЕРФІЗИЧНИХ СИСТЕМАХ

05.13.21 «Системи захисту інформації»

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
доктора технічних наук

Київ – 2024

Дисертацією є рукопис.

Робота виконана на кафедрі кібербезпеки Національного технічного університету «Харківський політехнічний інститут».

Науковий консультант: доктор технічних наук, професор
Євсеєв Сергій Петрович,
Національний технічний університет
«Харківський політехнічний інститут»,
завідувач кафедри кібербезпеки навчально-наукового інституту комп'ютерних наук та інформаційних технологій

Офіційні опоненти: доктор технічних наук, професор
Хорошко Володимир Олексійович
Національний авіаційний університет,
професор кафедри кафедри інформаційних технологій;

доктор технічних наук, професор
Казакова Надія Феліксівна,
Одеський державний екологічний університет,
завідувач кафедри інформаційних технологій;

доктор технічних наук, професор
Казмірчук Світлана Володимирівна,
Державний університет інформаційно-комунікаційних технологій,
професор кафедри систем та технологій кібербезпеки;

Захист відбудеться «__6__» _грудня_ 2024 року об 11 годині на засіданні спеціалізованої вченої ради Д 26.861.06 у Державному університеті інформаційно-комунікаційних технологій за адресою: 03110, м. Київ, вул. Солом'янська, 7, конференц-зал.

З дисертацією можна ознайомитись у бібліотеці Державного університету телекомунікацій за адресою: 03110, м. Київ, вул. Солом'янська, 7.

Автореферат розісланий «__7__» _листопада_ 2024 року.

Учений секретар
спеціалізованої вченої ради
PhD Віталій МАРЧЕНКО

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Стрімке зростання кількості кіберінцидентів, які стають все більш серйозними, призводить до необхідності підвищення безпеки, особливо у вразливій галузі, якою є кіберфізична система об'єктів критичної інфраструктури. Однією з проблем безпеки критичних інфраструктур є рівень обізнаності про наслідки кібератак. Основною причиною ескалації кібератак у галузі кіберфізичних систем (CPS) може бути те, що більшість систем управління, які застосовуються для CPS, більше не використовують пропрієтарні протоколи та програмне забезпечення, а експлуатують стандартні рішення. В результаті CPS є системами критично важливої інфраструктури та стають більш уразливими й схильними до кіберзагроз, ніж будь-коли раніше. Важливо розуміти, які типи атак відбулися, оскільки це може допомогти спрямувати зусилля щодо кібербезпеки від реальних загроз критичній інфраструктурі.

Кіберпростір значно розширився і перетворився на велику, динамічну та заплутану мережу обчислювальних пристроїв. Ця ситуація також вплинула на системи критичної інфраструктури. Крім позитивних ефектів технологічної експансії, є недоліки. Кіберфізична система є основою повсякденного життя в суспільстві, і тому її належне функціонування має важливе значення. Довгий час найбільш важливі інфраструктурні системи вважалися несприйнятливими до кібератак через їхню залежність від пропрієтарних мереж та обладнання. Проте недавній досвід і кібератаки показують, що це нестійко – перехід до відкритих стандартів та вебтехнологій робить критично важливі інфраструктурні системи більш уразливими.

Ненавмисні або зловмисні дії, здійснені в кіберпросторі, мають наслідки для критичних інфраструктур у фізичному світі. Атаки в кіберпросторі не обмежуються діяльністю уряду з розвідувальною метою. Будь-яка частина CPS від систем життєзабезпечення та комунальних служб до транспортування або постачання товарів першої необхідності може зазнавати атак.

Способи атак на CPS різноманітні та включають прямий або анонімний доступ до захищених мереж через Інтернет і диспетчерський контроль та збір даних (SCADA) або порушення працівниками процедур безпеки. Все це призводить до поширення шкідливих програм усередині брандмауера.

Проблема з аналізом кібератак у галузі CPS полягає в тому, що деякі кібератаки залишаються непоміченими. При цьому деякі організації вкрай неохоче повідомляють про інциденти, вважаючи, що це призводить до потенційних труднощів у веденні бізнесу. Одна з проблем кіберпростору полягає в тому, що боротьба настільки незбалансована і для захисту критично важливої інфраструктури потрібні величезні ресурси, а для початку атаки

необхідно лише один заражений комп'ютерний диск. Таким чином, кіберзахист став одним із найважливіших питань у стратегіях національної оборони.

Оскільки масштаб і природа CPS критичних інфраструктур не дозволяють проводити експерименти, важкість усвідомлення критичних інфраструктур та їх взаємозв'язків, властивостей і стійкості до зловмисних дій, що виникають, направлене на прагнення, яке спрямоване на побудову моделей. Зроблено спробу сформувати концепцію побудови систем безпеки, в основі яких лежить безліч моделей, що описують різні сторони об'єктів критичної інфраструктури. Питанням побудови моделей і систем захисту кіберфізичних систем присвячено велику кількість наукових робіт Сідерс Д., Ройчоудурі Р., Генрі Дж., Бончек Т., Рексфорд Д. та інших вчених. У цих роботах розглядаються питання створення додаткових механізмів виявлення й аналізу трафіку, використання стандартів безпеки у CPS, але при цьому не визначаються контури та платформи CPS, що не дозволяє об’єктивно враховувати можливості цільових (змішаних, APT) атак.

Проблеми побудови систем безпеки CPS на основі використання як сучасних криптосистем, так й систем на основі постквантових алгоритмів досліджують такі вчені, як: Корченко О.Г., Хорошко В.О., Грищук Р.В., Дудикевич В.Б., Савченко В.А., Альшу Х., Лаувенс К., Гарві А., Кон Е. та інші.

Однак при цьому вони розглядають CPS як моносистему, яка не може забезпечувати об’єктивність оцінки можливих загроз та їх наслідків, тому що значною мірою не враховано її розподіл на дві платформи: платформи кіберфізичних систем (датчики, сенсори, системи охорони, відеонагляду тощо) і платформи кіберпростору (яка, у більшості випадків, розташована у хмарі). Крім цього, для забезпечення криптостійкості даних у CPS використовуються симетричні й несиметричні криптосистеми. Однак з появою повномасштабного квантового комп’ютера на основі алгоритмів Шора та Гровера такі системи можуть суттєво знизити рівень стійкості або зламати за поліноміальний час. Таким чином, на підставі проведеного аналізу, результатів вивчення наукових публікацій за темою досліджень, дисертацій, патентів, монографій та практичних розробок встановлено, що на сучасному етапі розвитку прогресивних інформаційних технологій існує об’єктивне протиріччя між системами захисту кіберфізичних систем та новітніми інформаційними технологіями в умовах обмеженого часу та збільшенні кількості та складності кіберзагроз.

Для розв’язання вказаного протиріччя в дисертаційній роботі сформульовано актуальну науково-прикладну проблему щодо розробки методології підвищення ефективності захисту інформаційних ресурсів у кіберфізичних системах.

Зв’язок роботи з науковими програмами, планами, темами. Тематика дисертаційної роботи й отримані результати безпосередньо відповідають

пріоритетності розвитку інформаційних та комунікаційних технологій в Україні. Згідно із Законом України «Про пріоритетні напрями розвитку науки і техніки» № 2623–III від 11.07.2001; зі змінами, внесеними згідно із Законом України «Про інформацію» №2658–XII від 02.10.1992; Законом України «Про доступ до публічної інформації» № 2939–VI від 13.01.2011; Законом України «Про захист даних» № 4452–VI від 23.02.2012.

Дисертаційна робота виконана відповідно до планів наукової і науково-дослідної діяльності Державного університету інформаційно-комунікаційних технологій. Ця робота є частиною досліджень в рамках у госпрозрахункової науково-дослідної роботи «Моделі і методи захисту інформації в кіберфізичних системах» (Державний реєстраційний номер 0121U114233, ХНЕУ, м. Харків), яку виконував Харківський національний економічний університет імені Семена Кузнеця у 2020 р., частиною досліджень науково-дослідницької роботи «Геоінформаційні і інтелектуальні технології підтримки прийняття рішень в задачах оцінки та прогнозування екологічної безпеки територій» (Державний реєстраційний номер 0119U03671, ОДЕКУ м. Одеса), яку виконував Одеський Державний екологічний університет у 2023-2024 рр., частиною досліджень науково-дослідницької роботи «Розробка симетричної криптосистеми на основі використання згорткової штучної нейронної мережі» (Державний реєстраційний номер 0123U101020, НТУ «ХПІ», м. Харків), яку виконує Національний технічний університет "Харківський політехнічний інститут" 2023-2025рр., частиною досліджень науково-дослідницької роботи «Розробка моделей соціо-кіберфізичних систем, спрямованих на побудову систем безпеки та підвищення рівня її ефективності у кібер-просторі» (Державний реєстраційний номер 0123U101018, НТУ «ХПІ», м. Харків), яку виконує Національний технічний університет «Харківський політехнічний інститут» 2023-2025рр.

Мета і завдання дослідження. Мета дисертаційної роботи полягає у підвищенні ефективності захищеності інформації на основі запропонованих моделей і методів захисту в кіберфізичних системах шляхом побудови багатоконтурних систем захисту інформації з використанням постквантових алгоритмів.

Відповідно до поставленої мети для вирішення науково-прикладної проблеми в роботі сформульовано такі завдання:

1. Проаналізувати сучасні моделі, методи забезпечення захисту кіберфізичних систем з метою визначення набору критеріїв та ідентифікуючих і оціночних компонентів, які використовуються для створення та вибору найбільш ефективного інструментарію, орієнтованого на вирішення відповідних завдань захисту інформації.

2. Розробити концепцію побудови багатоконтурної системи захисту кіберфізичних систем.

3. Розробити моделі систем захисту на основі моделі Лотки-Вольтери з урахуванням класифікатора загроз на кіберфізичні системи.

4. Розробити методи забезпечення конфіденційності, цілісності й автентичності інформаційних ресурсів програмно-апаратного комплексу при одночасній дії на них загроз інформаційної безпеки, кібербезпеки та безпеки інформації.

5. Розробити метод забезпечення закриття каналу мобільного «Інтернету» та каналу циркуляцію інформації в кіберфізичних системах із забезпеченням необхідного рівня захищеності, серверного програмно-апаратного комплексу.

6. Удосконалити класифікатор загроз безпеці інформаційних ресурсів кіберфізичних систем.

7. Розробити методологію побудови багатоконтурної системи безпеки інформаційних ресурсів у кіберфізичних системах, яка забезпечує контроль поточного стану об’єкту захисту та необхідний рівень захищеності в умовах появи повномасштабного квантового комп’ютера.

Об’єктом дослідження є процес забезпечення захисту інформації в кіберфізичних системах на основі багатоконтурної системи безпеки з використанням постквантових алгоритмів.

Предметом дослідження є моделі і методи захисту інформації в кіберфізичних системах.

Методи дослідження. Проведені дослідження ґрунтуються на теоретично обґрунтованих і практично апробованих методах теорії множин (формалізовано загрози безпеки інформаційних ресурсів, здійснено їх класифікацію, визначено вимоги та повноту забезпечення безпеки інформаційних ресурсів), теорії криптографії, теорії кодування й теорії скінченних полів Галуа (використано при розробці гібридних крипто-кодових конструкцій на збиткових, кодах LDPC (Low Density Parity Check) та обґрунтуванні їх стійкості), теорії ймовірностей і математичної статистики (використано для дослідження властивостей гібридних крипто-кодових конструкцій на збиткових, LDPC-кодах), експертного оцінювання (для визначення вагових коефіцієнтів загроз для формування класифікатора загроз), математичної логіки і теорії автоматів (для оцінювання енергетичних затрат при практичній реалізації гібридних крипто-кодових конструкцій (ККК) на збиткових, LDPC-кодах, побудові серверної частини програмно-апаратного комплексу), системного аналізу (для ієрархічного подання кіберфізичних систем), законах синергії (для побудови моделі загроз, дослідження її впливу на систему безпеки інформаційних ресурсів).

Наукова новизна одержаних результатів полягає у такому:

1. Вперше розроблено концепцію побудови багатоконтурної системи захисту кіберфізичних систем, яка за рахунок інтеграції: методу забезпечення конфіденційності, цілісності й автентичності інформаційних ресурсів

програмно-апаратного комплексу; методу забезпечення закриття каналу мобільного «Інтернету» і каналу циркуляції інформації та математичної моделі з урахуванням класифікатора загроз дає можливість створити ефективні системи захисту інформації в кіберфізичних системах і відкрити новий напрямок у побудові системи захисту інформаційних ресурсів внутрішнього й зовнішнього контуру безпеки фізичної платформи та платформи управління кіберфізичних систем.

2. Вперше розроблено математичну модель безпеки кіберфізичних систем, яка на підставі розробленої концепції за рахунок врахування вагового коефіцієнту, що відображає можливості порушника, час та ймовірності реалізації загрози, дозволяє своєчасно визначити спрямованість загроз, врахувати обчислювальні ресурси нападників.

3. Вперше розроблено метод забезпечення конфіденційності, цілісності й автентичності інформаційних ресурсів кіберфізичних систем, у якому за рахунок використання гібридних крипто-кодових конструкцій зі збитковими кодами на основі модифікованої крипто-кодової конструкції Нідеррайтера на LDPC-кодах, що дозволяє зменшити складність формування (лінійного перетворення) та розкодування у криптограмі, забезпечити достовірність OTP-паролів в протоколі автентифікації в умовах дії гібридних загроз.

4. Набув подальшого розвитку метод забезпечення закриття голосового каналу мобільного Інтернету, в якому за рахунок використання алгоритмів постквантової криптографії у крипто-кодових конструкціях Нідеррайтера на еліптичних кодах підвищується стійкість протоколів послуг безпеки у структурі технологій LTE та забезпечується високий рівень захищеності голосового каналу мобільного зв’язку.

5. Удосконалено класифікатор загроз безпеці інформаційних ресурсів кіберфізичних систем, який за рахунок врахування рівня критичності загроз, відношення загрози до складової безпеки, послуги безпеки, впливу загрози відповідно до регуляторів та оцінки фінансових можливостей порушника дозволяє оцінювати гібридність загроз і відкриває новий підхід побудови діючих та перспективних систем захисту інформаційних ресурсів кіберфізичних систем.

6. Вперше розроблено методологію побудови системи безпеки інформаційних ресурсів кіберфізичних систем, яка за рахунок використання концепції побудови багатоконтурної системи безпеки, методу забезпечення конфіденційності, цілісності й автентичності інформаційних ресурсів, методу забезпечення закриття каналу мобільного Інтернету і каналу циркуляції інформації та математичної моделі з урахуванням класифікатора загроз дозволяє відкрити новий емерджентний підхід побудови наявних і перспективних систем безпеки, що підвищують ефективність захисту інформаційних ресурсів кіберфізичних систем на 5%.

Наукова цінність основних положень дисертації полягає в розробці концепції, моделей і методів безпеки кіберфізичних систем та методології створення системи безпеки кіберфізичних систем, в основу яких покладено концепцію побудови багатоконтурної системи безпеки, та які базуються на гібридних крипто-кодових конструкціях зі збитковими кодами на основі модифікованої крипто-кодової конструкції Нідеррайтера на LDPC-кодах.

Практичне значення отриманих результатів.

Практична цінність роботи полягає в тому, що:

1. Запропоновано методику застосування класифікатора загроз безпеки інформаційних ресурсів (електронний доступ: http://skl.khpi.edu.ua), яка дозволяє в режимі онлайн здійснювати об'єктивну оцінку загроз, визначення критичних точок інфраструктури кіберфізичних систем, можливості превентивних заходів і формувати оцінку потокового стану захищеності.

2. Запропоновано програмно-апаратний комплекс на основі мікроконтролерів, якій забезпечує автономне управління елементами кіберфізичної системи, закриття каналів зв'язку (як дротових, так й бездротових на основі крипто-кодових конструкціях Нідеррайтера на LDPC-кодах).

3. Розроблений практичний протокол LoRa, якій забезпечує циркуляцію інформації в кіберфізичних системах із забезпеченням необхідного рівня захищеності, серверного програмно-апаратного комплексу та дозволяє аналізувати ефективність функціонування системи захисту кіберфізичних систем.

4. Впровадження розроблених методів забезпечення конфіденційності, цілісності й автентичності інформаційних ресурсів кіберфізичних систем на гібридних крипто-кодових конструкціях Нідеррайтера забезпечує зменшення складності формування (лінійного перетворення) та розкодування в криптограмі.

Впровадження розроблених методів забезпечення конфіденційності, цілісності й автентичності інформаційних ресурсів на гібридних крипто-кодових конструкціях забезпечує зменшення в 2 – 3 рази енергетичних витрат при використанні у складі кіберфізичних систем відкритих каналів зв'язку й передачі даних при одночасному забезпеченні заданих показників безпеки.

Результати досліджень прийняті до впровадження в Державному підприємстві «Науково-технічний комплекс «Імпульс»(акт від 07.12.2021р.), в ТОВ «Мікрокрипт Текнолоджіс» (акт від 07.12.2023р.), в ТОВ «Сайфер ІТ» (акт від 10.01.24р.), в навчальному процесі кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут» при викладанні дисципліни «Основи побудови та захисту мікропроцесорних систем», «Інтернет речей та сервісів» для студентів спеціальності 125 «Кібербезпека» денної форми навчання (акт від 15.10.2024 р.).

Особистий внесок здобувача. Всі положення, які виносяться на захист, належать особисто автору. В роботах, які опубліковано у співавторстві, особисто здобувачу належать: в [1] запропонованій концепції багатоконтурних систем безпеки з урахуванням гібридності та синергії сучасних цільових кібератак; в [2] розглянуто практичні аспекти методології побудови постквантових алгоритмів для асиметричних криптосистем МакЕліса та Нідеррайтера на алгебраїчних кодах (еліптичні та модифіковані еліптичні коди), їх математичні моделі та практичні алгоритми; в [3,7] визначено показники, за якими проводиться аналіз текстових повідомлень, і критерії, за якими приймається рішення щодо наявності ознак; в [4,18] визначено чисті й змішані стратегії для різних початкових умов, що дозволяє виключити з розгляду стратегії, які не входять в рішення, та сформовано синергетичний підхід до класифікації і формальному опису процедур, реалізованих в системі безпеки, що дозволяє формалізувати підхід до аналізу та подальшого синтезу необхідного процедурного базису при проектуванні і реінжинірингу систем безпеки, що збільшується ефективність управління механізмами захисту контуру процесів обміну даними; в [5,12,13,24] розроблена класифікація сучасних загроз, які комплексуються з методами соціальної інженерії і набувають ознак синергії і гібридності та запропоновано синергетичну модель загроз на CPS, яка враховує спрямованість загроз на синергію і гібридність, і комплексований вплив складових безпеки; в [6,20,21,23] розроблена модель постквантових алгоритмів крипто-кодових конструкції Нідеррайтера на кодах LDPC із малою щільністю перевірок на парність, запропонована концепція побудови безпеки на основі двох контурів, для забезпечення безпеки бездротових мобільних каналів запропоновано математична модель крипто-кодової конструкції Нідеррайтера на LDPC–кодах, гібридної ККК на ущербних кодах, що дозволяє забезпечити необхідний рівень криптостійкості в кіберфізичних системах без зниження показників пропускної спроможності; в [8,16,17,22] розроблено метод оцінки безпеки кіберфізичних систем, що ґрунтується на базі запропонованого класифікатора загроз із урахуванням їхньої гібридності та синергізм, що враховує фізичну складову кіберфізичних систем і вимагає створення багатоконтурних систем захисту інформації, а також формування об’єктивності при оцінці загроз як на внутрішній (фізичний рівень) контур системи захисту інформації, так і на зовнішній контур (рівень управління), на основі моделі Лотки-Вольтери, запропоновано моделі безпеки кіберфізичних систем: “хижак-жертва” з урахуванням обчислювальних можливостей і спрямованості цільових кібератак, “хижак-жертва” з урахуванням можливої конкуренції зловмисників по відношенню до “жертви”, “хижак-жертва” з урахуванням взаємозв’язків між “видами жертв” і “видами хижаків”, “хижак-жертва” з урахуванням взаємозв’язків між “видами жертв” і “видами хижаків”; в [9,10] обґрунтовано необхідність дослідження впливу

трансформації частотної функції розузгодження когерентної пачки радіоімпульсів на якість вирішення завдання радіолокаційного розділення за частотою та реалізації в криптосистемах гібридного формувача випадкових чисел із двома типами джерел ентропії; в [11,14,15] розроблена модель структури інтегральної інформаційної мережі на основі нестаціонарної ієрархічної та стаціонарної гіпермережі, з врахуванням руйнівних впливів різного характеру у рамкам розробленої концепції перевершують наявні методи та методики, які використовуються в сучасних автоматизованих комплексах пошуку цифрових засобів негласного отримання інформації по виявленню, розпізнаванню та локалізації сигналів цифрових засобів негласного отримання інформації; в [19] запропонована структурна схема забезпечення послуг безпеки на основі ККК, що суттєво зменшує можливість створення "хаосу" при появі повномасштабного квантового комп'ютеру та можливості зламу CCIS/ CPSS (SCADA) на основі постквантових алгоритмів Гровера й Шора; в [25] проведено математичне моделювання удосконаленої моделі захисту інформації в мережі залежно від специфічних її параметрів; в [27] розроблено пристрій на основі мікро-контролеру СКЗІ(ESP-WROOM-32) із вбудованими алгоритмами крипто-кодових конструкцій Нідеррайтера на модифікованих LDPC кодах в алгоритмі шифрування технології LoRaWAN для забезпечення безпеки зовнішнього контура, використано розроблений сервер, який фізично розміщується в місці, де буде знаходитися шлюз із виходом до зовнішнього каналу зв'язку мережі інтернет.

Апробація результатів дисертації. Основні результати дисертаційних досліджень доповідалися й обговорювалися на конференціях і семінарах, а саме:

International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2022, (Scopus), форма участі – заочна.

2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2022, (Scopus), форма участі – заочна.

2021 CEUR Workshop Proceedings 3200, (Scopus), форма участі –заочна.

2022 IEEE 4th International Conference on Modern Electrical and Energy System (MEES), Kremenchuk, Ukraine, 2022, (Scopus), форма участі –заочна.

2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 2022, (Scopus), форма участі –очна.

Modern directions of scientific research development. Proceedings of the 6th International scientific and practical conference. BoScience Publisher. Chicago, USA, форма участі –заочна.

Proceedings of the 5rd International scientific and practical conference. SPC «Sci-conf.com.ua». Kharkiv, Ukraine, форма участі –заочна.

The 4th International scientific and practical conference “Innovations and prospects of world science” (December 1-3, 2021) Perfect Publishing, Vancouver, Canada, форма участі –заочна.

Регіон. круг. стіл «Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони». Харків, 2020, форма участі –заочна.

Cybersecurity issues in the internet of things. 1st International Conference: Modern Information, Measurement and Control Systems: Problems and Perspectives (MIMCS’2019), форма участі –заочна.

Міжнародна науково-практична конференція «Економічний розвиток і спадщина Семена Кузнеця»: тези доповідей, 30 – 31 травня 2019 р. – Х.: ХНЕУ імені Семена Кузнеця, форма участі –очна.

«Modern Information, Measurement and Control Systems: Problems, Applications and Perspectives 2022 (MIMCS’2022)» , форма участі –заочна.

Публікації. За результатами дисертаційних досліджень опубліковано 44 наукові праці, із них 27 наукових статей у фахових виданнях. Одна монографія та вісім статей опубліковані в науковому виданні, що входить до науково-метричної бази Scopus. Також 17 праць опубліковано в матеріалах наукових конференцій, з них вісім, що входять до науково-метричної бази Scopus.

Структура та обсяг дисертації. Структура та обсяг дисертації. Дисертація складається зі вступу, 5 розділів, висновків, списку використаних джерел з 255 найменувань на 29 сторінках. Повний обсяг дисертації 330 сторінок, з них 261 сторінок основного тексту.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЇ

У вступі обґрунтовано актуальність теми дисертації, сформульовано науково–прикладну проблему, мету, об’єкт, предмет, завдання дослідження, наукову новизну одержаних результатів, практичне значення результатів, зв'язок роботи з науковими програмами, планами, темами досліджень Національного технічного університету «Харківський політехнічний інститут» та Державного університету інформаційно-комунікаційних технологій. Визначено особистий внесок здобувача, відомості про апробацію результатів роботи, публікації.

У першому розділі дисертації здійснено аналіз наявних методів захисту інформації. Проведено аналіз вітчизняної та зарубіжної наукової літератури за темою дисертаційної роботи. Розглянуто наявні загрози інформаційних ресурсів у кіберфізичних системах. Проаналізовано сучасний стан проблеми захисту інформаційних ресурсів у кіберфізичних системах. Здійснено постановку проблеми дослідження.

Доведено, що розвиток мережевих технологій та квантових обчислень забезпечує високу швидкість передачі даних і низькі затримки, що є критичним

для ефективної роботи CPS. Це спонукає дослідити CPS як платформу розподілених систем, де різні компоненти можуть ефективно взаємодіяти між собою, незалежно від їхнього фізичного розташування.

Розроблена та наведена візуалізована схема кіберфізичних систем (рис. 1).

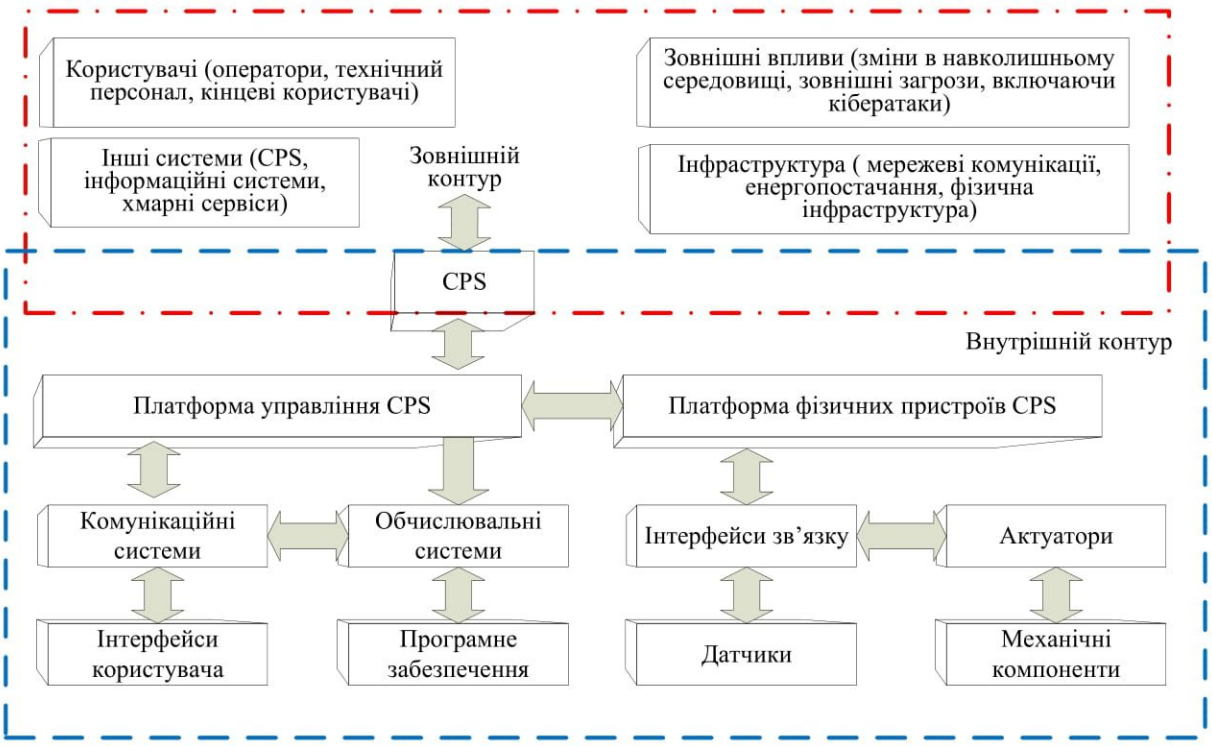


Рис. 1. Схема інтеграції та взаємодії компонентів кіберфізичної системи.

Здійснюється аналіз різних типів наявних моделей впливів й атак на систему захисту інформації.

Для математичного опису загальної моделі кіберфізичної системи (CPS) з урахуванням платформ і контурів використовується система рівнянь та функцій, які пояснюють взаємодію між компонентами.

Математична модель функції визначає взаємодію між компонентами платформи управління і фізичної платформи та характеризується рівнянням:

$$fu(C,S,N,Iu,D,A,M,Ic) \quad (1)$$

де, *Платформа управління*:

$C(t)$ – обчислювальні ресурси в момент часу t;

$S(t)$ – програмне забезпечення в момент часу t;

$N(t)$ – комунікаційні системи в момент часу t;

$I_u(t)$ – інтерфейси користувача в момент часу t;

Платформа фізичних пристроїв:

$D(t)$ – дані від датчиків у момент часу t;

A(t) –актуатори в момент часу t;

M(t) – механічні компоненти в момент часу t;

$I_c(t)$ – інтерфейси зв'язку в момент часу t.

Математична модель внутрішньої взаємодії (*Внутрішній контур*) між компонентами платформи управління та платформи фізичних пристроїв описується рівнянням:

$$fu(C,S,N,I_u,D,A,M,I_c)=0, \quad (2)$$

Це рівняння відображає баланс між даними, що надходять із датчиків, обробкою цих даних обчислювальними ресурсами та програмним забезпеченням, і діями, що виконуються актуаторами.

Взаємодія із зовнішнім середовищем (*Зовнішній контур*) описується набором рівнянь (3,4):

$$\begin{aligned} & U(t)=g_u(I_u(t))U(t) \\ O(t)= \; & g_o(N(t),I(t))O(t) \\ & I(t)=g_i(I_c(t),E(t))I(t) \end{aligned} \quad (3)$$

де, U(t) – взаємодія з користувачами;

O(t) – взаємодія з іншими системами;

I(t) – взаємодія з інфраструктурою;

E(t) – зовнішні впливи (зміни в навколишньому середовищі, кібератаки).

Загальне рівняння можна записати так:

$$\frac{dX(t)}{dt} = F(\mathrm{X}(t), \mathrm{U}'(t), \mathrm{E}'(t)) \quad (4)$$

де,

X(t) – вектором стану, що включає всі основні компоненти внутрішнього контуру;

U'(t) – вектор вхідних впливів від користувачів, інших систем та інфраструктури:

$$\mathrm{U}'(t) = \begin{bmatrix} U(t) \\ O(t) \\ I(t) \end{bmatrix}$$

E'(t) – вектор зовнішніх впливів, включаючи зміни в навколишньому середовищі та кібератаки: E'(t)=E(t).

Ця система рівнянь формує комплексний підхід до моделювання CPS, враховуючи як внутрішні взаємодії між компонентами, так і зовнішні впливи.

Дослідження методів захисту мережі. Перший напрямок дозволяє зробити висновок, що базовий захист мережі можливо розділити на наступні етапи:

– елементарний і обов'язковий етап, де головним інструментом захисту виступає firewall, який повинен лімітувати використання сервісів, наданим користувачам, а також повинен стежити за всіма з'єднаннями, як з одного, так і з іншого боку;

– наступний етап орієнтований вже на захист мережі, де необхідним є оснащення датчиками атаки мережевого обладнання та програмного забезпечення провайдера, що забезпечує хостинг і забезпечення вірного оброблення надходження сигналу про небезпеку та її нейтралізації;

– установка програмного забезпечення на рівні хостингу – останній етап, де рівень безпеки повинен бути вищим, тому що можливі заперечення самої хостинг-компанії та складність самого програмного забезпечення.

Можливі окремі рівні безпеки додатків із файлом конфігурації доступу ресурсів, які захищаються, захисту веб-сторінки від аналізу вихідного коду тощо.

Наприклад, двофакторна автентифікація – це спосіб ідентифікації користувача на онлайновому сервісі шляхом використання комбінації двох різних методів автентифікації. Методи можуть бути засновані на тому, що користувач знає (наприклад, пароль або PIN-код) і чим користувач володіє (наприклад, апаратний токен або мобільний телефон), або що є його невід'ємною частиною (наприклад, відбитки пальців).

Як показав аналіз, шлях рішення проблеми захисту першого напрямку загроз – це визначення нападу або втручання з метою пошкодження (заміни) інформації від користувача до сервера, зберігання та обробки інформації. Для цього можливо використовувати моделі та методи визначення нападу на систему або моделі виявлення вразливостей системи передачі інформації. Але на сьогодні нема однозначного методу гарантованого виявлення атаки або виявлення вразливостей. Це обумовлено тим, що варіанти атаки на мережу ускладняються та постійно удосконалюються. Іншим варіантом захисту від загроз першого напрямку є метод створення захищених каналів передачі інформації, але цей метод також має недолік. Він потребує додаткових зусиль по налагоджуванню захищеного каналу передачі даних і додаткових обчислюваних ресурсів системи.

Шлях рішення проблеми захисту другого напрямку загроз – це втручання з метою порушення цілісності інформації від користувача до сервера зберігання та обробки інформації. Рішення цього напрямку може бути досягнуто за рахунок надійної та вірної конфігурації операційної системи, під чиїм керівництвом працює веб-сервер. Кожна операційна система дозволяє створювати контрольні листи безпеки (security checklist). Ці установки повинні бути узгоджені з операційними системами вендорів, які співпрацюють з компанією. Установка спеціального програмного забезпечення виконує роль прошарку між операційною системою веб-сервера та всіма додатками. Такий

буфер дозволяє запобігти атаці хакерів на вразливі додатки, які беруть під контроль всю операційну систему під час свого виконання. Це не найдешевший варіант, тому що, як і на попередньому рівні, необхідно забезпечити підтримку програмного забезпечення, яким оперують веб-сервери. Наступний шлях може бути пов'язано з установкою, орієнтованих на конкретні програми firewall або проксі-серверів. Вони орієнтовані на HTTP-протокол і дозволяють запобігти атакам перш, ніж потенційні зловмисники зможуть дістатися до запуску додатків, встановлених на веб-сервері. Однак проксі-сервер – це істотне обмеження в роботі. Конфігурація та налаштування проксі – теж свого роду мистецтво.

Використання операційних систем, які забезпечують управління додатками, та виконують всі програми захисту.

Останнім невирішеним питанням у процесі захисту CPS є процес захисту мережи передачі інформації від центрів (серверів) управління до виконавчих пристроїв. Це питання остаточно не вирішено тому, що найчастіше цей процес розглядється як процес, аналогічний першому шляху, тобто захисту мережі. Атака з метою зміни команди управління, або переадресація команди управління на другий виконавчий пристрій, не розглядається. У CPS за головне приймають збір даних із пристроїв, а не керування виконавчими пристроями. Розглядають тільки інформаційний канал, а не канал управління пристроями. Тому цьому напрямку найчастіше не приділяють достатньої уваги.

Проведені дослідження показали відсутність цілісної концепції захисту інформації в CPS: методики та моделі захисту не складають єдину методологію комплексного забезпечення захисту інформації, яка б поєднувала теоретичні методи, методики, моделі та технологічні підходи до захисту інформації в CPS.

Виходячи з проведеного аналізу, виникає науково-прикладна проблема щодо розробки методології підвищення рівня захищеності інформаційних ресурсів у кіберфізичних системах. Тому потрібно розробити методологію захисту інформації в кіберфізичних системах.

Таким чином, при розробці нових або модернізації наявних методів і методик захисту інформації потрібно застосовувати комплексний підхід до розробки алгоритму захисту інформації.

Проведені дослідження ґрунтуються на теоретично обґрунтованих і практично апробованих методах теорії множин (формалізовано загрози безпеки інформаційних ресурсів, здійснено їх класифікацію, визначено вимоги й повноту забезпечення безпеки інформаційних ресурсів), теорії криптографії, теорії кодування та теорії скінченних полів Галуа (використано при розробці гібридних крипто-кодових конструкцій на збиткових, LDPC-кодах та обґрунтуванні їх стійкості), теорії ймовірностей і математичної статистики (використано для дослідження властивостей гібридних крипто-кодових

конструкцій на збиткових, LDPC-кодах), експертного оцінювання (для визначення вагових коефіцієнтів загроз для формування класифікатора загроз), математичної логіки й теорії автоматів (для оцінювання енергетичних затрат при практичній реалізації гібридних крипто-кодових конструкцій на збиткових, LDPC-кодах, побудові серверної частини програмно-апаратного комплексу), системного аналізу (для ієрархічного подання кіберфізичних систем), законах синергії (для побудови моделі загроз, дослідження її впливу на систему безпеки інформаційних ресурсів).

Отже, після рішення завдань розробки й удосконалення моделей та методик захисту інформації буде розроблено методологічні основи захисту захисту інформації в кіберфізичних системах.

Другий розділ присвячений розробці моделей захисту інформації в кіберфізичних системах на основі моделі Лотки-Вольтерри.

Оцінка рівня загроз неможлива без оцінки можливостей самих нападників (зловмисників, кіберзлочинців тощо). Від їхньої "компетентності", обчислювальних ресурсів, часових характеристик, їхньої вмотивованості багато в чому залежить можливість реалізації загрози. Таким чином, невід'ємною частиною аналізу загроз є розробка моделі "небезпеки" порушника. Такий підхід дає змогу сформувати безліч загроз залежно від можливостей нападників, сформувати безліч можливих впливів, оцінити стан превентивних засобів захисту. Для формування вагових коефіцієнтів "небезпеки" порушників пропонується використовувати таку класифікацію порушників (рис. 2).

Класифікація дає змогу ввести елементи безлічі категорій зловмисників: користувачі ICS (CPS); керівництво ICS (CPS), службовець ICS (CPS).

Користувачі «в зоні ризику»; експлуатаційний персонал; технічний допоміжний персонал; особи, які не є співробітниками ICS (CPS).

Зовнішні зловмисники: кібертерористи, спецслужби, хакери, кіберзлочинці, конкуренти, кримінал, вандали.

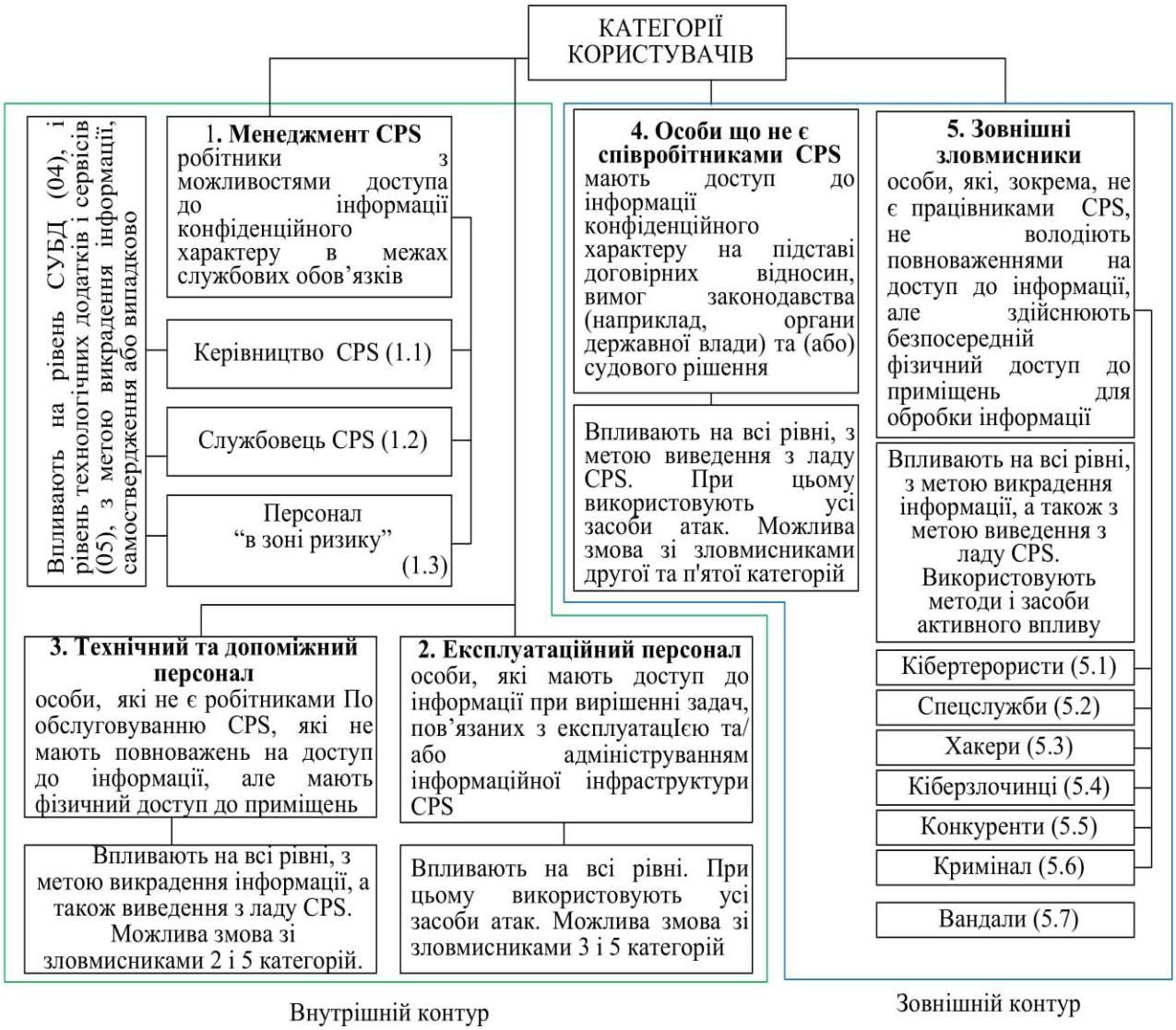


Рис. 2. Класифікація зловмисників

Модель "небезпеки" порушника визначимо з урахуванням наступних складових:

$$G_{CPS}^{ICS} = \left\{ aid_i, \beta_i^{ICS} \in \left\{ \beta_i^{ICS} \right\}, \beta_i^{CPS} \in \left\{ \beta_i^{CPS} \right\}, p_{rj}, r_{\text{motiv}}, T \right\}, \quad (5)$$

де: $aid_i \in \{aid\}$ – ідентифікатор порушника (категорія порушника);

$\beta_i^{ICS} \in \left\{ \beta_i^{ICS} \right\}$ – ваговий коефіцієнт можливостей порушника для ICS;

$\beta_i^{CPS} \in \left\{ \beta_i^{CPS} \right\}$ – ваговий коефіцієнт можливостей порушника CPS;

T – час успішної реалізації загрози;

p_{rj} – ймовірність реалізації хоча б однієї загрози j-му активу;

i – загроза, $\forall i \in n$,

n – кількість загроз;

j – інформаційний ресурс (актив), $\forall j \in m$,

m – кількість активів;

r_{motiv} – ймовірність мотивації зловмисника до реалізації загрози.

Аналіз класифікації зловмисників дає змогу сформувати експертну оцінку й отримати ваговий коефіцієнт можливості реалізації загроз (i-ї загрози).

Ваговий коефіцієнт "небезпеки" зловмисника визначимо за формулою:

$$\gamma_{ICS}^{CPS} = \frac{1}{N}\sum_{i=1}^{N}\gamma_{ICS\,i}^{CPS}, \tag{6}$$

причому:

$$\gamma_{ICS\,i}^{CPS} = \left(\beta_i^{ICS} \cup \beta_i^{CPS}\right) \times p_{rj} \times r_{motiv}, \tag{7}$$

де: $\beta_i^{ICS} = W_{cp}^{ICS} \cap W_{cash}^{ICS} \cap T^{ICS}$, $\beta_i^{CPS} = W_{cp}^{CPS} \cap W_{cash}^{CPS} \cap T^{CPS}$ – вагові коефіцієнти можливостей порушника для ICS та CPS (відповідно);

$W_{cp}^{ICS}\left(W_{cp}^{CPS}\right)$ – обчислювальні ресурси порушника (1 – необмежені ресурси кібертерористів, 0,75 – ресурси держави (спецслужб), 0,5 – ресурси кіберзлочинців, 0,25 – ресурси криміналу, конкурентів, хакерів, 0,001 – ресурси вандалів);

$T^{ICS}(T^{CPS})$ – час для виконання загрози (1 – загроза реалізується щодня, 0,75 – загроза реалізується протягом тижня, 0,5 – загроза реалізується протягом місяця, 0,25 – загроза реалізується протягом року, 0,001 – необмежений час);

$W_{cash}^{ICS}\left(W_{cash}^{CPS}\right)$ – економічні можливості нападників (1 – необмежені ресурси кібертерористів, 0,75 – ресурси держави (спецслужб), 0,5 – ресурси кіберзлочинців, 0,25 – ресурси криміналу, конкурентів, хакерів, 0,001 – ресурси вандалів).

Введення вартісних показників загроз дає змогу реалізувати алгоритм побудови рейтингу потенційних загроз і важливості інформаційних ресурсів, що підлягають захисту.

Під час реалізації алгоритму допускається, що сторони конфлікту визначають критичність кіберзагроз, які економічно доцільно проводити та/або від яких необхідно захистити IoT насамперед. Тоді алгоритм визначимо:

1-й крок. Визначення кіберзагроз, ефект від реалізації яких перевищує витрати на їх проведення:

$$Tr_R^A = \left\{Tr_i \mid \left(P_i^A - C_i^A\right) > 0\right\} \forall Tr_i \in Tr, \tag{8}$$

де: Tr_R^A – безліч потенційних загроз, реалізація яких ефективна для атакуючого;

Tr_i – загроза i-му інформаційному ресурсу;

P_i^A – оцінка вартості успішності реалізації атаки на *i*-й ресурс з боку атакуючого;

C_i^A – вартість проведення атаки на *i*-й ресурс з боку атакуючого.

2-й крок. Визначення напряму захисту, який забезпечує ефект вищий, ніж витрати на їх забезпечення:

$$Tr_C^D = \left\{ Tr_j \mid \left(P_i^D - C_i^D \right) > 0 \right\} \forall Tr_j \in Tr, \tag{9}$$

де: Tr_C^D – безліч загроз, проти яких економічно доцільно вибудовувати захист;

P_i^D – оцінка вартості втрати і-го інформаційного ресурсу для сторони захисту;

C_i^D – вартість захисту *i*-го інформаційного ресурсу для сторони захисту;

3-й крок. Визначення коефіцієнтів важливості для атакуючих. Визначаються як частки виграшу від загальної суми виграшу, що може бути отримана потенційно в разі реалізації всього комплексу загроз для нападників:

$$K_i^A = \frac{P_i^A - C_i^A}{\sum_{i=1}^{M} \left(P_i^A - C_i^A \right)}, \ \forall Tr_i \in Tr_R^A, \ M = \left| Tr_R^A \right|, \tag{10}$$

де: K_i^A – рейтинговий коефіцієнт (важливості) реалізації загрози *i*-му інформаційному ресурсу;

M – потужність множини відібраних потенційно ефективних загроз для атакуючої сторони.

4-й крок. Визначення коефіцієнтів важливості для захисників. Визначаються як частка виграшу від загальної суми виграшу, яка може бути отримана потенційно при реалізації всього комплексу захисних заходів:

$$K_j^D = \frac{P_i^D - C_i^D}{\sum_{i=1}^{N} \left(P_i^D - C_i^D \right)}, \ \forall Tr_j \in Tr_C^D, \ N = \left| Tr_C^D \right|, \tag{11}$$

де: K_j^D – рейтинговий коефіцієнт (важливості) вибудовування захисту *j*-го інформаційного ресурсу.

5-й крок. Добір критичних загроз, для яких на основі оцінки добуток коефіцієнтів важливості атакуючого і того, хто захищається, виявляється максимальним:

$$Tr_l = \arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A. \tag{12}$$

Тоді коефіцієнт народжуваності "жертв" пропонується розраховувати, як:

$$\alpha = \frac{\left| \{ Tr_l \} \right|}{Q}, \tag{13}$$

де: $\left|\{Tr_l\}\right|$ – безліч критичних кіберзагроз, для яких у системі захисту інформації (СЗІ) немає засобів захисту або вони частково є, але реалізація загрози може призвести до істотного та/або критичного руйнування контуру безпеки;

Q – загальна кількість відомих кіберзагроз.

Отриманий коефіцієнт забезпечує розуміння керівництва необхідності встановлення додаткових засобів захисту проти виявлених критичних атак.

Таким чином, використовуючи отримані вирази, модель Лотки-Вольтерри можна представити в такому вигляді:

$$\begin{cases} \dfrac{dN_1}{dt} = \left(\arg \max\limits_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \left(\sum\limits_{i=1}^{Q} \begin{pmatrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix} \right) - \\ - \left(\sum\limits_{i=1}^{M} \begin{pmatrix} w_{CPSi}{}^C \bigcap w_{CPSi}{}^I \bigcap w_{CPSi}{}^A \bigcap \\ \bigcap w_{CPSi}{}^{Au} \bigcap w_{CPSi}{}^{Aff} \end{pmatrix} \chi_i^{CPS} \right) \times \tilde{N}_1 \left(N_2 \times \left| W_{\text{hybrid } C,I,A,Au,Af\ synerg} \right| \right); \\ \dfrac{dN_2}{dt} = -\left(\dfrac{1}{M} \sum\limits_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \tilde{N}_2 + \left(\dfrac{1}{KB} \sum\limits_{k=1}^{K} \sum\limits_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right) \right) \tilde{N}_2 \tilde{N}_1. \end{cases} \quad (14)$$

Отже, пропонований підхід моделі безпеки CPS дає змогу, з практичного погляду, розглядати кіберпростір як екосистему, враховувати обчислювальні можливості зловмисників і спрямованість цільових кібератак. Крім цього, кібератаки розглядаються з урахуванням їхнього комплексування з методами соціальної інженерії, що дає змогу формувати зловмисникам цільові атаки. Запропонована модель враховує можливість прояву цільових атак в екосистемі ознак синергізму та гібридності, яка суттєво впливає на кількісні показники оцінки поточного стану рівня захищеності.

Доведено, що однією з особливостей CPS є відсутність забезпечення захисту інформації в елементах інфраструктури, передача сигналів від датчиків/сенсорів відкритими каналами і забезпечення управління та адміністрування на основі хмарних технологій. Це істотно знижує можливості формування контуру безпеки та призводить до збільшення критичних точок для реалізації кібератак. За таких умов оцінювання безпеки необхідно проводити в офлайн-режимі, що дає змогу враховувати динаміку, як кіберзагроз, із одного боку, так і можливість засобів захисту протистояти їм.

На рис. 3 представлено структурну схему пропонованого методу оцінювання:

Рис. 3. Структурна схема методу оцінювання безпеки CPS на основі моделі Лотки-Вольтерри "хижак-жертва"

Запропонований метод базується на оцінці безпеки CPS із плином часу. Описовою характеристикою зміни поточного стану безпеки CPS є його *інтенсивність* $l(t)$ – середнє число змін, що відбулися з поточним станом безпеки CPS в одиницю часу. Для оцінки інтервалів часу $\Delta t_{[i-q]}$ між змінами рівня безпеки CPS використовуємо формулу:

$$\Delta t_{[i-q]}(t) = \frac{K}{l(t)}, \tag{15}$$

де: K – сумарна кількість змін рівня безпеки;

$l(t)$ – інтенсивність змін рівня безпеки;

$i, q \in [1; n]$ – порядкові номери змін;

$i \ge q$.

Зміни рівнів безпеки визначимо у вигляді кінцевого автомата H^{CPS}, стану якого описує формула:

$$H^{CFS} = \left\langle S^I, value, \Pi, S_0^I \right\rangle, \quad (16)$$

де: S^I – кінцевий стан рівня безпеки CPS;

value – значення змін рівня безпеки CPS;

П – функція переходів рівня безпеки CPS зі стану *k* в стан *j*;

S_0^I – початковий стан рівня безпеки CPS.

Функція переходів рівня безпеки CPS П зі стану *k* в стан *j* оцінимо за формулою:

$$\Pi = S_0^I \times value \to S^I . \quad (17)$$

Для визначення станів безпеки використовуємо одну із запропонованих моделей Лотки-Вольтерри з урахуванням можливостей як “жертви”, так і “хижаків”.

Аналіз результатів моделювання [154] дає змогу зробити доволі загальний висновок, що в умовах обмежених фінансових коштів, які спрямовуються на розробку та впровадження нових засобів, що забезпечують послуги безпеки, їхній розподіл, має здійснюватися таким чином. Визначається той із коефіцієнтів, зміна якого призводить до більш істотних змін з точки зору рівня безпеки. З'ясовується найбільш значущий фактор, який призводить до змін розглянутого коефіцієнта. Визначаються заходи, що призводять до подібних змін. У роботі наведено порівняльні результати аналізу практичного використання методу оцінювання стану безпеки CPS на основі моделі Лотки-Вольтерри:

Третій розділ присвячений розробки підходу до забезпечення захисту каналу зв’язку на основі постквантових алгоритмів

Створення сучасних синтезованих мереж ґрунтується на гібридизації технологій бездротових мобільних та CPS на основі IoT. Класичні комп'ютерні системи та технології інтегрують елементи IoT і формують принципово нові напрямки розвитку IT-індустрії, smart-технології, які поєднують усі досягнення мобільних, бездротових і CPS. Однак стрімке розширення mesh-, сенсорних мереж із використанням стандартів бездротових каналів: мобільних технологій LTE (Long-Term Evolution – довгострокова еволюція), IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE802.11, Bluetooth – не забезпечує конфіденційності та цілісності.

Доказова стійкість для забезпечення безпеки інформації в бездротових мережах на основі мобільних технологій.

Висновок 1. Обсяг секретного ключа (в бітах) у дослідженій крипто-кодової системи на основі ККК Нідеррайтера, побудованій на LDPC *(n, k, d)*

кодах над *GF(q),* визначається сумою елементів матриць *X, P, D* (у бітах) і задається виразом:

$$l_{K+} = 5 \times n^2 \times k^2. \tag{18}$$

Доведення. Дійсно, секретний ключ у ККК Нідеррайтера – достатньо визначити набір коефіцієнтів $a_1 \ldots a_6$, $\forall a_i \in GF(q)$ і елементи матриць маскування. Всього необхідно зберігати $l_{K+} = 5 \times n^2 \times k^2$ бітів секретної ключової інформації.

Вираз (11) дозволяє оцінити обсяг секретних ключових даних у ССС Niederreiter на LDPC.

Висновок 2. Обсяг інформаційної посилки складає $l_I=k$, та не повинен перевищувати за вагою Гемінга (кількість ненульових елементів) вектора e виправної здатності використовуваного LDPC-коду:

$$\forall i : 0 \le w(M_i) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor. \tag{19}$$

Доведення. Дійсно, розмірність інформаційної посилки визначається спроможністю виправлення завадостійкого коду – достатньо визначити за вагою Гемінга (кількість ненульових елементів) вектора e виправну здатність використовуваного LDPC-коду:

$$\forall i : 0 \le w(M_i) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor. \tag{20}$$

Висновок 3. Обсяг криптограми складає:

$$l_S = e \times H^T = S. \tag{21}$$

Доведення. Дійсно, розмірність інформаційної посилки визначається шляхом формування синдрому LDPC-коду, що подається в канал зв'язку.

Висновок 4. Відносна швідкість криптосистеми визначимо, як:

$$R = (t+1) / \left(2\sqrt{q} + q + 1\right). \tag{22}$$

Доведення. Дійсно, відносна швидкість формування кодового слову визначається співвідношенням інформаційної посилки k до n, де $n = 2\sqrt{q} + q + 1$,

тому при використанні ККК Нідеррайтера на LDPC-кодах необхідно визначити, що вона дорівнює $R = (t+1)/\left(2\sqrt{q}+q+1\right)$ та приблизно дорівнює 1.

Кількісною мірою ефективності нанесення збитку є ступінь руйнування значення, що дорівнює різниці ентропій збиткового тексту і вихідного тексту на різних відрізках довжини збиткового тексту [1]:

$$d = H(FTC) - \sum_{i=1}^{s} H(M_i)p_i, \tag{23}$$

$$\sum_{i=1}^{s} p_i = 1, s = \left[\frac{L_0 - L_{FTC}}{L_{FTC}}\right], \tag{24}$$

де: M_i – частина вихідного тексту, що відповідає i-му відрізку;

p_i – її ймовірність;

L_0 – довжина M_i дорівнює довжині L_{FTC} – збиткового тексту;

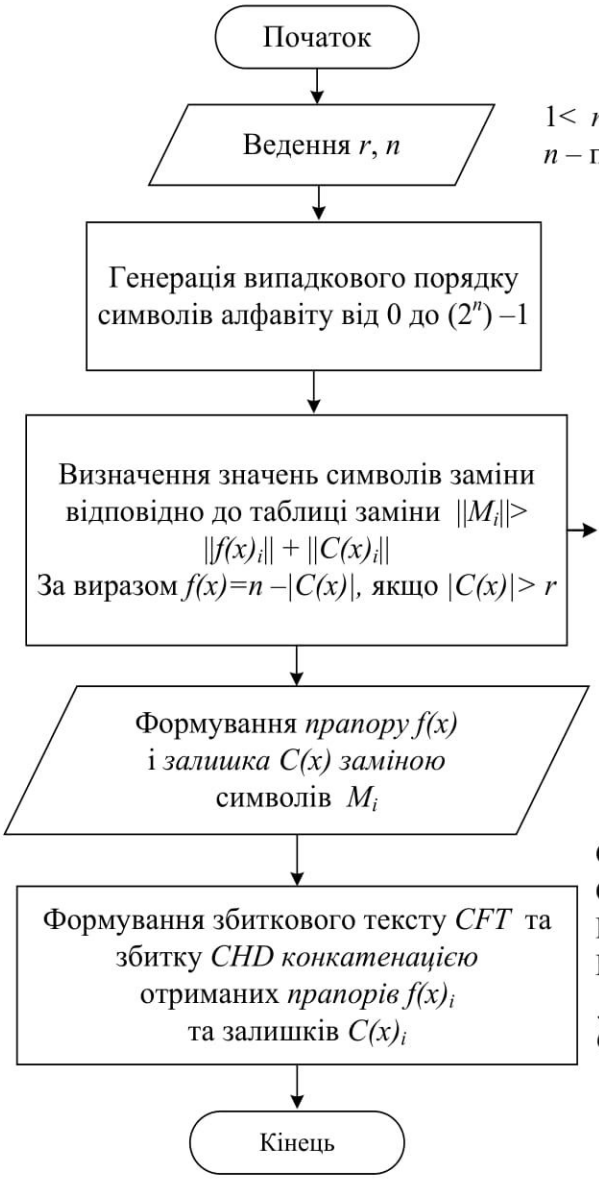
s – кількість відрізків.

Універсальний механізм нанесення збитку C_m може бути описаний як [1, 127]:

$$\begin{aligned} &CFT / CH_{FT} = E_1\left(M, KU^{LDPC}\right), \\ &CHD / CH_D = E_2\left(M, KU^{LDPC}\right), \\ &M = E_{1,2}^{-1}(CFT / CH_{FT}, CHD / CH_D, KU^{LDPC}), \\ &CFT / CH_{FT} = CFT / CH_{FT}^i, ..., CFT / CH_{FT}^m, \\ &KU^{LDPC} = \varphi(K_D^i, ..., K_D^m, KU_1^{LDPC}, ..., KU_m^{LDPC}, \\ &CHD / CH_D = CHD / CH_D^i, ..., CHD / CH_D^m \end{aligned} \tag{25}$$

Отже, у результаті маємо два шифртексти (збиток (CH_D) і збитковий текст (FTC)), кожен із яких не має сенсу ні в алфавіті початкового тексту, ні в алфавіті шифртексту. Фактично шифртекст вихідного повідомлення (M) подається у вигляді сукупності двох збиткових шифртекстів, кожен із яких окремо не може відновити вихідний текст. Для відновлення початкової послідовності немає необхідності знати проміжні збиткові послідовності. Необхідно знати тільки останню збиткову послідовність (останній збитковий текст після виконання всіх циклів) і всі збитки з правилами їх нанесення.

На рис. 4 наведений універсальний механізм нанесення збитку (алгоритм *MV*2 (формування збиткового тексту):



Символ	Довжина залишку	Залишок $C(x)$	Прапор $f(x)$
S_1	r	0^r	$0^{n-r-1}1$
S_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
$S_2{}^r{}_{+1}$	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$S_2{}^{n-1}{}_{-2^r}$	$n-2$	1^{n-2}	01
$S_2{}^{n-1}{}_{-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$S_2{}^n{}_{-2^r}$	$n-1$	1^{n-1}	1
$S_2{}^n{}_{-2^r+1}$	r	0^r	0^{n-r}
...	…	…	…
$S_2{}^n$	r	1^r	0^{n-r}

CFT/ CH_{FT} – шифротекст збиткового текста
CHD/CH_D – шифротекст збитку
FTC/ FT_{CH} – збитковий шифротекст
DCH/D_{CH} – збиток шифротексту
$f(x)$ – прапор (збиток)
$C(x)$ – залишок (збитковий код)

Рис. 4. Універсальний механізм нанесення збитку (алгоритм MV2 (формування збиткового тексту)

У таблиці 1 наведені результати досліджень залежності довжини вхідної послідовності на алгоритм *MV*2 від кількості тактів процесора на виконання елементарних операцій в програмній реалізації.

Таблиця 1

Результати досліджень залежності довжини вхідної послідовності на алгоритм *MV*2 від кількості тактів процесора

Довжина кодової послідовності		*MV*2		
		10	100	1000
Кількість викликів функцій, що реалізовують елементарні операції	сумування	3942	28673	275499
	різниця	1794	3810	23881
	ділення	3274	4804	20104
	множення	19	109	1009
	порівняння	8939	60963	578784

Сума		17968	98359	899277
Тривалість виконання функцій * в мілісекундах	сумування	19.53	93.58	2297.36
	різниця	8.89	12.43	199.14
	ділення	16.22	15.68	167.65
	множення	0.09	0.36	8.41
	порівняння	44.28	198.96	4826.43
Сума		89	321	7499
Тривалість виконання функцій * в мілісекундах		89	321	7499

*Примітки: * Тривалість 1000 операцій в тактах процесора: читання символу – 27 тактів, порівняння рядків – 54 такти, конкатенація рядків – 297 тактів. ** Для розрахунку взято процесор з тактовою частотою 2 ГГц з урахуванням завантаження операційною системою 5%*

Алгоритм формування криптограми в ГККК DC Нідеррайтера представимо у вигляді послідовності кроків*:*

Крок 1. Введення інформації, яка підлягає кодуванню. Введення відкритого ключа H_X^{LDPC}.

Крок 2. Формування вектора помилки *e*, вага якого не перевищує $\leq t$ – виправляє здатність LDPC-коду на основі алгоритму рівноважного кодування;

Крок 3. Формування кодограми:

$$S^* = e_n \times H_X^{LDPC^T}. \tag{26}$$

Крок 4. Формування збиткових тексту (залишок) і флагу (збиток):

$$E_{K_{MV2}} : S^* \to \left\| f\left(x\right)_i \right\| + \left\| C\left(x\right)_i \right\|. \tag{27}$$

Алгоритм розкодування кодограми в ГККК DC Нідеррайтера представимо у вигляді послідовності кроків:

Крок 1. Отримання осмисленого тексту кодограми на основі алгоритму *MV*2:

$$E_{K_{MV2}}^{-1} : \left\| f\left(x\right)_i \right\| + \left\| C\left(x\right)_i \right\| \to S^*. \tag{28}$$

Крок 2. Введення кодограми S_X, що розкодовується. Введення закритого ключа – матриць *X, P, D*.

Крок 3. Знаходження одного з можливих рішень рівняння

$$S^* = \overline{c}^* \times \left(H_X^{LDPC} \right)^T. \tag{29}$$

Крок 4. Зняття дії діагональної і переставної матриць:

$$\overline{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}. \tag{30}$$

Крок 5. Розкодування вектора $\overline{c}^{*}$. Формування вектора e_x'.

Крок 6. Перетворення вектора e_x':

$$e_x = e_x' \times P \times D. \quad (31)$$

Крок 7. Формування вектору помилки e:

$$e = e_x + IV. \quad (32)$$

Крок 8. Перетворення вектора e на основі використання недвійковий рівноважного коду в інформаційну послідовність.

На рис. 5-7 наведені результати досліджень складності формування криптограми в різних $GF(2^m)$:

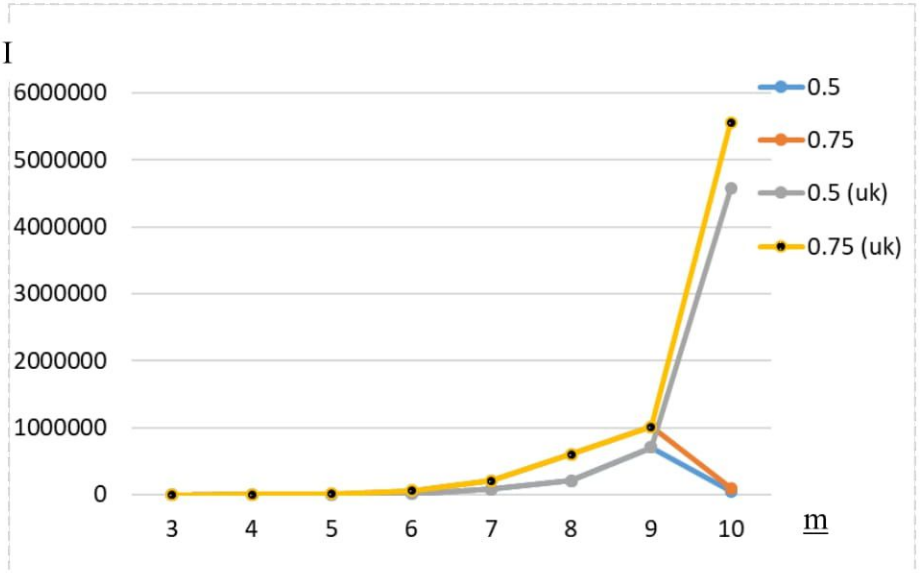


Рис. 5. Залежність складності формування криптограми в різних $GF(2^m)$

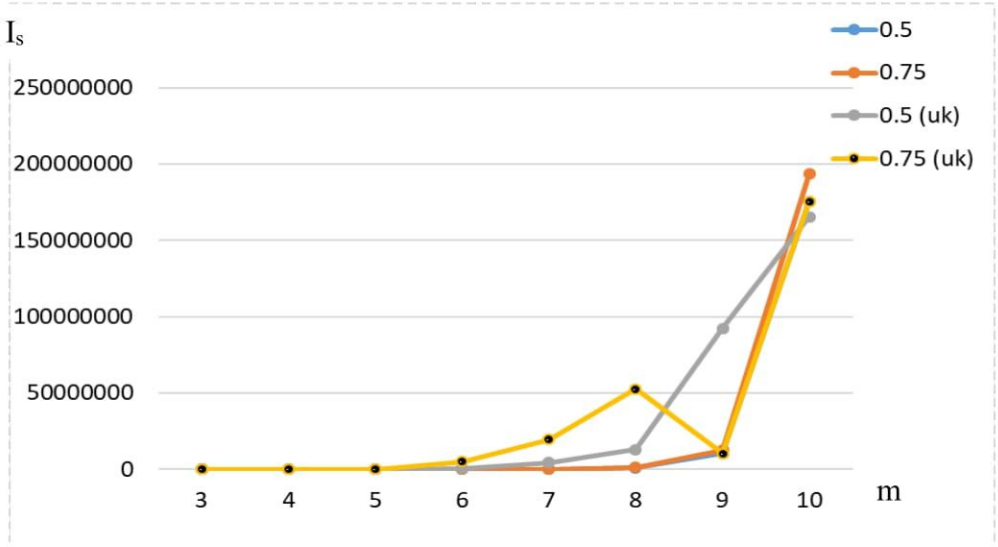


Рис. 6. Залежність складності розкодування криптограми в різних $GF(2^m)$

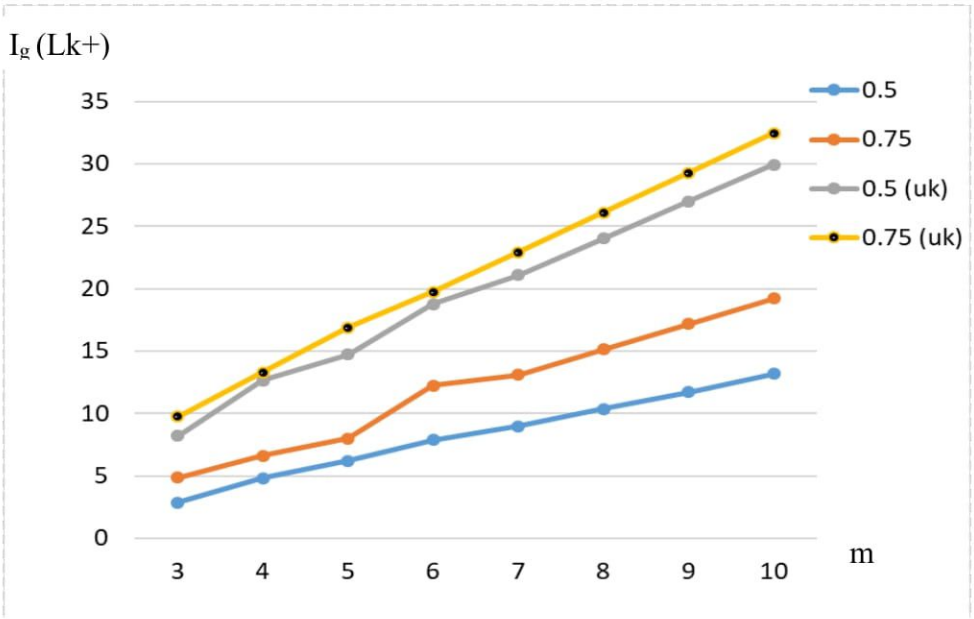


Рис. 7. Залежність складності злому над $GF(2^m)$ (переставне декодування)

Аналіз результатів розрахунків свідчить про зростання швидкості формування криптограми при використанні скорочених LDPC-кодах.

Для проведення статистичних досліджень стійкості зазначених криптосистем скористаємося пакетом *NIST STS* 822. Окремо розглядаються відсотки більше 99%, більше 96% і менше 96%.

ККК Нідеррайтера на LDPC-кодах 99% означає, що 149 з 189 тестів, або приблизно 78.83% всіх тестів, були пройдені з результатом більше 99%. Це свідчить про високу стійкість криптосистеми ККК Нідеррайтера на LDPC-кодах до статистичних тестів. Усі 189 тестів пройдені з результатом більше 96%, що демонструє повну відповідність алгоритму вимогам безпеки. Жоден із тестів не показав результату менше 96%, що підтверджує відсутність слабких місць у цій криптосистемі.

Для ККК Нідеррайтера на скорочених LDPC-кодах цей показник трохи вищий порівняно з базовою реалізацією, що свідчить про дещо більшу стійкість, тобто 96%: 189 тестів (100%). Як і в попередньому випадку, всі тести пройдені з результатом більше 96%. Повна відсутність тестів з результатом менше 96% вказує на високу надійність.

Ще більша кількість тестів у ККК DC Нідеррайтера на подовжених LDPC-кодах пройдені з результатом більше 99%, 152 тести (80.42%), що свідчить про ще вищу стійкість криптосистеми з подовженими кодами.

ГККК DC Нідеррайтера на подовжених LDPC-кодах 99%: 153 тести (80.95%) - високий показник стійкості, демонструє перевагу цієї комбінації. Повна відповідність вимогам безпеки для всіх тестів - менше 96%: 0 тестів (0%). Відсутність тестів з результатом менше 96% підтверджує надійність системи.

Найвищий показник серед всіх розглянутих криптосистем - ГККК DC Нідеррайтера на скорочених LDPC-кодах, що свідчить про найбільшу стійкість

ції конфігурації - 99%: 155 тестів (82%). Усі тести пройдені з результатом більше 96%, як і у всіх інших випадках.

Жоден тест не показав результату менше 96%, що підтверджує високу надійність.

Всі розглянуті криптосистеми демонструють високу стійкість до статистичних тестів випадковості, проведених за допомогою пакету NIST STS 822. Серед них ГККК DC Нідеррайтера на скорочених LDPC-кодах показала найвищі результати, проходячи 82% тестів з результатом більше 99%. Це свідчить про те, що такі конфігурації криптосистем мають значний потенціал для використання в умовах, де критично важлива стійкість до статистичного аналізу. Всі системи пройшли всі 189 тестів з результатом більше 96%, що підтверджує їх надійність і відповідність високим стандартам безпеки

Четвертий розділ присвячено розробці математичної моделі та методики захисту. Розвиток технологій IoT з низьким споживанням енергії та високим покриттям є однією з ключових тенденцій у сфері IoT. Ця область технологій продовжує еволюціонувати та розвиватися, і наступні напрямки її розвитку особливо актуальні.

Схема методики захисту наведена на рис.8.

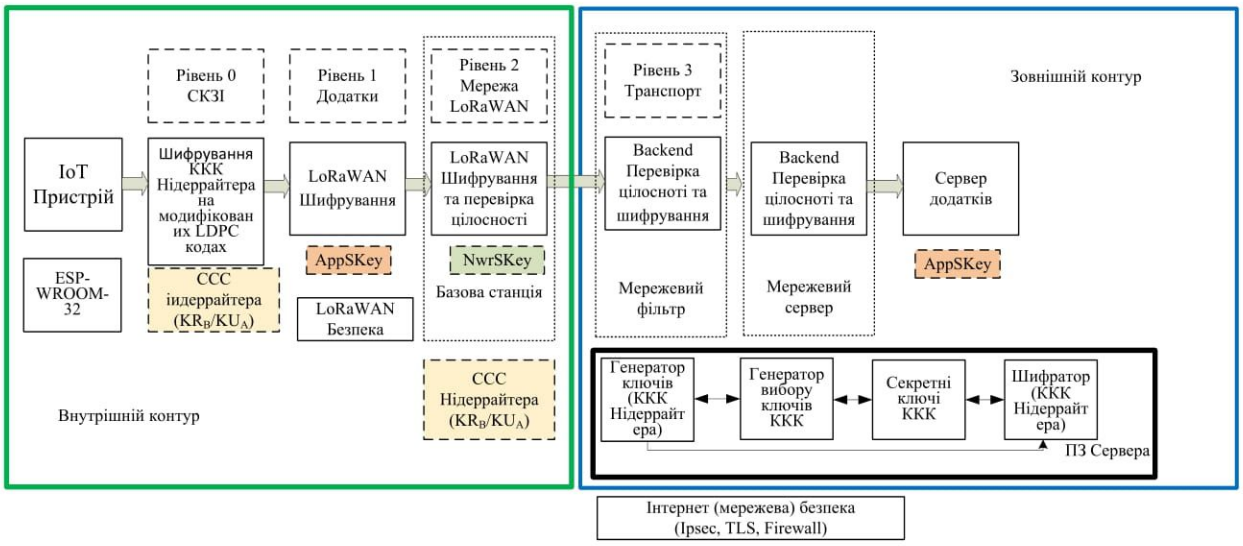


Рис. 8. Схема безпеки даних у мережі LoRaWAN з додатковим рівнем ЗКЗІ

Наведена схема пояснює розроблену методику, яка визначається таким алгоритмом:

1) обирається ознака класифікації з множини $\{H\}$, що визначає рівні впливу на ICS (CPS);

2) визначається кортеж загрози за пропонованим класифікатором;

3) формується вектор V_{ij} на основі кортежу і сформованої множини критичних загроз (на основі оцінки добутку коефіцієнтів важливості атакуючого і нападника);

4) за допомогою вектора V_{ij} визначається максимальна категорія порушника, починаючи з порушника першої категорії $\left(L_1^{del}\right)$.

Таким чином, на основі запропонованої методики будується перелік критичних загроз для кожної категорії порушників.

У разі виключення суб'єктів атак із числа потенційних порушників можна зменшити максимальну категорію порушника, а отже, і кількість критичних загроз.

Нова концепція захисту CPS повинна позбутися недоліків наявних систем і перевершує їх за наступними параметрами:

- швидкістю виявлення радіосигналів атак (це здійснюється за рахунок проведення декілька сканувань радіодіапазону за один і той же час);
- чутливістю (вимірювання проводиться двома різними за принципом дії пристроями);
- завадостійкістю, тому що апаратним і програмним способом прибираються шуми та завади радіодіапазону;
- здатністю розпізнавати випадкові радіосигнали, які можуть бути радіосигналами атак на систему, за рахунок використання нового принципу розпізнавання радіосигналів;
- здатністю створення захищених каналів або передачі захищеної інформації при передачі інформаційних сигналів і сигналів управління від виконуючих пристроїв до сервера сховища й обробки інформації.

Основним напрямком концепції є здатність створення захищених каналів при передачі інформаційних сигналів і сигналів управління від виконуючих пристроїв до сервера сховища та обробки інформації, тому що гарантований механізм передачі управлінської інформації дозволяє надійно працювати CPS.

Отже, розроблена концепція процесу захисту CPS, практично, за усіма параметрами суттєво випереджає наявні системи захисту інформації. Запропонована концепція побудована на збалансованому співвідношенні системи захисту інформації при передачі кіберпростором і системи безпеки інформації у цілому.

При моделюванні досліджувались коефіцієнт прийому пакетів (PRR) та коефіцієнт прийому бітів (BRR) для LoRa-з'єднань для двох коефіцієнтів кодування (CR) кодів Геммінга, а саме 4/5 і 4/7. Для CR 4/5 до кожних чотирьох бітів додається один перевірочний біт, який може виявити одну бітову помилку, але не може виправити жодної помилки в п'яти бітах. Для CR 4/7 коди Геммінга можуть виправити одну помилку в кожних семи бітах (рис. 9).

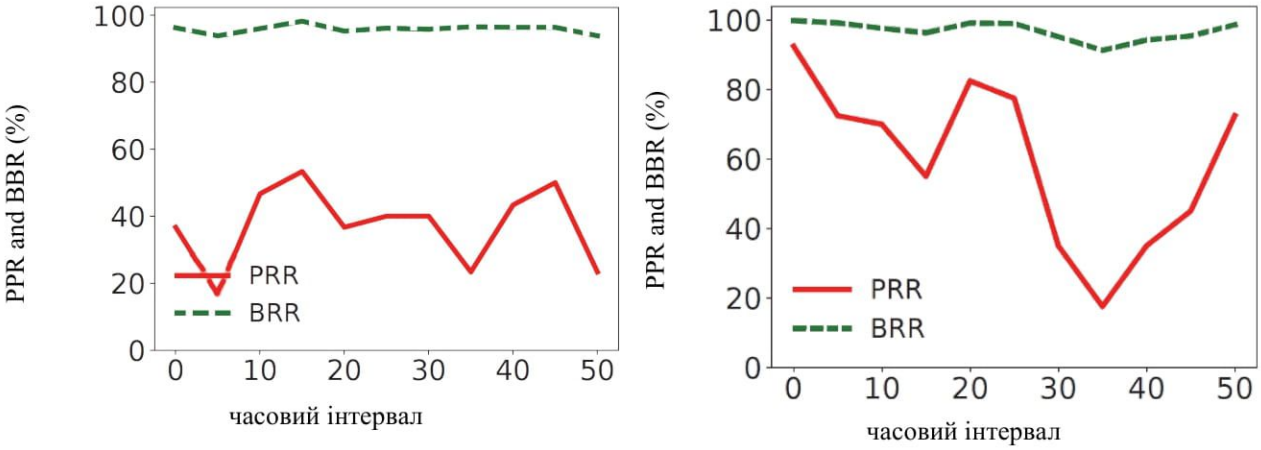


Рис. 9. Коефіцієнт прийому пакетів (PRR) та коефіцієнт прийому бітів (BRR) для різних CR кодів Геммінга для LoRa-з'єднань.

На рис.9 наведено PRR і BRR для LoRa-з'єднань для двох CR. Високий BRR і низький PRR показують, що кількість помилкових бітів у пошкоджених пакетах є невеликою, навіть якщо багато пакетів зіпсовано під час передачі.

Наведені результати моделювання підтвердили адекватність отриманих теоретичних результатів.

П'ятий розділ присвячений реалізації серверного програмно-апаратного комплексу в кіберфізичних системах та аналіз ефективності функціонування системи захисту CPS. Крім того, у розділі розроблено рекомендацій щодо застосування отриманих наукових положень і результатів. Визначено переваги розробленої методології та проведено оцінку достовірності запропонованих наукових результатів. У сучасних кіберфізичних системах особливий інтерес становить використання мікроконтролерів, що дозволяє застосовувати компактні й енергоефективні сервери для управління пристроями через веб-інтерфейси (рис.10).

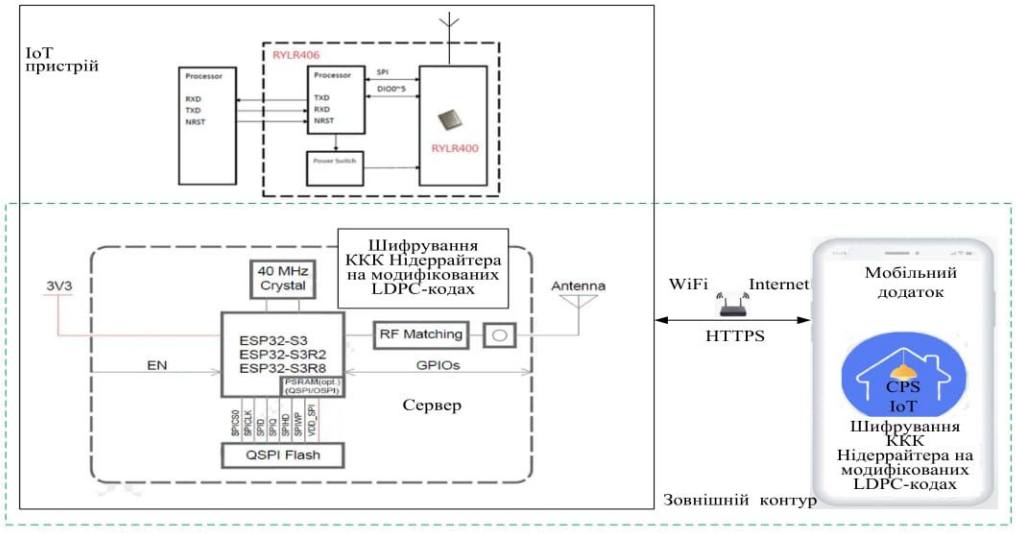


Рис. 10. Принципова схема роботи Веб серверу на базі мікроконтролеру ESP32-WROOM

Реалізація серверного програмно-апаратного комплексу на базі ESP32-WROOM показала високу ефективність у контексті кіберфізичних систем. Веб-сервер на цьому мікроконтролері забезпечує достатній рівень функціональності для віддаленого керування фізичними об'єктами через інтернет, а впровадження шифрування на основі криптосистеми Нідеррайтера з використанням LDPC-кодів у програмно-апаратному комплексі на базі ESP32-WROOM є перспективним рішенням для забезпечення захисту інформації в кіберфізичних системах. Такий підхід забезпечує високу стійкість до квантових і класичних атак, ефективне використання ресурсів для пристроїв з обмеженою обчислювальною потужністю, захист даних під час бездротової передачі.

На основі методів і моделей побудови багатоконтурних систем безпеки, а також механізмів забезпечення основних послуг безпеки на основі постквантових алгоритмів – ККК на LDPC-кодах, які відрізняються швидкістю та використовуються в мобільних «Інтернет-технологіях», запропонована нова методологія побудови системи безпеки інформаційних ресурсів на основі методів і моделей побудови багатоконтурних систем безпеки (рис.11), що містить п’ять основних етапів. Такий підхід сприяє синтезу внутрішнього та зовнішнього контурів, враховуючи оперативність, енергоефективність і відносну безпеку кожного з них.

Це дозволяє об'єктивно оцінити загрози кожного контуру з урахуванням обчислювальних ресурсів та фінансових можливостей зловмисників за допомогою комплексного показника функціональної ефективності CPS. У табл. 2 наведені результати аналізу показників даних про KPI_{norm}, KPI_{effinv} та $KPI(eff)$.

$$KPI\,(_{eff}) = \frac{R-T}{R} \times B \times P \times KPI_{effin} \times KPI_{norm}, \tag{33}$$

$$KPI_{effinv} = w_1 \frac{P}{P_{\max}} + w_2 \frac{Ef}{Ef_{\max}} + w_3 (1 - \frac{Ed}{Ed_{\max}}) + w_4 \frac{Bi}{Bi_{\max}} + ... + w_m \frac{Bn}{Bn_{\max}}, \tag{34}$$

Таблиця 2

Показники ефективності бездротових технологій низької потужності широкого радіусу

Технологія	Нормований коефіцієнт ефективності KPI_{norm}	Коефіцієнт ефективності інвестицій KPI_{effinv}	Коефіцієнт ефективності $KPI(eff)$
LoRa	0,21	0,794	0,04218
Sigfox	0,14	0,735	0,00050
LTE-M	0,68	0,378	0,00423
NB-CPS	0,56	0,753	0,00691
EC-GSM-CPS	0,35	0,875	0,36610
LoRa HCCC на LDPC-кодах	0,21	0,919	0,58586
LoRa CCC на LDPC-кодах	0,21	0,981	0,83385

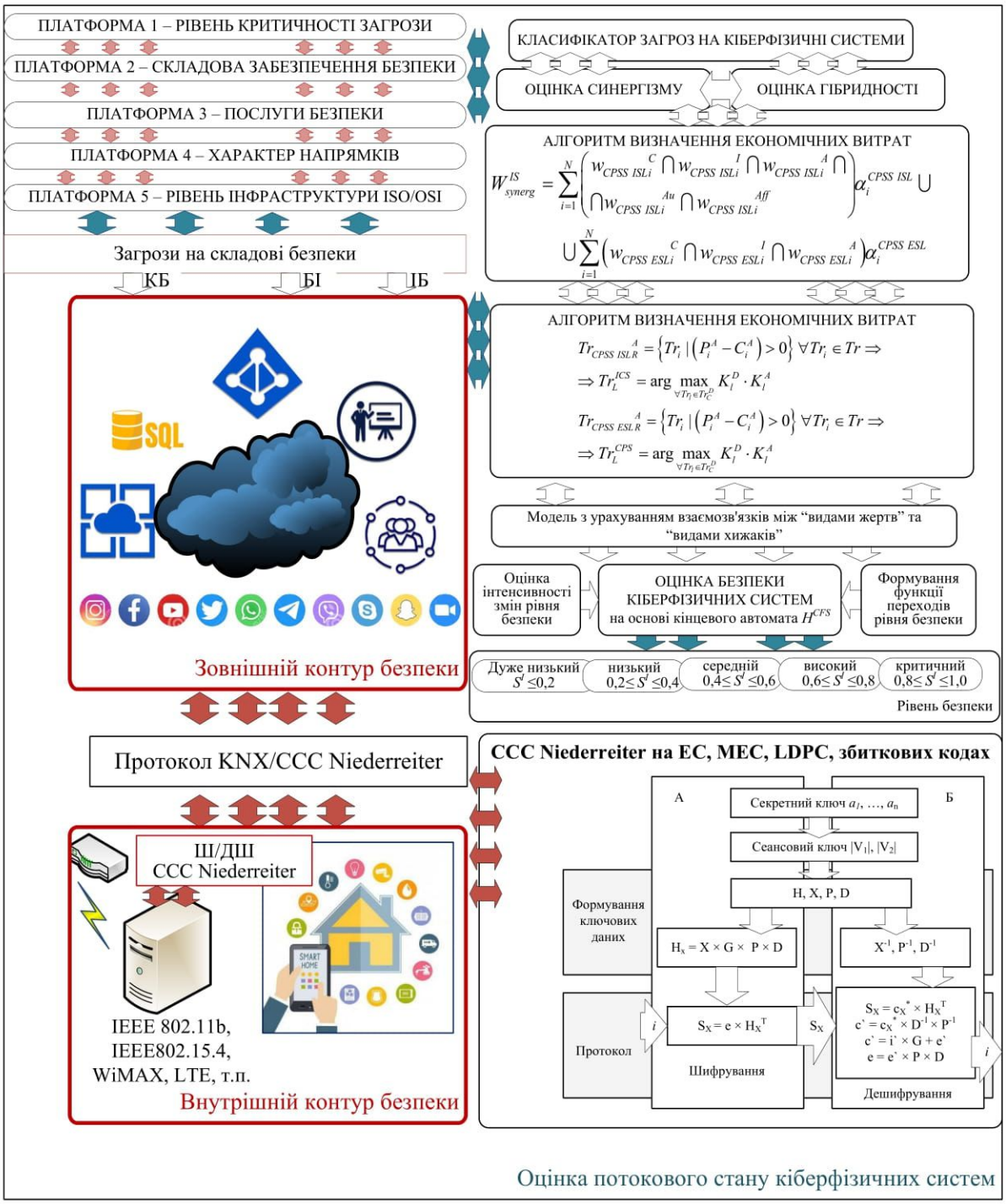


Рис. 11. Оцінка потокового стану CPS

Для підвищення показника функціональної ефективності KPI(eff) CPS пропонується застосування протоколів управління обміном даними, які дозволять забезпечити необхідні показники: оперативності передачі даних, завадостійкості та безпеки (рис.12, 13).

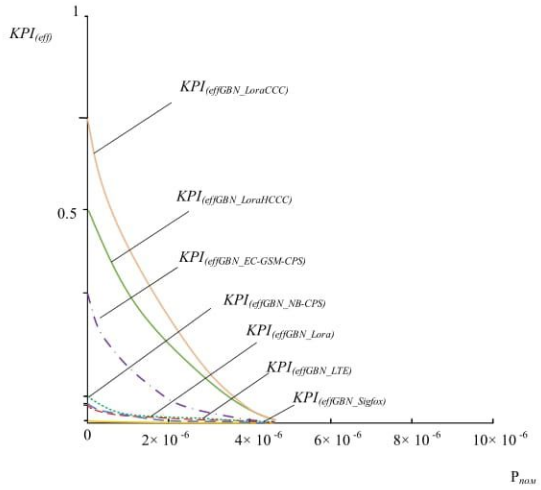


Рис.12 Оцінка комплексного показника ефективності в каналах без пам'яті

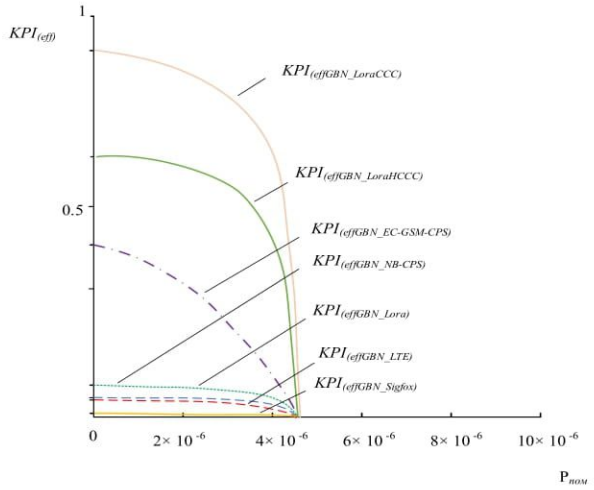


Рис. 13. Оцінка комплексного показника ефективності в каналах з пам'яттю

Результати, наведені на рис. 12, 13 і в табл. 2, підтверджують, що комплексний показник ефективності також, як й моделі каналу, без пам'яті збільшується на 10 % (LoRa ГККК на LDPC-кодах KPIeff дорівнює 0,917235,а LoRa ККК на LDPC-кодах KPIeff дорівнює 0,644446). Однак при цьому забезпечується необхідний рівень безпеки, що в умовах появи повномасштабного квантового комп'ютера (постквантовий період) та дії цільових (змішаних) атак із ознаками гібридності та синергізму забезпечує необхідний рівень безпеки елементів інфраструктури CPS.

Запропонована методика оцінки потокового стану кіберфізічної системи передавання даних безпровідними каналами зв'язку забезпечує підвищення рівня об'єктивності оцінки не тільки цільових атак (із урахуванням фінансових, обчислювальних і людських можливостей зловмисника\ів). Крім цього, забезпечується аналіз критичних точок (точок можливого несанкціонованого проникнення в інфраструктуру), а також можливості протидії кібератакам на основі спеціальних механізмів з урахуванням рівнів безпеки, які визначені.

Отже, розроблені моделі і методи захисту інформації в кіберфізичних системах. Мета досліджень щодо підвищення рівня захищеності інформації на основі запропонованої методології безпеки кіберфізичних систем шляхом побудови багатоконтурних систем захисту інформації, шляхом розробки та реалізації моделей і методів захисту інформації в кіберфізичних системах досягнута, та всі часткові завдання вирішені повністю.

ВИСНОВКИ

У результаті дисертаційних досліджень вирішена важлива науково-прикладна проблема щодо розробки моделей і методів захисту інформації в кіберфізичних системах, яка є внеском у теоретичні, методологічні, технічні, технологічні й організаційні основи створення комплексних систем захисту інформації, зокрема інформації, що зберігається, оброблюється й передається в

комп'ютерних системах і мережах та в математичні моделі інформаційних структур, що потребують захисту, шифрів, шифросистем і криптографічних протоколів. Розробка та розвиток моделей і методів захисту інформації в кіберфізичних системах має суттєве значення для проектування й модернізації наявних систем захисту інформації в кіберфізичних системах. Відсутність запропонованих у даній роботі аналогічних рішень у нашій країні та за кордоном робить результати досліджень пріоритетними.

У дисертації одержані такі основні наукові результати:

На підставі проведеного аналізу наявних моделей і методів захисту інформації в кіберфізичних системах, виявлено протиріччя між системами захисту кіберфізичних систем і навісними інформаційними технологіями в умовах обмеженого часу та збільшенні кількості й складності кіберзагроз. Відтак наявність такого протиріччя обумовлює актуальність теми дисертації, а тому вирішення поставленої науково-прикладної проблеми має важливе наукове та практичне значення.

1. Вперше розроблено концепцію побудови багатоконтурної системи захисту кіберфізичних систем, яка за рахунок інтеграції: методу забезпечення конфіденційності, цілісності й автентичності інформаційних ресурсів програмно-апаратного комплексу; методу забезпечення закриття каналу мобільного Інтернету й каналу циркуляції інформації та математичної моделі з урахуванням класифікатора загроз дає можливість створити ефективні системи захисту інформації в кіберфизичних системах і відкрити новий напрямок у побудові системи захисту інформаційних ресурсів внутрішнього й зовнішнього контуру безпеки фізичної платформи та платформи управління кіберфізичних систем.

2. Вперше розроблено математичну модель безпеки кіберфізичних систем, яка за рахунок врахування вагового коефіцієнту можливостей порушника, часу та ймовірності реалізації загрози дозволяє своєчасно визначити спрямованість загроз, врахувати обчислювальні ресурси нападників, забезпечити "зниження" ризику реалізації кіберзагроз і загалом підвищити ефективність системи захисту кіберфізичних систем.

3. Вперше розроблено метод забезпечення конфіденційності, цілісності й автентичності інформаційних ресурсів кіберфізичних систем, у якому за рахунок використання гібридних крипто-кодових конструкцій зі збитковими кодами на основі модифікованої крипто-кодової конструкції Нідеррайтера на LDPC-кодах дозволяє зменшити складність формування (лінійного перетворення) і розкодування в криптограмі, забезпечити достовірність OTP-паролів у протоколі автентифікації в умовах дії гібридних загроз.

4. Набув подальшого розвитку метод забезпечення закриття голосового каналу мобільного Інтернету, у якому за рахунок використання алгоритмів постквантової криптографії в крипто-кодових конструкціях Нідеррайтера на еліптичних кодах підвищується стійкість протоколів послуг безпеки в структурі технологій LTE та забезпечується високий рівень захищеності голосового каналу мобільного зв'язку.

5. Удосконалено класифікатор загроз безпеки інформаційних ресурсів кіберфізичних систем, який за рахунок урахування рівня критичності загроз, відношення загрози до складової безпеки, послуги безпеки, впливу загрози відповідно до регуляторів та оцінки фінансових можливостей порушника дозволяє оцінювати гібридність загроз і відкриває новий підхід побудови дієвих та перспективних систем захисту інформаційних ресурсів кіберфізичних систем.

6. Вперше розроблено методологію побудови системи безпеки інформаційних ресурсів кіберфізичних систем, яка за рахунок використання концепції побудови багатоконтурної системи безпеки, методу забезпечення конфіденційності, цілісності й автентичності інформаційних ресурсів, методу забезпечення закриття каналу мобільного Інтернету і каналу циркуляції інформації та математичної моделі з урахуванням класифікатора загроз дозволяє відкрити новий емерджентний підхід побудови діючих і перспективних систем безпеки, що підвищують ефективність захисту інформаційних ресурсів кіберфізичних систем на 5%.

7. Реалізація запропонованих моделей і методів захисту інформації в кіберфізичних системах дозволяє:

1) використовувати методику застосування класифікатора загроз безпеки інформаційних ресурсів (електронний доступ: http://skl.khpi.edu.ua) для визначення критичних точок інфраструктури кіберфізичних систем, можливості превентивних заходів та формувати оцінку потокового стану захищеності;

2) використовувати програмно-апаратний комплекс на основі мікроконтролерів, якій забезпечують автономне управління елементами кіберфізичної системи, закриття каналів зв'язку (як дротових, так й бездротових) на основі крипто-кодових конструкціях;

3) використовувати розроблений практичний протокол LoRa, який забезпечує циркуляцію інформації в кіберфізичних системах із забезпеченням необхідного рівня захищеності, серверного програмно-апаратного комплексу та дозволяє аналізувати ефективність функціонування системи захисту кіберфізичних систем.

8. Впровадження розроблених методів забезпечення конфіденційності, цілісності й автентичності інформаційних ресурсів на гібридних крипто-кодових конструкціях забезпечує зменшення в 2 – 3 рази енергетичних витрат при використанні у складі кіберфізичних систем відкритих каналів зв'язку й передачі даних при одночасному забезпеченні заданих показників безпеки.

9. Достовірність одержаних результатів підтверджується коректним використанням математичного апарату, обґрунтованими теоретичними твердженнями, а також збіжністю теоретичних результатів з результатами моделювання процесу захисту інформації в кіберфізичних системах.

10. Результати досліджень прийняті до впровадження в Державному підприємстві «Науково-технічний комплекс «Імпульс»(акт від 07.12.2021р.), в ТОВ «Мікрокрипт Текнолоджіс» (акт від 07.12.2023р.), в ТОВ «Сайфер ІТ» (акт від 10.01.24. в навчальному процесі кафедри кібербезпеки Національного

технічного університету «Харківський політехнічний інститут» при викладанні дисципліни «Основи побудови та захисту мікропроцесорних систем», «Інтернет речей та сервісів» для студентів спеціальності 125 “Кібербезпека” денної форми навчання (акт від 16.09.2022 р.).

11. Мета досліджень щодо підвищенні рівня захищеності інформації на основі запропонованої методології безпеки кіберфізичних систем шляхом побудови багатоконтурних систем захисту інформації, шляхом розробки й реалізації моделей і методів захисту інформації в кіберфізичних системах досягнута та всі часткові завдання вирішені повністю. Наукові результати досліджень є внеском у теоретичні, методологічні, технічні, технологічні й організаційні основи створення комплексних систем захисту інформації (СЗІ), зокрема інформації, що зберігається, оброблюється й передається в комп’ютерних системах і мережах та у математичні моделі інформаційних структур, що потребують захисту, шифрів, шифросистем і криптографічних протоколів.

12. Перспективними шляхами подальших досліджень у зазначеному напрямку може бути широке коло питань щодо розробки нових та удосконалення наявних методів і методик забезпечення безпеки каналів обміну інформації в кіберфізичних системах на фоні зростання завантаженості частотного радіодіапазону.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Yevseiev S., Hryshchuk R., Molodetska K, Pohasii S., Nazarkevych M., Hrytsyk V., Milov O. et. al.; (2022). Modeling of security systems for critical infrastructure facilities. Kharkiv: Pc Technology Center, 196p.

2. Yevseiev S., Ponomarenko V., Laptiev O., Milov O., Pohasii S., Korol O., Milevskyi S. et. al.; (2021). Synergy of building cybersecurity systems. Kharkiv: Pc Technology Center, 188p. (Scopus)

3. Yevseiev S., Katsalap V., Mikhieiev Y., Savchuk V., Pribyliev Y., Milov O., Pohasii S., Opirskyy I., Lukova-Chuiko N., & Korol I. (2022). «Development of a method for determining the indicators of manipulation based on morphological synthesis». Eastern-European Journal of Enterprise Technologies, 3(9 (117), pp.22–35. (Scopus)

4. Yevseiev S., Milov O., Milevskyi S., Voitko O., Kasianenko M., Melenti Y., Pohasii S., Stepanov H., Turinskyi O., & Faraon S. (2020). «Development and analysis of game-theoretical models of security systems agents interaction». Eastern-European Journal of Enterprise Technologies, 2(4 (104), pp.15–29. (Scopus)

5. Shmatko O., Balakireva S., Vlasov A., Zagorodna N., Korol O., Milov O., Petrov O., Pohasii S., RzayevK., & Khvostenko V. (2020). «Development of methodological foundations for designing a classifier of threats to cyberphysical

systems». Eastern-European Journal of Enterprise Technologies, 3(9 (105), pp.6–19. (Scopus)

6. Yevseiev S., Pohasii S., Zhuchenko O., Milov O., Lysechko V., Kovalenko O., Kostiak M., Volkov A., Lezik A., & Susukailo V. (2022). «Development of crypto-code constructs based on LDPC codes. Eastern-European Journal of Enterprise Technologies», 2(9 (116), pp.44–59. (Scopus)

7. Yevseiev S., Milov O., Pohasii S., Ryabukha Y., Milevskyi S., Melenti Y., Ivanchenko Y., Ivanchenko I., Opirskyy I., & Pasko I. (2021). «Development of a method for assessing forecast of social impact in regional communities». Eastern-European Journal of Enterprise Technologies, 6(2 (114), pp.30–43. (Scopus)

8. Yevseiev S., Pohasii S., Milevskyi S., Milov O., Melenti Y., Grod I., Berestov D., Fedorenko R., & Kurchenko O. (2021). «Development of a method for assessing the security of cyber-physical systems based on the Lotka–Volterra model». Eastern-European Journal of Enterprise Technologies, 5(9 (113), pp.30–47. (Scopus)

9. Yevseiev S., Biesova O., Kyrychenko D., Lukashuk,O., Milevskyi S., Pohasii S., Husarova I., Goloskokova A., & Sobchenko V. (2021). «Development of a method for estimating the effect of transformation of the normalized frequency mismatch function of a coherent bundle of radio pulses on the quality of radar frequency resolution». Eastern-European Journal of Enterprise Technologies, 4(4(112), pp.13–22. (Scopus)

10. Yevseiev S., Pohasii, S., Rzayev K., Laptiev O., Camalova J. (2022). «Development of a hardware cryptosystem based on a random number generator with two types of entropy sources». Eastern-European Journal of Enterprise Technologies 5(9-119), C. 6-16. (Scopus)

11. Pohasii S. (2021). «The mathematical model of information network protection based on hierarchic hypernetworks». Scientific discussion. Praha, Czech Republic.VOL 1, No 61, pp.31– 36

12. Pohasii S. (2021). «Analysis of information security threat assessment of the objects of information activity». International independent scientific journal. Poland. Vol. 1, №34, pp.33 – 39.

13. Pohasii S. (2021). «Information security of the e-government». Journal of science. Lyon. VOL.1, №27, pp. 49– 54.

14. Pohasii S. (2021). «Detection illegal of means of obtaining of information by the method of determining the deviation of the characteristics of radio signal from the specified parameters». Znanstvena misel journal. Slovenia. VOL., 1№6,1 pp. 23– 29

15. Pohasii S. (2021). «The methodology of automatical detection of digital illegal obtaining means of information». Scientific discussion. Praha, Czech Republic.VOL 1, No 62, pp.16– 22

16. Погасій С. (2022). «Моделі і методи захисту інформації в кіберфізичних системах». Безпека інформації. Том 28 № 2, С. 67– 79.

17. Погасій С. (2022). «Оцінка рівня безпеки в кіберфізичних системах. Захист інформації». Том 24 № 2, С. 81– 94.

18. Pohasii S., Milov O., Milevskyi S., Rzayev K. (2019). «Procedural basis of cybersecurity systems». Системи управління, навігації та зв'язку. Полтава : ПНТУ, Вип. 5(57). С. 81– 86.

19. Pohasii S., Voropay A., Korol O., Milevskyi S. (2022). «Development of security mechanismsfor scada systems in the postquantium period». Системи обробки інформації, 2022, випуск 2 (169), С. 25– 33.

20. Pohasii S., Milevskyi S., Zhuchenko O., Tomashevsky B., Rahimova I. and Serhiiev S. (2021). «Development of Niederriter crypto-code design models on LDPC-codes», Information Processing Systems, (4(167), pp. 58– 68.

21. Yevseiev S., Pohasii S., & Khvostenko V. (2021). «Development of a protocol for a closed mobile internet channel based on post-quantum algorithms». Information Processing Systems, (3(166), С.35– 40.

22. Milov O., Parkhuts L., Pohasii S., Milevskyi S. (2019) «Verification of the security systems antagonistic agents behavior model», Information Processing Systems, (4(159), pp. 65– 81.

23. Pohasii S., Milevskyi S., Tomashevsky B., & Voropay N. (2022). «Development of the double-contour protection concept in socio-cyberphysical systems». Advanced Information Systems, 6(2), С.57–66.

24. Rahimova I., Qubadova F., Asker zade B., & Pohasii S. (2019). «Javascript security using cryptographic hash functions». Advanced Information Systems, 3(4), С.105–108.

25. Лукова-Чуйко Н., Погасій С., Толюпа С., Лаптєва Т., & Лаптєв С. (2022). «Удосконалення моделі захисту інформаціїї в соціальних мережах». Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка, (73), С.88–103.

26. Наконечний В., Лаптєв О., Погасій С., Лазаренко С., Мартинюк Г. (2021). «Відбір джерел з неправдивою інформацію методом бджолиної колонії». Наукоємні технології № 4(52), pp.330– 337.

27. Погасій С. (2023). «Застосування збиткових LDPC кодів в стандарті LORAWAN». Ukrainian Scientific Journal of Information Security. № 29. С.73– 79.

28. Pohasii S., Yevseiev S., Tymchenko V., Kutsenko S. and Milevskyi S. (2022). «Measuring Signals Synthesis Method on the Basis of Triangular Time-Pulse Modulation for Control of Radiotechnic Systems Technical Condition», 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2022, pp. 1-5, (Scopus).

29. Pohasii S., Yevseiev S., Milevskyi S., Bortnik L., Alexey V. and Bondarenko K., (2022) «Socio-Cyber-Physical Systems Security Concept», 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2022, pp. 1-8, (Scopus).

30. Hatsenko L., Pohasii S., Lutsenko A., Skopintsev O. (2021). «Investigation of Measurement Errors of Electrical Signals Characteristics of Energy Supply Systems». 2021CEUR Workshop Proceedings 3126, C. 184-191, (Scopus).

31. Hatsenko L., Herasimov S., Pohasii S. (2021). «Investigation of the Effect of Harmonic Interference on the Error with Frequency Conversion of Energy Supply Systems on Water Transport Vehicles». 2021CEUR Workshop Proceedings 3188, C. 237-243, (Scopus).

32. Yevseiev S., Milov O., Pohasii S., Melenti Y., Milevskyi S. (2021). «Cyber Terrorism as an Object of Modeling». 2021 CEUR Workshop Proceedings 3200, C. 204-210, (Scopus).

33. Yevseiev S., Pohasii S., Korol O., Veselska O., Khvostenko V. (2021). «Evaluation of Cryptographic Strength and Energy Intensity of Design of Modified Crypto-Code Structure of McEliece with Modified Elliptic Codes». 2021CEUR Workshop Proceedings 3200, C. 135-148, (Scopus).

34. Vorobiov B., Pohasii S., Zaitsev R., Minakova K., Kirichenko M., Milevskyi S. (2022) «Regulation Quality Investigation on Different Plant Model Usage While Neural Network Training for DC Motor Control», 2022 IEEE 4th International Conference on Modern Electrical and Energy System (MEES), Kremenchuk, Ukraine, 2022, pp. 1-6, (Scopus).

35. Pohasii S., Korolov R., Vorobiov B., Bril M., Serhiienko O. and Milevskyi S. (2022). «UAVs Intercepting Possibility Substantiation: Economic and Technical Aspects,» 2022 IEEE 4th International Conference on Modern Electrical and Energy System (MEES), Kremenchuk, Ukraine, 2022, pp. 1-6 (Scopus).

36. Pohasii S., Baranova V., Bilotserkivskyi O., Haponenko O., Serhiienko O. and Vorobiov B. (2022). «Application of Cost-Effective Acoustic Intelligence to Protect Critical Facilities from Drone Attacks», 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 2022, pp. 1-6, (Scopus).

37. Herasymov S., Yevseiev S., Pohasii S., Olenchenko V. and Milevskyi S. (2022). «Investigation of the Dynamic Filters' Characteristics for the Analysis of Random Signals During Data Transmission», 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 2022, pp. 1-6, (Scopus).

38. Pohasii S., Vorobiov B. (2021). Analysis of the applicability of the model of the quality of software systems and the most important parameters of the quality of iot systems. Modern directions of scientific research development. Proceedings of the 6th International scientific and practical conference. BoScience Publisher. Chicago, USA. pp. 204-212.

39. Pohasii S., Vorobiov B. (2021). «Еволюція кіберфізичних систем». Topical issues of modern science, society and education. Proceedings of the 5rd International scientific and practical conference. SPC “Sci-conf.com.ua”. Kharkiv, Ukraine. pp. 440-446.

40. Pohasii S., Vorobiov B. (2021). Building an ontology of the software architecture of the internet of things. The 4th International scientific and practical conference “Innovations and prospects of world science” (December 1-3, 2021) Perfect Publishing, Vancouver, Canada. pp 252-257.

41. Погасій С., Гаврилова А. (2020). «Використання геш-кодів, створених за допомогою алгоритма UMAC на крипто-кодових конструкціях, для забезпечення необхідного рівня стійкості до зломів». Матеріали регіон. круг. столу «Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони». Харків, 2020. С. 290 – 294.

42. Pohasii S., Milevskyi S. (2019). «Cybersecurity issues in the internet of things». 1st International Conference: Modern Information, Measurement and Control Systems: Problems and Perspectives (MIMCS’2019), p. 33.

43. Pohasii S., Milevskyi S. (2019). «Internet security problems caused by artificial intelligence» Матеріали Міжнародної науково-практичної конференції «Економічний розвиток і спадщина Семена Кузнеця»: тези доповідей, 30 – 31 травня 2019 р. – Х.: ХНЕУ імені Семена Кузнеця, С.248-249.

44. Pohasii S., Milevskyi S., Voropay N., Korol O. (2022). «A Multilevel Approach to the Security of the Internet of Things». «Modern Information, Measurement and Control Systems: Problems, Applications and Perspectives 2022 (MIMCS’2022)».

АНОТАЦІЯ

Погасій С.С. Моделі і методи захисту інформації в кіберфізичних системах. – Рукопис.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». – Державний університет інформаційно-комунікаційних технологій, Київ, 2024.

У роботі вирішена важлива науково-прикладна проблема щодо розробки моделей і методів захисту інформації в кіберфізичних системах, яка є внеском у теоретичні, методологічні, технічні, технологічні й організаційні основи створення комплексних систем захисту інформації, зокрема інформації, яка зберігається, оброблюється і передається в комп’ютерних системах і мережах та в математичні моделі інформаційних структур, що потребують захисту, шифрів, шифросистем і криптографічних протоколів. Розробка й розвиток моделей і методів захисту інформації в кіберфізичних системах має суттєве значення для проектування та модернізації наявних систем захисту інформації в кіберфізичних системах. Впровадження розроблених методів забезпечення конфіденційності, цілісності й автентичності інформаційних ресурсів на гібридних крипто-кодових конструкціях забезпечує зменшення в 2 – 3 рази енергетичних витрат при використанні у складі кіберфізичних систем відкритих

каналів зв’язку та передачі даних при одночасному забезпеченні заданих показників безпеки

Ключові слова: кіберфізичні система, захист інформації, спектр радіосигналів, багатоконтурні системи безпеки, моделі безпеки, сінергія загроз, крипто-кодовіконструкції Нідеррайтера.

ABSTRACT

Pogasii S.S. Models and methods of information protection in cyber-physical systems. - The manuscript.

Dissertation for obtaining the scientific degree of Doctor of Technical Sciences in the specialty 05.13.21 «Information protection systems». - State University of Information and Communication Technologies, Kyiv, 2024.

The work solves an important scientific and applied problem regarding the development of models and methods of information protection in cyber-physical systems, which is a contribution to the theoretical, methodological, technical, technological and organizational foundations of the creation of complex information protection systems, in particular information that is stored, processed and transferred to a computer computer systems and networks and mathematical models of information structures that require protection, ciphers, cipher systems and cryptographic protocols. The development and evolution of models and methods of information protection in cyber-physical systems is essential for the design and modernization of existing information protection systems in cyber-physical systems. The implementation of the developed methods of ensuring the confidentiality, integrity and authenticity of information resources on hybrid crypto-code constructions ensures a 2-3 times reduction in energy costs when using open channels of communication and data transmission as part of cyber-physical systems while simultaneously ensuring the specified security indicators

Keywords: cyber-physical system, information protection, spectrum of radio signals, multi-contour security systems, security models, synergy of threats, Niederreiter's crypto-code constructions.