МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Семенов Сергій Геннадійович

УДК 004.77:621.39(043.3)

МЕТОДИ ТА ЗАСОБИ РОЗПОДІЛУ ДОСТУПУ І ЗАХИСТУ ДАНИХ В КОМП'ЮТЕРИЗОВАНИХ ІНФОРМАЦІЙНИХ УПРАВЛЯЮЧИХ СИСТЕМАХ КРИТИЧНОГО ЗАСТОСУВАННЯ

Спеціальність 05.13.05 – комп'ютерні системи та компоненти

Автореферат

дисертації на здобуття наукового ступеня

доктора технічних наук

Харків – 2013

Дисертацією є рукопис.

Роботу виконано на кафедрі обчислювальної техніки та програмування Національного технічного університету «Харківський політехнічний інститут» Міністерства освіти і науки України.

Науковий консультант: доктор технічних наук, професор **Порошин Сергій Михайлович**, Національний технічний університет «Харківський політехнічний інститут», завідувач кафедри мультимедійних інформаційних технологій і систем

Офіційні опоненти: доктор технічних наук, професор **Алішов Надір Ісмаіл-огли,** Інститут кібернетики ім. В.М.Глушкова НАН України, провідний науковий співробітник

доктор технічних наук, професор **Лужецький Володимир Андрійович**, Вінницький національний технічний університет, завідувач кафедри захисту інформації

доктор технічних наук, професор **Фурман Ілля Олександрович**, Харківський національний технічний університет сільського господарства ім. Петра Василенка, завідувач кафедри автоматизації та комп'ютерно-інтегрованих технологій

Захист відбудеться «07» листопада 2013 р. о 14.30 годині на засіданні спеціалізованої вченої ради Д 64.050.14 у Національному технічному університеті «Харківський політехнічний інститут» за адресою: 61002, Харків, вул. Фрунзе, 21 (електрокорпус, 1-й поверх, ауд. 54-Б).

З дисертацією можна ознайомитися у бібліотеці Національного технічного університету «Харківський політехнічний інститут».

Автореферат розісланий «03» жовтня 2013 р.

Вчений секретар
спеціалізованої вченої ради І.Г. Ліберг

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Активне впровадження комп'ютерних технологій критичного застосування в ключові сфери життєдіяльності суспільства є характерною рисою існування сучасної держави. При цьому одну з основних функцій, моніторингу та доставки даних про властивості й стан будь-якого об'єкту управління виконують комп'ютеризовані інформаційні управляючи системи. Проте чим складніше завдання автоматизації і чим відповідальніше галузь, в якій вони використовуються, тим критичнішими і жорсткішими стають вимоги до ключових показників, що визначають безпеку функціонування системи.

Події останніх років свідчать, що сучасні засоби забезпечення безпеки в комп'ютеризованих інформаційних управляючих системах критичного застосування (КІУСКЗ) потребують подальшого удосконалення. Пов'язано це передусім з тим, що масове поширення комп'ютерних мережевих технологій суттєво розширило можливості зловмисників у використанні методів і засобів несанкціонованого доступу до інформації. У той же час рівень розвитку засобів діагностування й реагування на деструктивні зміни режимів функціонування і внутрішніх характеристик КІУСКЗ не змінюється.

Сучасний прогрес в галузі комп'ютерних технологій сприяв розробці численних методів, призначених для забезпечення безпеки інформації. Проте стосовно до КІУСКЗ ці методи часто не мають належної теоретичної основи, а опис властивостей, переваг і недоліків спирається лише на практичний досвід використання, що не достатньо для забезпечення їхньої успішної роботи в умовах широкого спектра зовнішніх впливів на систему.

У теорії захисту інформації накопичений певний теоретичний матеріал і практичний досвід. Найбільш значними роботами в цій області є дослідження зарубіжних і вітчизняних учених, серед яких Д Д. Деннинг, Е. Спаффорд, В. Столлингс, Б. Шнаер, І.Д. Горбенко, В.І. Долгов, О.О. Кузнецов та ін. Проте динамічний розвиток комп'ютерної техніки, інтелектуалізація інформаційно-обчислювальних засобів, а також різноманіття програмних технологічних рішень сприяють тому, що постановка завдань захисту даних в КІУСКЗ значно видозмінюється через необхідність урахування впливу нових чинників.

Таким чином, проблема розробки методів та засобів розподілу доступу і захисту даних в КІУСКЗ для забезпечення гарантованого рівня безпеки в умовах зовнішніх впливів має науково-практичне значення, є актуальною і визначила напрями досліджень дисертаційної роботи.

Зв'язок роботи з науковими планами, програмами, темами. Дисертаційну роботу виконано на кафедрі обчислювальної техніки та програмування НТУ «ХПІ». Здобувач, як співвиконавець окремих етапів, проводив дослідження у рамках держбюджетних НДР МОН України: «Розвиток теорії стабільно-пластичних нейронних мереж для розв’язання задач класифікаційної оптимізації і керування динамічними об’єктами» (№ Д.Р. 0213 U 001289), «Розробка інтелектуальних систем підтримки прийнятих рішень для діагностики, керування та оптимізації технічних та біологічних об’єктів» (№ Д.Р. 0113 U 000449), «Розвиток, стандартизація, уніфікація, удосконалення та впровадження

інфраструктури відкритих ключів, включаючи національну систему ЕЦП на національному та міжнародному рівнях» (наказ МОН України №1177 від 30.11.2010 р.), та госпдоговірної НДР «Розробка методів, комплексів та засобів ІВК для національних та міжнародних інформаційно-телекомунікаційних систем та інформаційних технологій» (АТ ІІТ м. Харків) (№ Д.Р. 0111 U 002634).

Мета і завдання дослідження. Метою дисертаційної роботи стало забезпечення гарантованого рівня безпеки даних в комп'ютеризованих інформаційних управляючих системах критичного застосування в умовах зовнішніх впливів на основі розробки методів та засобів розподілу доступу і захисту даних.

Для досягнення мети поставлені такі завдання:

- провести аналіз вимог безпеки інформації, показників і критеріїв оптимізації, моделей і методів захисту даних в КІУСКЗ;
- розробити комплекс моделей КІУСКЗ, що враховують вплив управляючого і зовнішніх деструктивних дій, а також малих збурень і похибок виміру параметрів на вихідні характеристики системи;
- розробити метод оцінки захищеності КІУСКЗ, що відрізняється від відомих урахуванням особливостей структурної і функціональної побудови системи;
- розробити мережевий метод дослідження параметрів КІУСКЗ на основі багатошарової *GERT*-мережі, що дозволяє врахувати багаторівневість її структурно-функціональної побудови;
- розробити метод структурної ідентифікації стану КІУСКЗ, що враховує статистичні залежності в змінах стану системи в умовах зовнішніх впливів;
- розробити комплекс методів адаптивного управління КІУСКЗ, які використовують інтелектуальний підхід до виявлення порушень безпеки на множині параметрів КІУСКЗ;
- розробити метод підвищення скритності сигналів при передачі бінарних повідомлень в мобільному сегменті КІУСКЗ, який враховує особливості приховання інформації в сигналі, що представляє хаотичну послідовність;
- розробити метод оптимального налаштування параметрів розподілу доступу в КІУСКЗ, що відрізняється від відомих урахуванням основних показників адміністрування сучасних операційних систем;
- провести критеріальну порівняльну оцінку ефективності застосування розроблених методів та засобів захисту даних в КІУСКЗ.

Об'єкт дослідження – процес забезпечення безпеки даних в КІУСКЗ в умовах зовнішніх впливів.

Предмет дослідження – методи та засоби розподілу доступу і захисту даних в КІУСКЗ.

Методи дослідження. При розробці методу оцінки захищеності та методу мереженого моделювання КІУСКЗ використовувалися методи теорії нелінійної динаміки, динамічного хаосу, оптимізаційні методи дослідження операцій і методи теорії графів. При розробці методів структурної ідентифікації стану і управління безпекою даних використовувалися методи фрактального аналізу, теорії інформації і теорії складних систем, методи оцінки *BDS*-статистики, застосовувався математичний апарат інтелектуальних нейронних мереж. Оцінка

експериментальних даних, отриманих в ході роботи, проводилася на основі методів математичної статистики.

Вибір методів досліджень забезпечив *достовірність* отриманих результатів і висновків, що підтверджується збіжністю результатів експериментальних досліджень, отриманих при програмній реалізації алгоритмів ідентифікації й управління безпекою даних з теоретичними та практичними результатами, і обумовлена їхньою відповідністю положенням теорії захисту даних.

Наукова новизна отриманих результатів. У результаті виконання роботи набув подальшого розвитку науковий напрям, пов'язаний з розробкою методів та засобів розподілу доступу і захисту даних в КІУСКЗ. У рамках цього напряму отримані такі наукові результати.

Уперше розроблені:

- метод оцінки захищеності КІУСКЗ, який відрізняється від відомих урахуванням особливостей структурної і функціональної побудови системи, що дало можливість визначити рівень чутливості системи до деструктивних дій і оцінити міру впливу нелінійності зовнішніх дій і незалежності внутрішніх збурень на стан системи в трирівневому режимі функціонування, що дозволило до 15% підвищити точність виявлення зовнішніх впливів на систему;

- мережевий метод дослідження параметрів КІУСКЗ на основі багатошарової *GERT*-мережі, який на відміну від відомих враховує багаторівневість її структурно-функціональної побудови, що дозволило знайти функції і щільність розподілу ймовірності випадкових характеристик зовнішніх дій на систему та оцінити її основні ймовірнісно-часові характеристики;

Удосконалені:

- метод структурної ідентифікації стану КІУСКЗ, що враховує статистичні залежності в змінах стану системи в умовах зовнішніх впливів і відрізняється від відомих використанням як параметрів стану системи координат особливих точок квазістатичних циклів спостережуваних структурно-інформаційних портретів, що дозволило зменшити час структурної ідентифікації системи до 2 разів;

- метод оптимального налаштування параметрів розподілу доступу в КІУСКЗ, який відрізняється від відомих урахуванням основних показників адміністрування сучасних операційних систем, що дозволило мінімізувати складність налаштувань розподілу доступу в КІУСКЗ;

Отримали подальший розвиток:

- метод підвищення скритності сигналів при передачі бінарних повідомлень у мобільному сегменті КІУСКЗ, який відрізняється від відомих використанням процедури перемішування хаотичної послідовності несучої, що призводить до нерегулярної поведінки траєкторії сигналу у фазовому просторі (площини), характерному для випадкових процесів; робить неефективним використання відомих методів якісного та кількісного аналізу нелінійних динамічних систем у фазовому просторі і, як наслідок, дозволяє підвищити скритність сигналів при передачі бінарних повідомлень до 2 разів;

- комплекс методів адаптивного управління безпекою КІУСКЗ, який на відміну від відомих використовує інтелектуальний підхід щодо виявлення порушень безпеки на множині параметрів КІУСКЗ, що дозволить вирішувати

завдання виявлення причин деструктивних змін стану системи і контролю параметрів відповідно до гарантованих вимог безпеки. Це дозволить до 1,5 раза збільшити час функціонування КІУСКЗ у безпечному режимі.

Практичне значення отриманих результатів у галузі комп'ютерних систем і компонент даних полягає в тому, що розроблені в дисертаційній роботі методи та засоби розподілу доступу і захисту даних в КІУСКЗ є науково-методичною основою для розробки відповідних алгоритмів, програмних засобів і протоколів забезпечення безпеки інформації.

Метод структурної ідентифікації стану КІУСКЗ та комплекс методів адаптивного управління безпекою КІУСКЗ використані при розробці автоматизованих систем контролю і вимірів АСКВ "ТФ" і АСКВ "ТМА" на НТ СКБ "Полісвіт" Державного науково-виробничого підприємства "Комунар" (м. Харків).

Метод оптимального налаштування параметрів розподілу доступу в КІУСКЗ та метод підвищення скритності сигналів при передачі бінарних повідомлень в мобільному сегменті КІУСКЗ застосовані при удосконаленні засобів захисту комп'ютеризованої інформаційно-вимірювальної системи державного підприємства "Харківський науково-дослідний інститут технології машинобудування" (м. Харків).

Метод оцінки захищеності КІУСКЗ та комплекс моделей КІУСКЗ були використані при розробці систем захисту інформації Центру контролю космічного простору у рамках НДР шифр "Обгрунтування КС", шифр "Спостереження", та шифр "Перспектива-КА" (м. Євпаторія).

Комплекс математичних моделей КІУСКЗ та метод оцінки захищеності КІУСКЗ впроваджені при юстуванні обладнання зв'язку загону оперативно-рятувальної служби (м. Харків).

Метод структурної ідентифікації стану КІУСКЗ та алгоритми управління безпекою використані при налаштуванні системи захисту інформації служби автоматики і зв'язку КП "Київпастранс" (м. Київ).

Метод оцінки захищеності КІУСКЗ та модель адаптивного управління безпекою КІУСКЗ були використані при розробці системи захисту комп'ютерної мережі ТОВ "Транс-Техно-Сервіс" (м. Харків).

Розроблені методи та засоби впроваджені в навчальному процесі кафедри обчислювальної техніки та програмування Національного технічного університету «ХПІ» в курсах: «Захист інформації», «Комп'ютерні системи та їх тестування», в навчальному процесі кафедри програмного забезпечення Кіровоградського Національного технічного університету в курсах «Основи захисту інформації» «Захист інформації в комп'ютерних системах» «Дослідження та проектування комп'ютерних систем та мереж» та «Програмування комп'ютерних мереж».

Особистий внесок здобувача. Усі основні результати, які виносяться на захист, одержані здобувачем особисто, серед них – метод знаходження оптимальної множини маршрутів при управлінні інформаційними потоками у системі зв'язку стандарту *3G*, метод розподілу канальних ресурсів мережевого устаткування при інформаційному обміні в єдиній автоматизованій системі управління, класифікація методів прогнозування в телекомунікаційних мережах

автоматизованих систем управління, узагальнена структурно-функціональна модель КІУСКЗ з комплексним показником ефективності їхнього функціонування, структурно-інформаційний портрет інформаційної системи в умовах невизначеності на прикладі *Dos*-атаки, методика математичного моделювання КІУСКЗ на основі багатошарової *GERT*-мережі.

Апробація результатів дисертації. Основні результати роботи доповідалися і обговорювалися на науково-технічних та науково-практичних конференціях: «Перспективи розвитку озброєння і військової техніки в Збройних Силах України» (Львів, 2008-2010); «Наукові технології – для захисту повітряного простору» (Харків, 2008-2012); «Проблемы информатики и моделирования» (Харків, 2008, 2011); «Проблемы интеграции информации – 2008: исследования, разработки, интеллектуальная собственность» (Харків, 2008); «Інформаційні технології в навігації і управлінні: стан та перспективи розвитку» (Київ, 2010, 2011); «Statistical Methods Of Signal and Data Processing (SMSDP–2010)» (Київ, 2010); «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (Харків, 2011); «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засоби управління» (Київ, 2011); «Modern problems of radio engineering, telecommunications and computer science» (TCSET'2012) (Львів-Славське, 2012); «Безопасность информации в информационно-телекоммуникационных системах» (Київ, 2012); «Інформаційні проблеми теорії акустичних, радіоелектронних та телекомунікаційних систем» (IPST-2012) (Алушта, 2012); «Современные направления развития информационно-телекоммуникационных технологий и средств управления» (Росія, Белгород, 2013).

Публікації. Основні результати роботи відображено у 60 наукових публікаціях, з них – 2 монографії, 37 статей у наукових фахових виданнях України та 21 – у матеріалах конференцій.

Структура та об'єм дисертації. Дисертаційна робота складається зі вступу, шести розділів, висновків, додатків та списку використаних джерел. Повний обсяг дисертації становить 348 сторінок: з них 73 рисунка за текстом; 11 рисунків на 9 окремих сторінках; 18 таблиць за текстом; 8 додатків на 44 сторінках; 234 найменувань використаних джерел на 25 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми дисертаційних досліджень, сформульовано її мету та задачі, визначено об'єкт, предмет і методи дослідження, наукову новизну та практичну значущість роботи.

У першому розділі проведено аналіз науково-технічної проблеми розподілу доступу та захисту даних в КІУСКЗ. Проаналізовані основні загрози і чинники, котрі впливають на стан захисту даних в КІУСКЗ, що дозволило підтвердити актуальність вибраного напрямку досліджень.

Зроблено аналіз вимог безпеки даних в КІУСКЗ в умовах зовнішніх впливів, обґрунтування критеріїв і показників оптимізації. Розроблено ієрархічну векторну систему показників якості функціонування КІУСКЗ.

Доведено, що одним з над важливих складових забезпечення ефективності функціонування КІУСКЗ є забезпечення безпеки даних. Одним з основних показників безпеки є час $T_б$ безпечного функціонування системи:

$$T_б = max\left\{T_{б_i}\right\}, \quad i = 1\ldots L\,,\; T_{б_i} = \frac{\aleph_i}{\psi \cdot \gamma_i}, \qquad (1)$$

де $T_{б_i}$ – безпечний час для виконання *i*- ої спроби; L – кількість спроб перебору; $\aleph_i$ – складність (кількість) операцій, необхідних для виконання *i*- ої спроби; ψ – продуктивність (кількість операцій за секунду) обчислювальної системи, що доступна зловмисникам; γ_i – коефіцієнт перерахунку за одиницю часу.

Визначено, що в теперішній час моделі систем розподілу доступу класифікуються по п'яти основних напрямах: моделі систем дискреційного розподілу доступу; моделі систем мандатного розподілу доступу; моделі ролевого розподілу доступу; суб’єктно-орієнтована модель ізольованого програмного середовища; моделі безпеки інформаційного потоку. Окрім цього, останнім часом з'явилися декілька перспективних напрямів математичного моделювання, заснованих на біоінформатиці, біоінженерії і ін.

Класифікація підходів і положень методології і математичного моделювання розподілу доступу та захисту КІУСКЗ наведена на рис. 1.

Рисунок 1 – Структурна схема класифікації і взаємозв'язку підходів та положень методології і математичного моделювання розподілу доступу та захисту КІУСКЗ

В результаті проведених досліджень виявлено ряд характерних особливостей, переваг та недоліків існуючих напрямів математичного моделювання КІУСКЗ. Визначено, що основним недоліком більшості звісних підходів математичного моделювання КІУСКЗ є складність, а іноді і неможливість, урахування чинника апріорної невизначеності в параметрах зовнішніх впливів на систему.

Виявлено, що засоби та протоколи захисту даних, які функціонують на сьогодні, не в змозі забезпечити достатньо жорсткі вимоги часу безпечного функціонування КІУСКЗ в умовах високоінтенсивних зовнішніх впливів. Це дало

можливість обґрунтувати та сформулювати окремі напрями та завдання дисертаційної роботи.

Другий розділ пов'язаний із розробкою методу оцінки захищеності КІУСКЗ, дослідження й оцінка функцій чутливості з урахуванням властивості нелінійності зовнішніх впливів і незалежності внутрішніх збурень.

В розділі проведена математична формалізація технології функціонування КІУСКЗ в умовах зовнішніх впливів. В процесі моделювання КІУСКЗ було наведено у вигляді системи:

$$\dot{x}(t) = A(t)x(t) + B(t)u(t) + E(t)\chi(t), \quad (2)$$

$$y(t) = C(t)x(t) + D(t)u(t) + E(t)\chi(t) + H(t)\zeta(t), \quad (3)$$

$$x(t_0) = x_0, \quad (4)$$

де $\dot{x}(t) \in \dot{X}$ – вимірюваний m-вимірний вектор координат стану системи, $x(t) \in X$ – m-вимірний вектор координат стану системи, $u(t) \in U$ – k-вимірний вектор управління, $A(t)$, $B(t)$, $E(t)$, $C(t)$, $D(t)$, $H(t)$ – безперервні матриці неспостережуваних похибок виміру; $\chi(t)$ – m-вимірний вектор неконтрольованих зовнішніх впливів, $\zeta(t)$ – вектор контрольованих зовнішніх впливів.

При цьому вплив зовнішніх (зловмисних) дій, а також змін, викликаних цими діями, можна досліджувати за допомогою функції чутливості:

$$\dot{\chi}_j = E(t)\chi_j, \quad (j = 1,\dots J), \quad (5)$$

де функція χ_j оцінюються як $\chi_j = \partial x / \partial p_{зовнj}$, а $p_{зовнj}$ – параметр чутливості системи до зовнішніх впливів.

Для оцінки впливу малих внутрішніх збурень на стан захищеності КІУСКЗ скористаємося основними положеннями теорії чутливості. Нехай матриці $A(t), B(t), E(t), C(t), D(t), H(t)$ залежать від деяких параметрів $p = (p_1, p_2, \dots, p_n)$. Якщо p постійний і дорівнює p_0, то система рівнянь (2, 3) має єдиний розв'язок $x(t)$ або $y(t)$ при будь-якому $u(t)$ і $\chi(t)$, визначений при $t \in [t_0, t_f)$. При незначних змінах параметра p_0 ($p_0 + \Delta p$) виникає мала варіація вектора стану $x(t)$ і вихідної координати $\delta y(t)$. Вплив таких змін можна досліджувати за допомогою функції чутливості:

$$\dot{U}_j = A(t)U_j + \partial f / \partial p_j, \quad (j = 1,\dots J), \quad (6)$$

де $f \equiv A(t)x(t) + B(t)u(t) + E(t)\chi(t) + H(t)\zeta(t)$ – функція, що характеризує чутливість КІУСКЗ до похибок моніторингу внутрішніх параметрів, а функція $U_j = \partial x / \partial p_j$ оцінюється аналогічно виразу (5).

За допомогою функції чутливості можливо описати нерівномірність відхилу випадкових траєкторій поведінки системи (2, 3) відносно вектора вихідних координат Y по всіх напрямах, а також вказати ділянки вектора Y, найбільш і найменш чутливі до змін вхідного сигналу і зовнішніх завад. Тоді:

$$\delta x(t_f) = \dot{\Phi}(\aleph_U(t_f)\delta p + \aleph_\chi(t_f)\delta p), \quad (7)$$

$$\delta y(t_f) = \dot{\Phi}_1\left[C(t_f)\left[\aleph_U(t_f)\delta p\right] + D(t_f)\left[\aleph_U(t_f)\right] + E(t_f)\left[\aleph_\chi(t_f)\right]\right], \quad (8)$$

де $\aleph_U$ і $\aleph_\chi$ – матриці чутливості; $\dot{\Phi}$ і $\dot{\Phi}_1$ – нелінійні вектор-функції.

На основі множини вимірюваних (апостеріорних) і апріорних даних про стан КІУСКЗ (I_{an} і I_a відповідно) проведений вибір показника оптимізації КІУСКЗ. Для цього припущено, що виходячи з існуючого рівня апріорної інформації I_a, стану і значень характеристик матриць чутливості $\aleph_U$ і $\aleph_\chi$ можуть проводитися виміри та аналіз даних $I_{an}(t)$, $\forall t \in J$, формуватися множина I_s кількісних узагальнених оцінок для елементів великої кількості I_{an} і множина I_ψ даних про вхідні збурення. Аналіз даних $I_{an}(t)$ множини I_{an} може проводитися як апріорі, так і в ході вирішення задачі ідентифікації. В результаті цього аналізу формуються множини I_{Ω_A} і I_{Ω_s} додаткової інформації про обмеження і характеристики об'єкта, причому $I_{\Omega_A} \subset I_{\Omega_s}$, а Ω_A – обмежена, але апріорі невідома область внутрішніх параметрів системи.

Вибраний показник рівня захищеності КІУСКЗ наводиться у вигляді функції:

$$T_б(I_{an}) = T(A \in R^{m\times m}, U \in \boldsymbol{U}, \chi \in \boldsymbol{\Psi}, t \in \boldsymbol{J} \mid A \in \Omega_A, U \in I_s, \chi \in I_\psi), \quad (9)$$

де $\boldsymbol{U}$, $\boldsymbol{\Psi}$ – сукупність просторів вхідних сигналів та зовнішніх збурень відповідно, а $\boldsymbol{J}$ – інтервал спостереження за об'єктом управління в КІУСКЗ.

Оптимізаційне завдання сформулюємо таким чином: необхідно знайти таке перетворення F множини I_{an} і додаткових даних I_{Ω_A}, I_{Ω_s} і I_ψ про КІУСКЗ, щоб при заданому рівні апріорної інформації I_a забезпечити максимізацію часу функціонування системи у безпечному режимі:

$$\forall t \in J, \; F : I_{an} \times I_a \to I_{an} \times I_s \Rightarrow \max_{I_s, I_\psi} T_б(I_{an}). \quad (10)$$

Таким чином, розв'язання оптимізаційної задачі (10) слід розглядати з системних позицій і одна з функцій системи має полягати в аналізі великої кількості I_{an} з метою синтезу методики оцінювання, що якнайповніше враховує реальні умови функціонування КІУСКЗ. Перетворення F розуміється в широкому сенсі і є кортежем операторів, сукупністю алгоритмів, способів і прийомів, що дозволяють реалізувати низку перетворень F.

Розглянуто систему(2–4) з урахуванням того, що в стаціонарному стані Y є інваріантним вектором вихідних координат системи y ($y \in Y$, $Y \subset R^{n\times n}$). Нехай вектор вихідних станів Y є експоненційно стійким (інваріантний вектор Y називається експоненційно стійким в середньому квадратичному для системи (2–4) в околі $\tilde{Y}$, якщо при деяких $K > 0, \ell > 0$ для всіх $t \geq 0$ виконується умова $E\left\|\Delta\left(y\left(t\right)\right)\right\|^2 \leq Ke^{-\ell t} E\left\|\Delta\left(y_0\right)\right\|^2$, де $y(t)$ – роз'вязок системи (2–4) з початковою умовою $y(0) = y_0 \in \tilde{Y}$. Для спрощення математичного опису системи (2–4) у процесі дослідження чутливості вектора Y до змін управляючого впливу U і зловмисним або іншим негативним збуренням скористаємося рівнянням (5).

У результаті дії неконтрольованих зовнішніх збурень ($\chi(t)|_{M\neq 0}$) випадкові траєкторії системи відхиляються від заздалегідь відомого положення, визначуваного вектором Y, і формують навколо нього деякий пучок (тор). На

практиці виникає завдання дослідження та математичного опису можливих станів системи і оцінки ступеня впливу функції чутливості на процес зміни стану.

Запропоновано, що для оцінки функції чутливості (5–6), а також знаходження асимптотики ряду стохастичних характеристик виходу з усталеного режиму (сформованої траєкторії) доцільно використовувати спеціально конструйовану функцію Ляпунова, яка називається квазіпотенціалом.

Асимптотика стаціонарної щільності розподілу випадкових траєкторій системи навколо вектора Y, для малих впливів має вигляд

$$\rho(y,a) \approx Ke^{\left(-\frac{\varpi(y)}{a^2}\right)}, \tag{11}$$

де a – параметр інтенсивності збурень, $\varpi(y) = -\lim\limits_{a\to 0} a^2 \ln \rho(y,a)$ – квазіпотенціал.

Квазіпотенціал $\varpi(y)$ пов'язаний із завданням мінімізації функціонала дії і задовольняє умові Гамільтона–Якобі

$$\frac{1}{2}\left(\partial\varpi/\partial y, Q(y)Q^T(y)\partial\varpi/\partial y\right) + \left(f(x), \partial\varpi/\partial y\right) = 0 \tag{12}$$

якщо $\varpi|_M = 0$, $\varpi|_{U/M} > 0$, де – $Q(y)$ – $n\times n$-матрична функція, що задає залежність збурень від стану захищеності системи.

Визначення 1. Функція $\varpi(y)$ називається Y-квадратичною, якщо при деяких $k_1 > 0, k_2 > 0$ для всіх $y \in \tilde{Y}$ виконується нерівність: $k_1\|\Delta(y)\|^2 \le \varpi(y) \le k_2\|\Delta(y)\|^2$, де $\|\bullet\|$ – евклідова норма.

Якщо функція $\varpi(y)$ є Y-квадратичною, то для експоненційної стійкості вектору Y системи (2-4) в околі $\tilde{Y}$ необхідно існування деякої Y-квадратичної функції $\omega(y)$, при якій:

$$L\varpi(y) = -\omega(y), \tag{13}$$

$$L\varpi(y) = \left(f(y), \partial\varpi/\partial y(y)\right) + \frac{1}{2}\sum_r^m \left(Q_r(y), \partial^2\varpi/\partial y^2(y) Q_r(y)\right). \tag{14}$$

Властивість захищеності системи від ряду зовнішніх зловмисних впливів може виходити з властивості експоненційної стійкості вектора Y системи (2–4) у разі, якщо окіл $\tilde{Y}$ вектора Y не перевищує допустимого розміру $\tilde{Y}_{доп}$. Враховуючи це, сформулювали наступну теорему.

Теорема 1. Якщо квазіпотенціал $\varpi(y)$ в околі $\tilde{Y}$ вектора Y є Y–квадратичною функцією Ляпунова і вектор Y є експоненційно-стійким, то за допомогою функції $\varpi(y)$ можна оцінити стан захищеності системи.

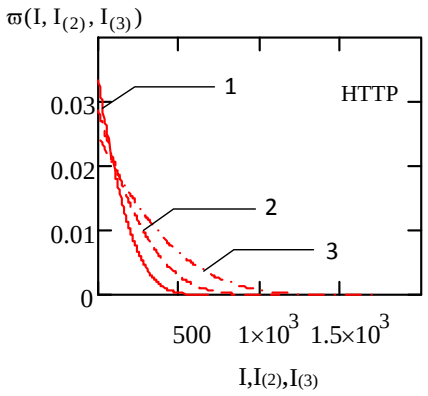
Доведення. Нехай функція $\varpi(y)$ є вирішенням рівняння Гамільтона–Якобі. Тоді відповідно до (14) квазіпотенціал задовольняє співвідношенню

$$\left(f(y), \partial\varpi/\partial y\right) = -\omega(y), \tag{15}$$

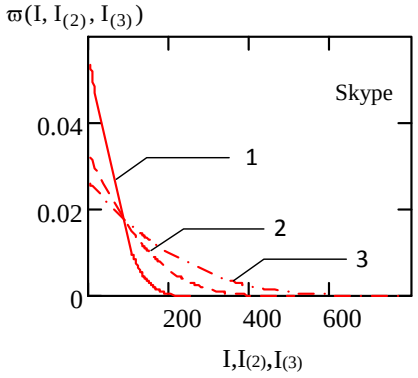
де $\omega(y) = 1\left(\partial\varpi/\partial y, Q(y)Q^T(y)\partial\varpi/\partial y\right)$.

Виходячи з властивостей рівняння Гамільтона–Якобі функція $\omega(y)$ як і $\varpi(y)$ є квадратичною, що доводить експоненційну стійкість вектора Y. Крім того, згідно з виразом (14) існує залежність розміру околу $\tilde{Y}$ від функції $\varpi(y)$.

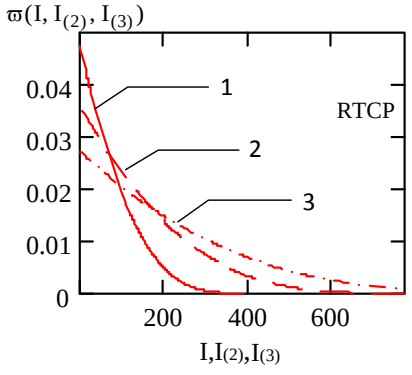
Наведені фактори доводять можливість функції $\varpi(y)$ визначати стан захищеності системи. Оцінимо ці можливості за допомогою графіків залежності квазіпотенціала від значень інтенсивності вхідного потоку даних ($\varpi(I, I_{(2)}, I_{(3)})$) (рис. 2) різних мережевих протоколів (*HTTP*, *Skype*, *RTCP*) в умовах зловмисних впливів (*Dos*-атаки) з декількох напрямів відповідно. Крива 1 графіків рис. 2 є ілюстрацією квазіпотенціала $\varpi(I)$, що характеризує функціонування захищеної системи (атака не досягає свого результату). Крива 2 графіків ілюструє поведінку функції $\varpi(I_{(2)})$, в умовах, коли зловмисні атаки на КІУСКЗ досягли свого результату з двох напрямків. Крива 3 графіків ілюструє ситуацію, коли *Dos-атаки* на КІУСКЗ відразу з трьох напрямів досягли свого результату.



а



б



в

Рисунок 2 – Графіки залежності $\varpi(I, I_{(2)}, I_{(3)})$

Як видно з рис. 2 у нормальному режимі функціонування квазіпотенціал $\varpi(I, I_{(2)}, I_{(3)})$ в області визначень $I \to 0$ має максимальні значення для всіх без винятку практичних випадків надходження інформаційного трафіку. У той же час аномальний вплив на КІУСКЗ *Dos*-атаки призводить до зниження значень квазіпотенціала в області $I, I_{(2)}, I_{(3)} \to 0$ до 1,4 раза при забезпеченні телекомунікаційних послуг по протоколу *HTTP*, до 2 разів при інформаційному обміні по протоколу *Skype*, і до 1,7 раза при використанні протоколу *RTCP*.

Відзначено, що квазіпотенціал $\varpi(I, I_{(2)}, I_{(3)})$ може оцінювати рівень захищеності КІУСКЗ не тільки в області $I, I_{(2)}, I_{(3)} \to 0$, а й на іншому інтервалі досліджуваної області інтенсивності вхідних даних. Так, при зниженні рівня захищеності КІУСКЗ функція $\varpi(I, I_{(2)}, I_{(3)})$ уповільнює спад своїх значень. Це в кінцевому підсумку призводить до того, що в незахищених КІУСКЗ

значення функції $\varpi\left(I, I_{(2)}, I_{(3)}\right)$ прямують до нуля при інтенсивностях $I_{(3)} > I_{(2)} > I$.

У табл. 1 наведені результати регресійного аналізу (рівняння лінійного тренду і величини достовірності апроксимації $\left\{R^2\right\}$) для граничного (гіршого з точки зору виявлення атак) випадку (діапазон досліджуваних значень інтенсивностей $I, I_{(2)}, I_{(3)}$ максимальний).

Таблиця 1 – Результати регресійного аналізу функції чутливості

	HTTP	*Skype*	*RTCP*
Атака не досягає результату	$-9\times10^{-5}x+0{,}026$ $R^2=0{,}8517$	$-3\times10^{-4}x+0{,}048$ $R^2=0{,}7319$	$-1{,}5\times10^{-4}x+0{,}036$ $R^2=0{,}8213$
Атака з двох напрямків	$-3\times10^{-5}x+0{,}018$ $R^2=0{,}7364$	$-8{,}5\times10^{-5}x+0{,}026$ $R^2=0{,}9971$	$-5\times10^{-5}x+0{,}023$ $R^2=0{,}7511$
Атака з трьох напрямків	$-2\times10^{-5}x+0{,}014$ $R^2=0{,}6564$	$-4\times10^{-5}x+0{,}019$ $R^2=0{,}6334$	$-3\times10^{-5}x+0{,}017$ $R^2=0{,}4369$

Результати моделювання свідчать, що для більшості практичних прикладів систем, в яких атака не досягає результату, кутовий коефіцієнт k рівняння лінійного тренду не перевищує значення -10^{-4} (за винятком прикладу *HTTP*-трафіку). У той же час, якщо атаки досягають свого результату, значення коефіцієнта k завжди вище -9×10^{-5}. Це свідчить, що значення кутового коефіцієнта k можна використовувати як еталонне при виявленні атаки і оцінці захищеності КІУСКЗ.

Таким чином, у результаті математичного моделювання на основі функції-квазіпотенціала сконструйована спеціальна функція оцінки захищеності КІУСКЗ.

Для порівняльного дослідження як еталон обрана система виявлення атак на основі описової статистики, котра використовується в системах *IDES, NIDES, EMERIAND* та ін. На рис. 3 наведені результати дослідження у вигляді графіків залежності імовірності $P_{\text{вияв}}$ виявлення комп'ютерної атаки від відношення інтенсивності зловмисної атаки $I_{\text{атаки}}$ до інтенсивності вхідного потоку $I_{\text{сд}}$ санкціонованих даних в умовах впливу *Dos*-атаки і *SYN*-атаки.

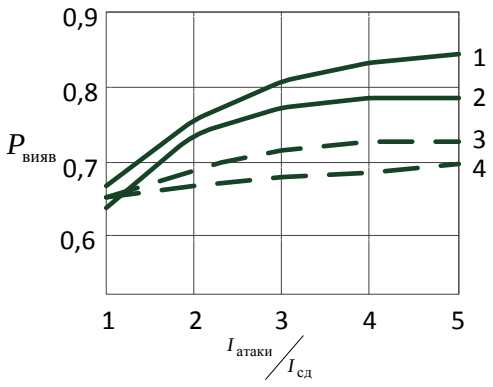


Рисунок 3 – Графікі залежності $P_{\text{вияв}}$ від $I_{атаки}/I_{сд}$

На рис. 3 крива 1 ілюструє залежність імовірності $P_{\text{вияв}}$ від відношення інтенсивностей $I_{атаки}/I_{сд}$ при використанні розробленого методу синтезу функції чутливості в умовах *Dos*-атаки, крива 2 – аналогічну залежність в умовах *SYN*-атаки, криві 3 і 4 характеризують систему виявлення комп'ютерних атак на основі описової

статистики в умовах *SYN* і *Dos*-атак відповідно. Результаті графіків свідчать, що використання синтезованої функції чутливості в умовах впливу *SYN*-атак до 1,1 раза, а в умовах *Dos*-атаки до 1,25 раза підвищує ймовірність виявлення комп'ютерної атаки (до 15% підвищує точність виявлення).

Проведено аналіз хибних виявлень комп'ютерних атак. На рис. 4. наведені результати дослідження у вигляді графіків залежності імовірності $P_{хвияв}$ хибного виявлення комп'ютерної атаки від відношення інтенсивності $I_{\text{атаки}}$ зловмисної атаки до інтенсивності $I_{\text{сд}}$ вхідного потоку санкціонованих даних в умовах впливу *Dos*-атаки і *SYN*-атаки. Криві графіків доводять, що в більшості практичних випадків $\left(I_{атаки}/I_{сд} \geq 2\right)$ імовірність $P_{хвияв}$ системою на основі сконструйованої функції чутливості порівнянна з імовірністю хибного виявлення атак системами, розробленими на основі описової статистики (*IDES, NIDES, EMERIAND* та ін.)

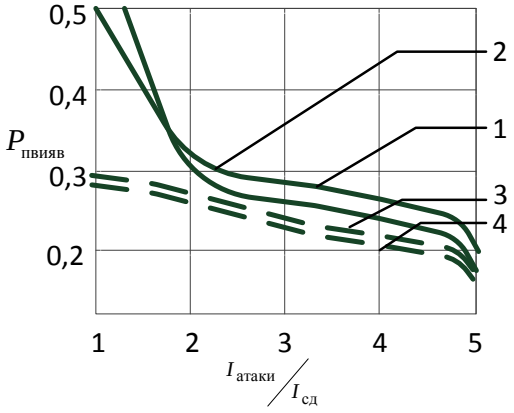


Рисунок 4 – Графікі залежності $P_{хвияв}$ від $I_{атаки}/I_{сд}$

Третій розділ присвячено розробці мережевого методу дослідження параметрів КІУСКЗ в умовах зовнішніх впливів.

Як показали результати проведених досліджень, математичне моделювання багаторівневої КІУСКЗ за допомогою багатошарової *GERT*-мережі може бути проведено при виконанні певних умов. Для забезпечення послуг безпеки використовується декілька засобів захисту даних в комплексі на різних рівнях *NGN*-архітектури; процес функціонування засобів захисту даних на кожному з рівнів *NGN*-архітектури може бути описаний за допомогою одношарової *GERT*-мережі; процес функціонування КІУСКЗ в цілому моделюється як послідовні переходи з одного стану в інший: $S_1^{(\ell)}, S_2^{(\ell)}, \ldots$, де $\ell = \{1,2,3\}$ – номер рівня *NGN*-архітектури; кожному з переходів ставиться у відповідність імовірність $p_k^{(\ell)}$, де k – номер переходу на одному з рівнів. Кінцева імовірність проходження послідовності станів на одному рівні у багатошаровій *GERT*-мережі визначається за правилом множення $P\left\{\left(S_{k_0}^{(\ell)},\ldots,S_{k_n}^{(\ell)}\right)\right\} = p_{k_0}^{(\ell)},\ldots,p_{k_n}^{(\ell)}$. Кінцева імовірність проходження послідовності станів між рівнів багатошарової *GERT*-мережі визначається аналогічно попередньому правилу $P\left\{\left(S_{k_0}^{(\ell_j)},\ldots,S_{k_n}^{(\ell_m)}\right)\right\} = p_{k_0}^{(\ell_j)},\ldots,p_{k_n}^{(\ell_m)}; \quad \forall(S_k^{(\ell_j)}, S_k^{(\ell_m)})$ і $(S_{k_j}^{(\ell)}, S_{k_m}^{(\ell)})$ ставляться у відповідність умовні імовірності $p_k^{(\ell_{j,m})}$ і $p_{k_{j,m}}^{(\ell)}$ відповідно.

Аналіз і проведені дослідження процесу функціонування КІУСКЗ дозволили визначити, що основними етапами математичного моделювання на основі багатошарової *GERT*-мережі є.

1. Визначення рівня деталізації (стратифікація) і структуризація математичної моделі КІУСКЗ.

2. Представлення КІУСКЗ у вигляді простору багатошарової *GERT*-структури $\overline{G} = (G, C)$, де $G = (\tilde{N}, \tilde{A})$ – підпростір рівнів моделювання, $C = (N, A)$ – підпростір стохастичних мереж $\tilde{N}, N$ – *GERT*-вузли (вершини), $\tilde{A}, A$ – гілки (дуги) *GERT*- мережі.

3. Визначення умовної імовірності і функції моментів кожної гілки.

4. Обчислення $\tilde{W}$ і W-функцій кожної гілки в підпросторах G і C відповідно.

5. Еквівалентні, спрощуючі перетворення багатошарової *GERT*-мережі.

6. Перехід від $\tilde{W}$ і W-функцій багатошарової *GERT*-мережі до характеристичних функцій $\chi(\zeta)$ і обчислення дійсних $\chi_{\mathrm{Re}}(\zeta)$ і уявних $\chi_{\mathrm{Im}}(\zeta)$ значень характеристичних функцій дуг у вузлах інтерполяції.

7. Опис процесу передачі від витоку до вихідного (внутрішнього) вузла багатошарової *GERT*-мережі на основі топологічного рівняння Мейсона.

8. Перетворення багатошарової *GERT*-мережі за формулою Мейсона у еквівалентну мережу, що складається з однієї еквівалентної гілки, котра характеризується W-функцією $W_E(s) = p_E M_E(s)$, де p_E – імовірність проходження стоку, $M_E(s)$ – еквівалентна функція моментів.

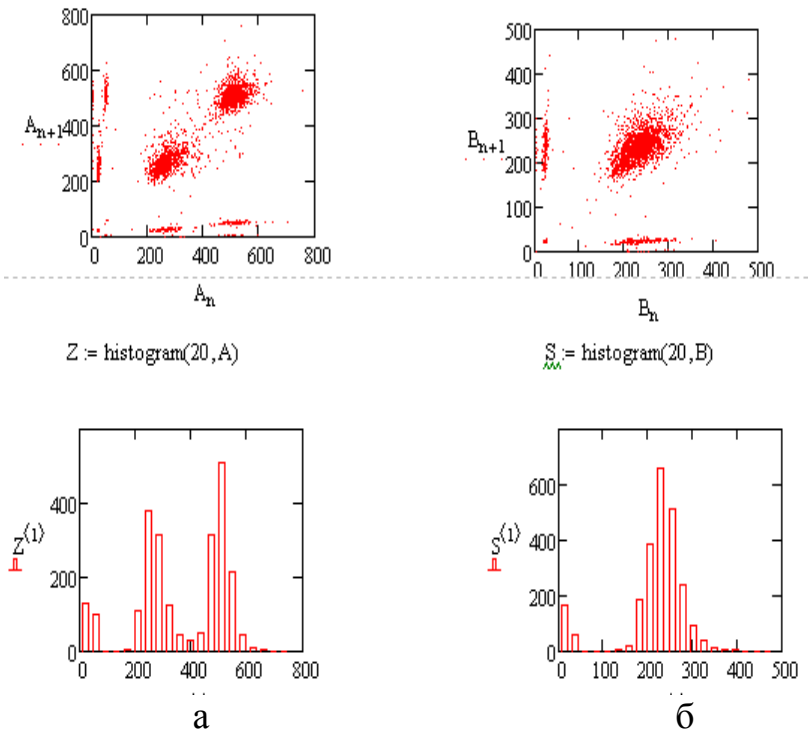
9. Обчислення дійсних $\tilde{X}_{\mathrm{Re}}(\zeta)$ і уявних $\tilde{X}_{\mathrm{Im}}(\zeta)$ значень еквівалентної характеристичної функції $\tilde{X}_E(\zeta) = X_E(\zeta) e^{-0,5\zeta^2}$ *GERT*-мережі у вузлах інтерполяції.

10. Визначення закону розподілу і щільності розподілу імовірності випадкової величини.

11. Знаходження математичного сподівання і дисперсії часу проходження *GERT*-мережі.

Таким чином, розроблений мережевий метод дослідження параметрів КІУСКЗ на основі багатошарової *GERT*-мережі, що враховує багаторівневість структурно-функціональної побудови КІУСКЗ. Це дозволило знайти і оцінити щільність розподілу імовірності випадкових характеристик зовнішніх впливів.

Четвертий розділ присвячено розробці методів ідентифікації стану і адаптивного управління безпекою в КІУСКЗ. Для оцінки статистичних властивостей інформаційного трафіку в умовах зовнішніх впливів і структурної ідентифікації стану за допомогою *BDS*-тестування здійснене імітаційне моделювання КІУСКЗ в умовах впливу на систему *DoS*-атаки. Результати ідентифікації стану трафіку (фазові портрети та гістограми розподілу), що поступає в КІУСКЗ, приведені на рис. 5. Як видно з графіків інтенсивності вхідного потоку даних аномального і нормального трафіків суттєво відрізняються.



а б

Рисунок 5 – Результати ідентифікації стану трафіку в КІУСКЗ в нормальних та аномальних (*DoS*-атака) умовах

У табл. 2 приведених значень *BDS*-статистики для різного інформаційного трафіку в умовах нормального функціонування і під час впливу *DoS*-атаки. Як видно з табл. 2. в умовах, коли зловмисні зовнішні впливи досягли своєї мети результати *BDS*-тестування знижуються практично до 37 разів і досягають рівня, прийняття рішення про повну відсутність статистичних залежностей у вхідній послідовності інформаційного трафіку.

Аналіз системи ідентифікації стану КІУСКЗ на основі *BDS*-тестування показав, що разом з перевагами існують деякі недоліки. В першу чергу це висока обчислювальна складність, що не дозволяє на практиці використовувати вибірки вхідних характеристик великих розмірів.

Усунути зазначений недолік пропонується шляхом використання, як статистичних даних аналізу стану системи, координат особливих точок спостережуваних структурно-інформаційних портретів (ССІП) – центрів квазіциклів. Розкладання двовимірного ССІП КІУСКЗ на квазіцикли базується на візуалізації графічного представлення фрагментів цього портрета. При цьому береться до уваги характер обертання ланок, що з'єднують сусідні точки (x_i, x_{i+1}), (x_{i+1}, x_{i+2}) фрагмента ССІП. Координати особливих точок використовуються як вхідні дані *BDS*-тесту. Результати *BDS*- тесту особливих точок квазіциклів представлені в табл. 3.

Таблиця 2 – Значення *BDS*-статистики для різного трафіку при N=500

Послуги	m=6		m=5		m=4	
	ε=0.5	ε=0.25	ε=0.5	ε=0.25	ε=0.5	ε=0.25
IP-телефонія	17.512	26.893	16.431	22.455	15.709	18.691
Торрент послуги	45.876	67.028	40.727	49.076	35.145	41.392
Потокове відео	52.329	117.954	38.824	83.730	30.032	54.371
DoS-атака	1.391	4.298	1.692	4.939	1.847	5.231

Таблиця 3 – Значення *BDS*-статистики особливих точок квазіциклів ССІП КІУСКЗ

	m=6		m=5		m=4	
	ε=0.5	ε=0.25	ε=0.5	ε=0.25	ε=0.5	ε=0.25
DoS-атака	0.981	2.122	0.993	1.997	1.003	3.192

Проведений аналіз результатів тестування показав, чітку тенденцію зниження значень *BDS*-статистики в умовах зовнішніх впливів і непротиріччя отриманих результатів оцінки статистичних особливостей траєкторії особливих точок з результатами *BDS*-тесту повної статистичної вибірки показників КІУСКЗ.

Таким чином вдосконалено метод структурної ідентифікації стану КІУСКЗ, що враховує статистичні залежності в змінах стану системи в умовах зовнішніх впливів і відрізняється від відомих використанням, як параметрів стану системи, координат особливих точок квазістатичних циклів ССІП.

Для адаптивного реагування на зовнішні впливи на КІУСКЗ розроблено комплекс методів адаптивного управління безпекою КІУСКЗ. Складовими комплексу є адаптивний метод виявлення зловмисних зовнішніх впливів на КІУСКЗ на основі нейронних мереж та метод синтезу нейронних мереж для виявлення шкідливого програмного забезпечення.

Результати використання адаптивного методу виявлення зловмисних зовнішніх впливів на КІУСКЗ на основі нейронних мереж в режимі розпізнавання класу атаки приведені в табл. 4.

Таблиця 4 – Результати тестування для комп'ютерних атак

Клас	Всього	Виявлено	Розпізнано
DoS	391458	391441 (99.99%)	370741 (94.71%)
MAC - flooding	52	48 (92.31%)	42 (80.77%)
R2L	1126	1113 (98.85%)	658 (58.44%)
Probe	4107	4094 (99.68%)	4081 (99.37%)
Нормальний стан			
normal	97277	---	50831 (52.25%)

Синтез нейронних мереж для виявлення шкідливого програмного забезпечення запропоновано проводити на основі нейромережевих імунних детекторів, що грають одну з найбільш важливих ролей у виявленні зловмисного програмного забезпечення. Пройшовши стадії навчання і відбору, детектори придбавають здатність реагувати на шкідливі програми, скануючи їх структуру і ігнорувати чисті файли.

Таким чином, розроблено комплекс методів адаптивного управління КІУСКЗ, які на відміну від відомих, використовують інтелектуальний підхід щодо виявлення порушень безпеки на множині параметрів КІУСКЗ. Це дозволить вирішувати завдання виявлення причин деструктивних змін стану системи і контролю параметрів відповідно до гарантованих вимог безпеки КІУСКЗ.

П’ятий розділ присвячено розробці та дослідженню моделі джерела перешкод та методу підвищення скритності даних в мобільному сегменті КІУСКЗ.

Дослідження показали, що для моделі джерела перешкод, досить задати один параметр – імовірність похибки на елемент p_0, котрий дозволяє розрахувати імовірність появи помилок кратності n в m-елементній біноміальній кодовій комбінації

$$P_m(n) = C_m^n p_0^n (1 - p_0)^{m-n}. \qquad (16)$$

При наявності інформації про $P_m(n)$ можна, наприклад, вибрати код, що забезпечує оптимальні показники достовірності або безпеки КІУСКЗ. Відомо, що імовірність похибки на елемент p_0 залежить від відношення сигнал/шум

$$h^2 = \frac{U^2 \tau_0}{2\upsilon^2}, \qquad (17)$$

де U – амплітуда сигналу; τ_0 – тривалість одиничного елементу; υ – спектральна щільність шуму.

Для систем з кодовим розділенням каналів інтерференції інформаційних пакетів вираз для розрахунку імовірності похибки на біт має вигляд:

$$Po = \frac{2}{3}\left(\left(\frac{N}{3N_ч} + \frac{2E_c}{N_0}\right)^{-0,5}\right) + \frac{1}{6}Q\left(\left(\frac{N}{3N_ч} + \sqrt{3}\sigma}{N_ч^2} + \frac{2E_c}{N_0}\right)^{-0,5}\right) + \frac{1}{6}Q\left(\left(\frac{N}{3N_ч} - \sqrt{3}\sigma}{N_ч^2} + \frac{2E_c}{N_0}\right)^{-0,5}\right)$$

де $Q = \frac{1}{2\sqrt{2\pi}}\int_0^{\infty} \frac{-U^2}{2} du$; $N_ч$ – кількість чіпів, використовуваних для кодування одного інформаційного біта; E_c – енергія сигналу; N – кількість станцій, що використовуються в процесі обміну даними; $\frac{N_0}{2}$ – двостороння спектральна щільність адитивного гаусового шуму $\sigma^2 = k\left(N_ч \frac{23}{360} + N_ч\left(\frac{1}{20} + \frac{k-1}{36}\right) - \frac{1}{20} - \frac{k-1}{36}\right)$; k – кількість пакетів, що інтерферують.

Отримані результати розрахунків складають основу моделювання джерела перешкод в мобільному сегменті КІУСКЗ.

При розробці методу підвищення скритності даних в мобільному сегменті КІУСКЗ в дисертаційній роботі усувається недолік регуляризації структури сигналу в фазовій площині.

Нехай передане повідомлення $r(t)$ $(t \in (0, T_y))$ на інтервалі часу T_y задається бінарною послідовністю $\{r_q\}_{q=1}^{Q}$ $Q = [T_y / T_r]$ елементів r_q, кожний тривалістю T_r, які можуть змінювати значення ($r_q = 0$ або $r_q = 1$) у моменти $q = \lfloor t / T_r \rfloor$. Як несучу, що маскує повідомлення, використано хаотичну послідовність, котра створить множину $X = \{x_m\}_{m=0}^{M-1}$ $(M = \lfloor T_y / T_x \rfloor)$ упорядкованих елементів x_m тривалістю T_x, де x_0 – її початкове значення.

На приймальній стороні спостерігається адитивна суміш $Y = \{y_m\}_{m=0}^{M-1}$ інформаційної послідовності заданої елементами множини $S = \{s_m\}_{m=0}^{M-1}$, отриманими з хаотичної послідовності з урахуванням повідомлення $\{r_q\}_{q=1}^{Q}$ і

білого гаусівського шуму (БГШ) $\Xi = \{\xi_m\}_{m=0}^{M-1}$ з нульовим математичним сподіванням і дисперсією σ_ξ^2. Необхідно за спостереженням $\{y_m\}_{m=0}^{M-1}$ відновити повідомлення $\{r_q\}_{q=1}^{Q}$.

Найбільш поширений випадок внесення інформації до хаотичної послідовності (несучої), тобто отримання послідовності $\{s_m\}_{m=0}^{M-1}$, заснований на зміні (маніпуляції) керуючого параметра нелінійної динамічної системи або початкового значення хаотичної послідовності. Наприклад, для системи, що генерує хаотичну послідовність з використанням ітерацій логістичного відображення $g(u,\lambda)$:

$$u_{n+1} = \lambda(r_q)u_n(1-u_n),\ u_n \in (0,1), \qquad (18)$$

де $q = [n/l]$, а $l = [T_r/T_x]$, таким параметром може бути $\lambda(r_q)$, котрий приймає одне з двох можливих значень λ_0 або λ_1, а також початкове значення $u_0(r_q)$.

Розглянемо метод внесення інформації в хаотичну послідовність, що дозволяє приховати факт її передачі. Цей метод (хаотичного перемішування) дозволяє отримати інформаційну послідовність задану впорядкованою множиною $S = \{s_m\}_{m=1}^{M-1}$ елементів s_m, у якої зруйнована характерна для хаотичної послідовності регулярність на фазовій площині.

В основі методу лежить виділення L дотичних підмножин (фрагментів) $X_q = \{x_m\}_{m=(q-1)l}^{lq-1}$ ($q = 1,...,L; L = [M/l]$) вихідної хаотичної послідовності заданої впорядкованою множиною $X = \bigcup_{q=1}^{L} X_q$ і маніпуляція порядком проходження їх елементів.

Для забезпечення необхідної якості відновлення елемента повідомлення кількість l може варіюватися. Оператори перестановки $\{Perm(\lambda_q(r_q),u_{q,0}(r_q),l)\}_{q=1}^{L}$ виконують взаємно однозначне відображення множин $X_q = \{x_p(x_0)\cdot\}_{p=(q-1)l}^{ql-1}$ з l елементів на себе $S_q = \{s_m\}_{m=(q-1)l}^{lq-1}$.

Множини X_q і S_q складаються з одних і тих же елементів, але відрізняються порядком їхнього слідування, який визначається значенням елементу бінарного повідомлення r_q і моментом q його передачі. В операторі перестановки $\{Perm(\lambda_q(r_q),u_{q,0}(r_q),l)\}_{q=1}^{L}$ змінні $\lambda_q(r_q)$ і $u_{q,0}(r_q)$ є відповідно управляючими параметрами і початковими значеннями, наприклад, логістичного відображення $u_{q,n+1} = f(\lambda_q(r_q),u_{q,0}(r_q),u_{q,n})$, формуючого допоміжну хаотичну послідовність $\{u_{q,n}\}$ для q-го фрагмента.

Елементи допоміжної хаотичної послідовності масштабуються: $\{lu_{q,n}\}$.

Ціла частина $b_{q,n} = \lfloor lu_{q,n} \rfloor$ $(n = 0,...,l-1)$ елементу цієї послідовності визначає новий порядковий номер відповідного (n-го) елемента q-го фрагмента вихідної послідовності. Індекси q,n пов'язані з дискретними моментами часу $t_{q,n} = T_r q + T_x n$, в кожен з яких формується новий відлік хаотичної послідовності, причому $t_{q,l} = T_r q + T_x l = t_{q+1,0}$.

Зміна інформаційних символів відбувається в тактові моменти часу $t_{q,0}$. Варіюючи обома параметрами $(\lambda_q(r_q), u_{q,0}(r_q))$ або одним з них можна отримати множину різних хаотичних (псевдохаотичних) послідовностей і операторів $\{Perm(\lambda_q(r_q), u_{q,0}(r_q), l)\}_{q=1}^{L}$. Очевидно, що оператори перестановки мають властивість лінійності.

В результаті застосування цих операторів до хаотичної послідовності отримуємо множину $S = \bigcup_{q=1}^{L} S_q$ елементів інформаційної послідовності, в якій

$$S_q = \{s_m(x_0, \lambda_q(r_q), u_{q,0}(r_q), l)\}_{m=(q-1)l}^{ql-1}. \qquad (19)$$

Задачу оцінки повідомлення розглянуто як завдання перевірки L гіпотез про вигляд оператора перемішування $Perm(\lambda_q(r_q), u_{q,0}(r_q), l)$, відповідного виділеному q-му фрагменту спостереження, у випадках наявності або відсутності на приймальній стороні апріорної інформації про початкові значення x_0 хаотичної послідовності, параметрах $(\lambda_q(r_q), u_{q,0}(r_q), l)$ операторів перемішування, моментах дискретного часу t_q зміни інформаційного символу, тобто тактової синхронізації.

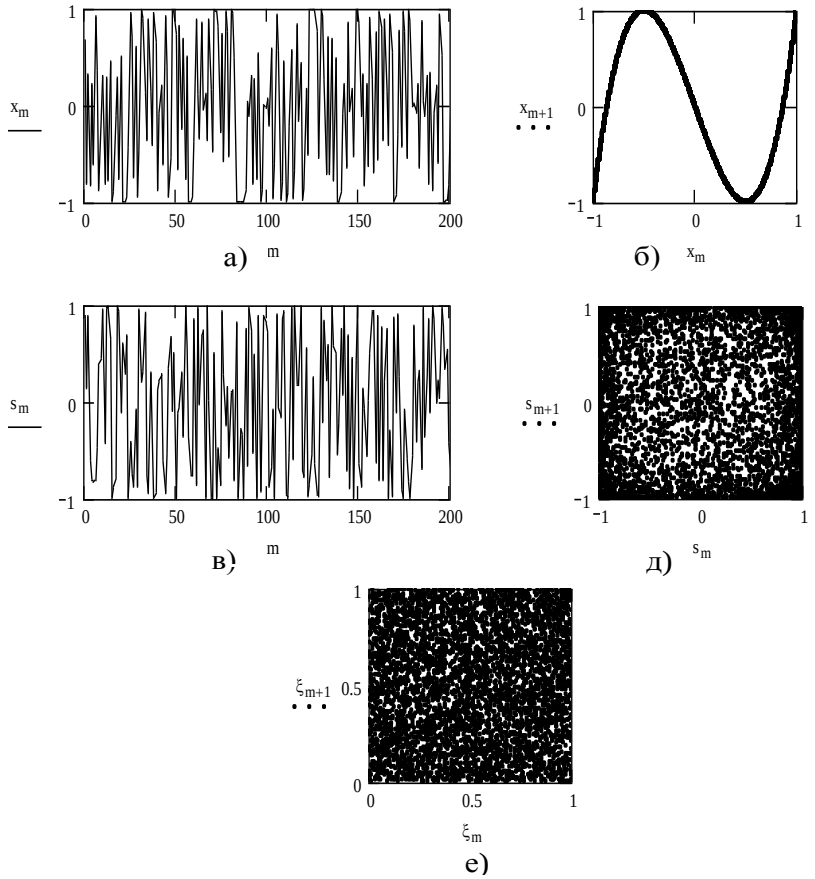


Рисунок 6 – Реалізація хаотичної послідовності до і після застосування оператора перемішування

Результати моделювання (рис. 6, *а* та 6, *в*) свідчать, що процедура перемішування не вносить помітних змін в поведінку реалізацій хаотичної послідовності і не впливає на їх

статистичні характеристики. У той же час, характерна для полінома Чебишева регулярність розподілення пар елементів послідовності на фазовій площині (рис. 6, *б*) руйнується (рис. 6, *д*). Для порівняння, на рис. 6, *е* проілюстровано поведінку на фазовій площині шуму з рівномірною щільністю імовірності на інтервалі (-1,1). Процедура перемішування «маскує» хаотичну послідовність під шум, що нехарактерно для інших відомих методів внесення інформації до хаотичної послідовності.

Для оцінки ефективності методу підвищення скритності використаний метод визначення структурної скритності сигналів, для якого не вимагається знання алгоритмів обробки в мобільній станції. При цьому методі визначається потенційна структурна скритність, що виражається кількістю двійкових вимірювань ($S, диз$), які необхідно здійснити для розкриття структури сигналу.

На рис. 7 зображено залежність структурної скритності $S, диз$ для сигналів *М*-послідовностей S_M; сегментів *М*-послідовностей S_{CM}; сигналів у вигляді випадкових двійкових послідовностей $S_{ВП}$; сигналів з псевдовипадковою перебудовою робочої частоти (ППРЧ) $S_{ППП}$ і відрізка хаотичного процесу як функції бази сигналу $S_{ХП}$.

Як видно з рис. 7, використання розробленого методу дозволяє до 2 разів підвищити скритність сигналу при передачі бінарних повідомлень в порівнянні з методом ППРЧ.

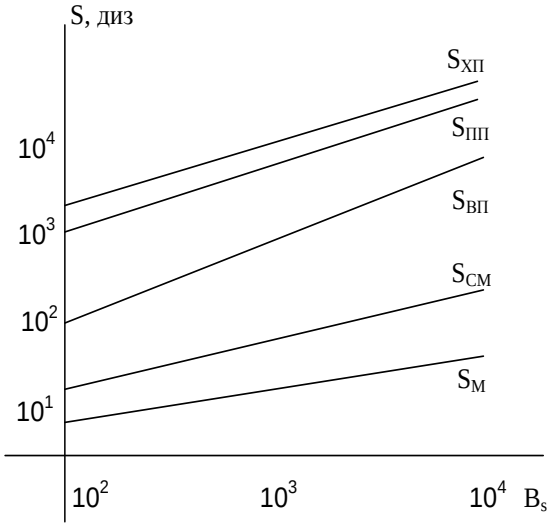


Рисунок 7 – Результати оцінки потенційної структурної скритності сигналів

Таким чином, розроблений у дисертаційній роботі підхід перемішування хаотичної послідовності призводить до нерегулярної поведінки траєкторії сигналу у фазовому просторі (площині), характерному для випадкових процесів, робить неефективним використання відомих методів якісного та кількісного аналізу нелінійних динамічних систем у фазовому просторі і, як наслідок, призводить до підвищення скритності сигналів при передачі бінарних повідомлень до 2 разів.

Шостий розділ присвячено розробці методу оптимального налаштування параметрів розподілу доступу в КІУСКЗ, оцінці ефективності розроблених методів та засобів розподілу доступу і захисту даних в КІУСКЗ, вибору найбільш раціонального варіанту налаштування параметрів цієї системи, і оцінці достовірності результатів дисертаційного дослідження.

Основною стратегічною метою налаштування параметрів системи розподілу доступу є максимізація часу функціонування комп'ютеризованої інформаційної системи у безпечному режимі $T_б$. Проведені дослідження показали, що цей

параметр багато в чому визначається часом реакції системи на зовнішні впливи, котра у свою чергу залежить від складності налаштування параметрів розподілу доступу в КІУСКЗ.

Саме тому виникає завдання мінімізації складності налаштувань розподілу доступу в КІУСКЗ: $minCl$, $T_б \geq T_{б_{доп}}, P_{хр} \leq P_{хр_{доп}}, P_{хі} \leq P_{хі_{доп}}$, де $T_{б_{доп}}$ – допустимий час функціонування КІУСКЗ у безпечному режимі; $P_{хр_{доп}}$ – допустима імовірність нав'язування КІУСКЗ хибних режимів роботи; $P_{хі_{доп}}$ – допустима імовірність введення в КІУСКЗ хибної інформації.

При вирішенні поставленого оптимізаційного завдання виникає необхідність вибору і урахування показників налаштування. У табл. 5 наведено зіставлення показників і відповідних способів настройки розподілу доступу.

Таблиця 5 – Відповідність показників і способів настройки розподілу доступу

Показник	**Спосіб настройки**
Складність реалізації облікових записів	Установка різноманітних політик, включаючи конфігурування локального входу в систему, резервного копіювання файлів і папок і т.і.
Складність модифікації облікових записів	Реконфігурація облікових записів безпосередньо до кожного об'єкту
Складність настройки локальних груп	Реалізація політики безпеки, з урахуванням поширення прав доступу по ієрархії об'єктів
Складність модифікації локальних груп	Реконфігурація привілеїв користувачів, призначення прав доступу до об'єктів групам користувачів
Складність реалізації мережної політики	Налаштування локальної політики безпеки і установка доступу до КІУСКЗ з мережі

Зобразимо кожен показник налаштування у вигляді цільової функції $f(z) = F$, областю означення $(z \in Z)$ якої є повноваження користувачів системи, а областю допустимих значень $(F \in C)$ – складність їхньої установки.

Тоді завдання багатокритеріальної оптимізації в загальному випадку має бути зображено в вигляді ансамблю екстремумів:

$$\begin{cases} min\{f_1(z) = F_1\}; \\ min\{f_2(z) = F_2\}; \\ \dots \\ min\{f_5(z) = F_5\}, \end{cases}$$

де $f_i(z)$ – цільова функція для i-го показника; F_i – значення цільової функції для i-го показника, $i \in [1,...,5]$.

Шляхом згортки обраних показників за допомогою виразу $\Phi(z) = \sum_i^5 a_i f_i(z),\ a_i \in C$ зобразимо узагальнений показник оптимізації налаштування параметрів розподілу доступу в КІУСКЗ.

Для визначення цільових функцій в дисертаційній роботі пропонується використовувати такі способи обчислень:

– складність реалізації облікових записів $f_1(z)=\frac{\sum_{j=1}^{m}K_j}{m}$, де m – кількість елементів КІУСКЗ; K_j – кількість користувачів, яким призначені дозволи на доступ до *j*-го об'єкту;

– складність модифікації облікових записів $f_2(z)=\frac{\sum_{j=1}^{m}G_j}{m}$, де G_J – кількість додаткових параметрів для зміни повноважень доступу до *j*-го об'єкту.

– складність налаштування локальних груп $f_3(z)=\frac{S\sum_{j=1}^{m}H_j}{m}$, де H_j – кількість прав і привілеїв, встановлених j-му об'єкту; S – кількість суб'єктів;

– складність модифікації локальних груп $f_4(z)=\frac{\sum_{j=1}^{S}A_j}{S}$, де A_j – кількість модифікацій, яку необхідно виконати при додаванні/видаленні в системі одного суб'єкта. Під сторонніми розуміються налаштування, котрі не потрібно виконувати безпосередньо при створенні/видаленні облікового запису суб'єкту, але які необхідні для повноцінної роботи нового суб'єкту або для нормальної роботи КІУСКЗ після видалення суб'єкту;

– складність реалізації мережної політики $f_5(z)=\frac{N_{net}}{S}$, де N_{net} – кількість мережевих налаштувань, значення яких визначені в КІУСКЗ.

При вирішенні завдання налаштування параметрів розподілу доступу в КІУСКЗ вибір рішення a_i здійснюється, виходячи з призначення системи, а також досвіду і практики її використання, на підставі таких даних, як частота оновлень і установки програмного забезпечення, кількість і інтенсивність можливих зовнішніх впливів, кількість користувачів, частота зміни їх повноважень. Способи вибору вагових коефіцієнтів a_i є різними. Одним з них є призначення a_i залежно від відносної важливості вибраних показників.

У табл. 6 наведено приклад розподілу вагових коефіцієнтів a_i в елементах КІУСКЗ за десятибальною шкалою.

Таблиця 6 – Приклад розподілу вагових коефіцієнтів для компонент КІУСКЗ

Призначення	Ваговий коефіцієнт *a*				
	П 1	*П 2*	*П 3*	*П 4*	*П 5*
FTP-сервер	3	3	10	9	9
Сервер СУБД *MS SQL*	1	10	2	9	10
Web-сервер	3	3	4	6	10
Робоча станція адміністратора	2	9	3	7	5
Робоча станція окремого користувача	7	8	6	4	5

Для підтвердження ефективності розробленого методу в порівнянні з методами, заснованим на принципах ролевого і мандатного доступу, наведені графіки (рис. 8) залежності часу функціонування системи у безпечному режимі

$T_б$ від відношення інтенсивності зловмисної атаки $I_{атаки}$ до інтенсивності вхідного потоку $I_{сд}$ санкціонованих даних (на прикладі *Dos*-атаки – ділянка 4, *MAC-flooding*- атаки – ділянка 3, *R2L*- атаки – ділянка 2 і *Probe*-атаки – ділянка 1).

На графіці рис. 8 наведено сімейство кривих залежності $T_б$ від $I_{атаки}/I_{сд}$ в умовах використання розроблених методів та засобів розподілу доступу і захисту даних (крива 1), методу мандатного розподілу доступу (крива 2) і методу ролевого розподілу доступу (крива 3).

Результати свідчать, що в цілому існує чітка тенденція зниження рівня часу функціонування системи у безпечному режимі при збільшенні інтенсивності атаки. Також рис. 8 ілюструє переваги розроблених методів та засобів розподілу доступу і захисту даних в КІУСКЗ в порівнянні з методами ролевого і мандатного доступу. Особливо це помітно при високій інтенсивності зловмисних атак. Так, використання розроблених методів та засобів дозволяє виконати вимоги гарантованого рівня безпеки в умовах, коли інтенсивність $I_{атаки}$ перевищує інтенсивність санкціонованих даних $I_{сд}$ до 5 разів, у той час, коли інші методи можуть забезпечити ці вимоги тільки при менших значеннях інтенсивностей зловмисних впливів. Таким чином відзначено, що використання розроблених методів та засобів дозволить підвищити рівень безпеки інформації до 1,1 разу при низькій інтенсивності зовнішніх впливів $\left(I_{атаки}/I_{сд} \le 1\right)$, і до 1,5 разів при високій $\left(I_{атаки}/I_{сд} > 1\right)$.

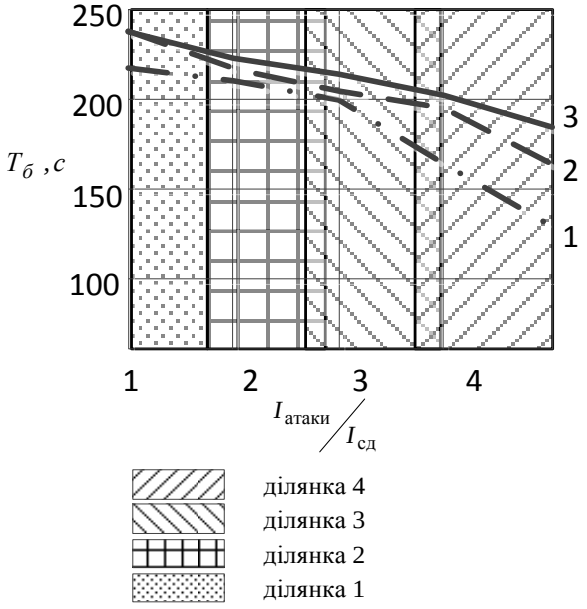


Рисунок 8 – Залежність $T_б$ від $I_{атаки}/I_{сд}$

У додатках наведено документи, що підтверджують практичне значення і впровадження результатів дисертаційної роботи, а також результати теоретичних, експериментальних досліджень та імітаційного моделювання.

ВИСНОВКИ

У дисертаційній роботі розв'язана науково-технічна проблема, яка полягає в розробці методів та засобів розподілу доступу і захисту даних в КІУСКЗ для забезпечення гарантованого рівня безпеки в умовах зовнішніх впливів.

До основних результатів роботи відносяться.

1. Аналіз вимог безпеки інформації, показників і критеріїв оптимізації, а також моделей, методів та засобів захисту даних в КІУСКЗ показав, що в умовах впровадження комп'ютерних технологій критичного застосування в ключові сфери життєдіяльності суспільства, збільшення інформації, а також підвищення небезпеки несанкціонованого доступу до неї з боку зловмисників,

використовувані на сьогодні методи розподілу ресурсів і захисту даних в КІУСКЗ не дозволяють забезпечити гарантований рівень безпеки в умовах зовнішніх деструктивних впливів на систему. Це дозволило визначити основні напрями дисертаційного дослідження і сформулювати оптимізаційне завдання максимізації часу функціонування системи у безпечному режимі.

2. Розроблений комплекс математичних моделей КІУСКЗ, на відміну від відомих, враховує вплив управляючого і зовнішніх деструктивних впливів, а також малих збурень і похибок виміру параметрів на вихідні характеристики системи, що дало можливість в порівнянні з відомими моделями підвищити точність моделювання до 10%.

3. Розроблений метод оцінки захищеності КІУСКЗ, що відрізняється від відомих урахуванням особливостей структурної і функціональної побудови системи, що дало можливість визначити рівень чутливості системи до деструктивних дій і оцінити міру впливу нелінійності зовнішніх дій і незалежності внутрішніх збурень на стан системи в трирівневому режимі функціонування. Використання цієї функції може до 15% підвищити точність виявлення зовнішніх впливів на КІУСКЗ.

4. Розроблений мережевий метод дослідження параметрів КІУСКЗ на основі багатошарової *GERT*-мережі, що враховує багаторівневість структурно-функціональної побудови КІУСКЗ. Це дозволяє знайти і оцінити щільність розподілу імовірності випадкових характеристик зовнішніх впливів на систему, а також основні параметри функціонування КІУСКЗ.

5. Проведено порівняно дослідження і розроблений метод структурної ідентифікації стану КІУСКЗ, що враховує статистичні залежності в змінах стану системи в умовах зовнішніх впливів, і відрізняється від відомих використанням як параметрів стану системи координат особливих точок квазістатичних циклів спостережуваних структурно-інформаційних портретів. Це дозволяє зменшити час структурної ідентифікації стану системи до 2 разів.

6. Розроблений комплекс методів адаптивного управління КІУСКЗ, які використовують інтелектуальний підхід до виявлення порушень безпеки на множині параметрів КІУСКЗ, що дозволяє вирішувати завдання виявлення причин деструктивних змін стану системи і контролю параметрів відповідно до гарантованих вимог безпеки КІУСКЗ.

7. Розроблений метод підвищення скритності сигналів при передачі бінарних повідомлень в мобільному сегменті КІУСКЗ, суттєво відрізняється від відомих використанням процедури перемішування хаотичної послідовності несучої, що призводить до нерегулярної поведінки траєкторії сигналу у фазовому просторі (площини), характерної для випадкових процесів, робить неефективним використання відомих методів якісного і кількісного аналізу нелінійних динамічних систем у фазовому просторі і, як наслідок, призводить до підвищення скритності сигналів при передачі бінарних повідомлень до 2 разів;

8. Розроблений метод оптимального налаштування параметрів розподілу доступу в КІУСКЗ, характеризується урахуванням основних показників адміністрування сучасних операційних систем, що дозволило мінімізувати складність налаштувань розподілу доступу в КІУСКЗ;

9. Проведена порівняльна оцінка ефективності застосування розроблених методів т засобів захисту даних в КІУСКЗ, яка показала їхню ефективність в умовах зовнішніх впливів. Зокрема: при впливі на систему *Dos*-атаки час функціонування КІУСКЗ у безпечному режимі збільшується до 1,5 раза; при впливі на систему *MAC-flooding*-атаки до 1,2 раза; при впливі на систему *R2L* і *Probe*-атаки до 1,1 раза.

В результаті проведеного дослідження впливу часу моніторингу КІУСКЗ на точність прогнозування стану безпеки виявлені часові діапазони розподілу доступу і захисту даних використання яких на практиці дозволить забезпечити гарантований рівень безпеки.

10. Результати дисертаційної роботи впроваджені у вигляді моделей, алгоритмів та програмних засобів для вирішення завдань управління безпекою КІУСКЗ та знайшли реалізацію при: розробці автоматизованих систем контролю і вимірів АСКВ "ТФ" і АСКВ "ТМА" НТ СКБ "Полісвіт" Державного науково-виробничого підприємства "Комунар"; удосконаленні засобів захисту комп'ютеризованої інформаційно-вимірювальної системи державного підприємства "Харківський науково-дослідний інститут технології машинобудування"; розробці систем захисту інформації Центру контролю космічного простору; юстуванні обладнання зв'язку загону оперативно-рятувальної служби; налаштуванні системи захисту інформації служби автоматики і зв'язку КП "Київпастранс"; розробці системи захисту комп'ютерної мережі товариства з обмеженою відповідальністю "Транс-Техно-Сервіс". Теоретичні аспекти та підходи математичного моделювання впроваджені у навчальний процес кафедри обчислювальної техніки та програмування Національного технічного університету «ХПІ» та кафедри програмного забезпечення Кіровоградського Національного технічного університету.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. *Семенов С.Г.* Модели и методы управления сетевыми ресурсами в информационно-телекоммуникационных системах / С.Г. Семенов, О.А. Смирнов, Є.В. Мелешко / [монография]. Харьков: НТУ «ХПИ». – 2012. – 212 с.

Здобувачем розроблені моделі і методи структурної ідентифікації інформаційно-телекомунікаційних систем.

2. *Семенов С.Г.* Методы и средства распределения доступа и защиты данных в компьютеризированных информационных управляющих системах критического применения / С.Г. Семенов / [монография]. Харьков: НТУ «ХПИ». – 2013. – 360 с.

3. *Семенов С.Г.* Метод знаходження оптимальної множини маршрутів у багатопролітній мережі системи зв’язку стандарту *3G* / С.Г. Семенов // Системи озброєння і військова техніка. – Харків:ХУ ПС. – 2007. – № 4 (12). – С. 98-101.

4. *Семенов С.Г.* Математическая модель процесса доставки информационных пакетов в компьютерной сети системы критического применения / С.Г. Семенов, И.В. Ильина // Радіоелектронні і комп’ютерні системи. – Харків.:НАКУ «ХАІ». – 2008. – Вип. 1(28). – С. 162-165.

Здобувачем здійснена постановка завдання математичного моделювання процеса доставки інформаційних пакетів.

5. *Семенов С.Г.* Распределение канальных ресурсов сетевого оборудования при информационном обмене в единой автоматизированной системе управления / С.Г. Семенов // Радіоелектронні і комп'ютерні системи. – Харків.:НАКУ «ХАІ». – 2008. – Вип. 6(33). – С. 307-310.

6. *Семенов С.Г.* Анализ методов прогнозирования в телекоммуникационных сетях автоматизированных систем управления / С.Г. Семенов // Системи управління, навігації та зв'язку. – К.:ЦНДІ навігації і управління. – 2008. – Вип. 2(6). – С. 134-137.

7. *Семенов С.Г.* Обгрунтування вимог до якості зв'язку при передачі інформації у комп'ютерних мережах систем критичного застосування / С.Г. Семенов, О.О. Можаєв, І.В. Ільїна // Системи озброєння і військова техніка. – Харків:ХУ ПС. – 2008. – Вип. 2(14). – С. 108-110.

Здобувачем проаналізовані вимоги щодо якості зв'язку при передачі інформації в комп'ютерних мережах систем критичного застосування.

8. *Семенов С.Г.* Дослідження особливостей та методів захисту інформаційних комп'ютерних мереж від СПАМу / С.Г. Семенов, Д.В. Гріньов, О.А. Малишев // Системи обробки інформації. – Харків: ХУ ПС. – 2008. – Вип. 7(74).– С. 115-117.

Здобувачем проаналізовані методи боротьби із СПАМом.

9. *Семенов С.Г.* Повышение скрытности хаотических сигналов при передаче бинарных сообщений / С.Г. Семенов, П.Ю. Костенко, С.М. Симоненко, К.С. Васюта // Известия высших учебных заведений «Радиоэлектроника». – К.: НТУУ «КПИ». – 2009.– Том 52, № 8. – С. 13-25.

Здобувачем розроблена модель зовнішніх дій на мобільний сегмент КСКЗ у вигляді хаотичних сигналів.

10. *Семенов С.Г.* Исследование потоковых свойств трафика, циркулирующего в компьютерных сетях систем критического применения для определения интервалов времени управления сетевыми ресурсами / С.Г. Семенов, В.Д. Дмитриенко, М.І. Науменко // Системи управління, навігації та зв'язку. – К.:ЦНДІ навігації і управління. – 2009. –Вип. 3(11).– С. 198-201.

Здобувачем проведено дослідження впливу часу моніторингу комп'ютерних систем критичного застосування (КСКЗ) на точність прогнозування стану безпеки.

11. *Семенов С.Г.* Аналіз та порівняльне дослідження засобів захисту інформації в телекомунікаційних мережах стандарту GSM / С.Г. Семенов, Р.В. Корольов, І.А. Ставицький // Системи обробки інформації. – Харків: ХУ ПС. – 2010. – Вип. 2(83). – С. 143-146.

Здобувачем проведені порівняльні дослідження засобів захисту інформації в мережах стандарту GSM.

12. *Семенов С.Г.* Сравнительные исследования методов идентификации трафика в телекоммуникационных сетях для повышения оперативности передачи данных / С.Г. Семенов, Є.В. Мелешко // Прикладна радіоелектроника. – Харків:ХНУРЕ. – 2010. Том 9, №3. – С. 444-448.

Здобувачем здійснена постановка завдання дослідження, вибір і оцінка показників оперативності передачі даних.

13. *Семенов С.Г.* Метод структурной идентификации информационных потоков в телекоммуникационных сетях на основе *BDS*-тестирования / С.Г. Семенов, О.О. Кузнецов, С.М. Симоненко, Є.В. Мелешко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУ ПС. – 2010.– Вип. 2(4). – С. 131-136

Здобувачем розроблений метод ідентифікації телекомунікаційного трафіку на основі BDS-тестування.

14. *Семенов С.Г.* Процедура идентификации информационного трафика на основе N-мерного шкалирования / С.Г. Семенов, И.В. Ильина, Е.В. Мелешко // Системи управління, навігації та зв'язку. – К.:ЦНДІ навігації і управління. – 2011. – Вип. 1(17). – С. 233-235.

Здобувачем здійснена постановка завдання дослідження і аналіз методів структурної ідентифікації систем.

15. *Семенов С.Г.* Структурно-функциональный анализ современных информационных систем с разработкой комплексного показателя эффективности их функционирования / С.Г. Семенов // Системи обробки інформації. – Харків: ХУ ПС. – 2011. – Вип. 2(92). – С. 145-150.

16. *Семенов С.Г.* Розробка і дослідження концептуальної моделі джерел помилок в сегменті мобільної мережі зв'язку / С.Г. Семенов, В.В. Босько, І.А. Березюк // Зб. наукових праць. Харківського університету Повітряних Сил. – Харків:ХУ ПС. – 2011. – Вип. 1(27). – С. 177-179

Здобувачем розроблена модель джерела перешкод в мобільному сегменті комп'ютерної системи критичного застосування.

17. *Семенов С.Г.* Сравнительный анализ и исследование систем обнаружения атак несанкционированного доступа / С.Г. Семенов, Р.В. Королев, С.О. Енгалычев // Системи обробки інформації. – Харків: ХУ ПС. – 2011. – Вип. 4(94). – С. 208-210.

Здобувачем проведено порівняльне дослідження систем виявлення атак несанкціонованого доступу.

18. *Семенов С.Г.* Розробка загальної структури ідентифікаційних вимірів з використанням окремих імовірнісно-часових характеристик сигналів / С.Г. Семенов, О.В. Петров, С.О. Єнгаличев // Системи озброєння і військова техніка. – Харків:ХУ ПС. – 2011. – Вип. 1(25). – С. 146-149.

Здобувачем розроблена узагальнена структура ідентифікаційних вимірів сигналів.

19. *Семенов С.Г.* Сучасний підхід щодо синтезу захищених інформаційно-телекомунікаційних систем інтегрованого типу / С.Г. Семенов, С.Б. Клімов, С.О. Єнгаличев // Системи управління, навігації та зв'язку. – К.:ЦНДІ навігації і управління. – 2011. – Вип. 2(18). – С. 265-268

Здобувачем проаналізовано методи синтезу захищених компьютерних систем та мереж.

20. *Семенов С.Г.* Безопасность операционных систем реального времени в автоматизированных системах управления технологическим процессом / С.Г. Семенов, С.Ю. Гавриленко, В.В. Давыдов // Авіаційно-космічна техніка і технологія. – Харків:НАКУ «ХАІ». – 2011. – Вип. 8(85). – С. 222-225.

Здобувачем здійснена постановка завдання аналізу безпеки операційних систем реального часу в автоматизованих системах управління технологічним процесом.

21. *Семенов С.Г.* Динамическая модель информационной системы на основе наблюдаемого структурно-информационного портрета / С.Г. Семенов, В.В. Давыдов // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків:НТУ «ХПІ». – 2011. –№36. – С. 156-163.

Здобувачем розроблена динамічна модель інформаційної системи на основі структурно-інформаційного портрета.

22. *Семенов С.Г.* Структурно-информационный портрет информационной системы в условиях неопределенности на примере *Dos*-атаки / С.Г. Семенов // «Радиотехника» – Харків:ХНУРЕ. – 2011. – №166. – С. 99-106.

23. *Семенов С.Г.* Оценка статистических свойств информационного трафика на основе метода нормированного размаха / С.Г. Семенов, Р.В. Корольов, О.В. Петров // Системи обробки інформації. – Харків: ХУПС. – 2011. – Вип. 8(98). – С. 237-240.

Здобувачем зроблена оцінка статистичних властивостей інформаційного трафіку на основі методу нормованого розмаху.

24. *Семенов С.Г.* Концепция защиты информации в *NGN*-сетях / С.Г. Семенов, В.В. Босько, І.А. Березюк, Є.В. Мелешко // Системи управління, навігації та зв'язку. – К.:ЦНДІ навігації і управління. – 2011. –Вип. 4(20). – С. 212-215.

Здобувачем проведений аналіз і розроблена концепція захисту інформації в NGN- мережах.

25. *Семенов С.Г.* Математическая модель мультисервисного канала связи на основе экспоненциальной *GERT*-сети / С.Г. Семенов, Є.В. Мелешко, Я.В. Ілюшко // Системи озброєння і військова техніка. – Харків:ХУ ПС. – 2011. –Вип. 3(27). – С. 64-67.

Здобувачем розроблена математична модель мультисервісного каналу зв'язку на основі експоненціальної GERT-мережі.

26. *Семенов С.Г.* Уязвимости операционной системы QNX в структуре автоматизированной системы управления технологическим процессом / С.Г. Семенов, В.В. Давыдов, Я.В. Ілюшко // Системи обробки інформації. – Харків: ХУ ПС. – 2012. – Вип. 2(100). – С. 215-218.

Здобувачем поставлено завдання оцінки уразливості операційної системи QNX в структурі АСУ технологічним процесом.

27. *Семенов С.Г.* Математична модель системи криптографічного захисту електронних повідомлень на основі *GERT*-мережі / С.Г. Семенов, О.О. Сур // Системи управління, навігації та зв'язку. – К.:ЦНДІ навігації і управління. – 2012. – Том 1. Вип. 1(21). – С. 131-137

Здобувачем розроблена математична модель системи криптографічного захисту електронних повідомлень на основі GERT-мережі.

28. *Семенов С.Г.* Исследования вероятностно-временных характеристик мультисервисного канала связи с использованием математического аппарата *GERT*-сети / С.Г. Семенов, В.В. Босько, І.А. Березюк // Системи обробки інформації. – Харків: ХУ ПС. – 2012. – Том 1. Вип. 3(101). – С. 139-142.

Здобувачем досліджено імовірнісно-часові характеристики мультисервісного каналу зв'язку з використанням математичного апарату GERT-мережі.

29. *Семенов С.Г.* Моделирование защищенного канала связи с использованием экспоненциальной *GERT*-сети / С.Г. Семенов, А.А. Можаев // Информатика, математическое моделирование, экономика. – Смоленськ.: Смоленский филиал АНО ВПО ЦС РФ "Российский университет кооперации". – 2012. – Том.1. – С. 152-160.

Здобувачем розроблена математична модель захищеного каналу зв'язку з використанням експоненціальної GERT-мережі.

30. *Семенов С.Г.* Біометрична аутентифікація на основі аналізу клавіатурного почерку / С.Г. Семенов, С.О. Енгаличев // «Прикладна радіоелектроника» – Харків:ХНУРЕ. – 2012. том 11, №2. – С.309-311.

Здобувачем проведено аналіз і поставлено завдання біометричної автентифікації користувачів комп'ютерних систем.

31. *Семенов С.Г.* Математическая модель распространения компьютерных вирусов в гетерогенных компьютерных сетях автоматизированных систем управления технологическим процессом / С.Г. Семенов, В.В. Давыдов // Вісник Національного технічного університету «ХПІ». – Харків:НТУ «ХПІ». – 2012. – №38. – С 163-171.

Здобувачем проведений аналіз математичних моделей поширення комп'ютерних вірусів в гетерогенних комп'ютерних мережах автоматизованих систем управління технологічним процесом.

32. *Семенов С.Г.* Методика математического моделирования защищенной ИТС на основе многослойной *GERT*-сети / С.Г. Семенов // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків:НТУ «ХПІ». – 2012. –№62 (968). – С 173-181.

33. *Семенов С.Г.* Усовершенствованный метод структурной идентификации компьютерных систем критического применения / С.Г. Семенов, Д.Ю. Задорожний, Т.С. Резниченко // Системи обробки інформації. – Харків:ХУ ПС. – 2012. – Вип. 9(107). – С. 207-211.

Здобувачем розроблено метод структурної ідентифікації компьютерних систем критичного застосування.

34. *Семенов С.Г.* Методика настройки параметров распределения доступа и защиты информации в компьютерных системах критического применения / С.Г. Семенов // Системи озброєння і військова техніка. – Харків:ХУ ПС. – 2012. – Вип. 4(32). – С. 153-158.

35. *Семенов С.Г.* Математическая модель технологии распространения злоумыленного программного обеспечения в компьютерных сетях / С.Г. Семенов, В.В. Давыдов // Східно-Европейський журнал передових технологій. – Харків, 2013. – Вип. 1/4(61). – С. 11-14.

Здобувачем поставлено завдання математичного моделювання процесу поширення програмних загроз з урахуванням топології комп'ютерних мереж.

36. *Семенов С.Г.* Модель специальной функции оценки защищенности информационно-телекоммуникационных систем / С.Г. Семенов, В.В. Босько, І.А. Березюк // Зб. наукових праць Харківського університету Повітряних Сил. – Харків:ХУ ПС. – 2013. – Вип. 1(34). – С. 126-130

Здобувачем розроблено метод синтезу функції чутливості.

37. *Семенов С.Г.* Разработка и исследования математической модели компьютеризированной информационно-измерительной управляющей системы критического применения с учетом фактора внешних воздействий / С.Г. Семенов, С.М. Порошин // Системи обробки інформації. – Харків: ХУ ПС. – 2013. – Вип. 2(110). – С. 208-210.

Здобувачем розроблено математична модель комп'ютеризованої інформаційно-вимірювальної управляючої системи критичного застосування з урахуванням фактору зовнішніх впливів.

38. *Семенов С.Г.* Комплекс методів адаптивного управління безпекою комп'ютеризованих інформаційно-вимірювальних управляючих систем критичного застосування / С.Г. Семенов, М.Й. Заполовський, О.І. Баленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУ ПС, 2013.– Вип. 1(10). – С. 167-173

Здобувачем розроблено метод адаптивного управління безпекою.

39. *Semenov S.* The Concept Definition of Mathematical Modelling of the Secured Information-Telecommunication System with Regard to Conditions of the Posterior Uncertainty / S.Semenov, O.Dorokhov, D.Grynov // Transport and Telecommunication Volume 14, No 2 – 2013 ISSN 1407-6160 ISSN 1407-6179 Riga – 2013 – P. 167-174.

Здобувачем розроблено математична модель інформаційно-телекомунікаційної системи и проведена оцінка достовірності результатів.

40. *Семенов С.Г.* Використання методу знаходження оптимальної множини маршрутів при управлінні інформаційними потоками у багатопролітній системі зв'язку стандарту *3G* / С.Г. Семенов, М.І. Гіневський, В.В.Косенко // Перспективи розвитку озброєння і військової техніки в Збройних Силах України: мат. наук.-техн. конф. – Л: ЛІСВ НУ «ЛПІ», 2008. – С. 217

Здобувачем запропоновано метод знаходження оптимальної множини маршрутів при управлінні інформаційними потоками у багатопролітній системі зв'язку стандарту 3G.

41. *Семенов С.Г.* Оптимальное распределение канальных ресурсов в статистическом мультиплексоре по критерию минимального сбалансированного времени доставки информационных пакетов / С.Г. Семенов // мат. IV наук.-техн. конф. ХУ ПС. – Харків: ХУ ПС – 2008 – С. 151.

42. *Семенов С.Г.* Использование статистического мультиплексирования для обеспечения качества обслуживания в телекоммуникационной сети системы критического применения / С.Г. Семенов, И.В. Ильина, С.Ф. Кривчач // Проблемы информатики и моделирования: мат. наук.-техн. конф. – Харьков: НАНУ, НТУ «ХПИ». – 2008. – С. 53.

Здобувачем поведено аналіз показників якості обслуговування.

43. *Семенов С.Г.* Использование процедуры перемешивания отсчетов хаотической несущей для повышения структурной скрытности систем передачи данных / С.Г. Семенов, С.М. Симоненко // Проблемы интеграции информации – 2008: исследования разработки, интеллектуальная собственность: мат. наук.-техн. конф. – Харьков: НТУ «ХПИ». – 2008. – С. 33.

Здобувачем запропоновано математична модель процесу зовнішнього впливу на основі теорії динамічного хаосу.

44. *Семенов С.Г.* Разработка предложений по обеспечению электромагнитной безопасности цифрових систем передачи информации / С.Г. Семенов // мат. V наук.-техн. конф. ХУ ПС. – Харків: ХУ ПС – 2009. – С. 110.

45. *Семенов С.Г.* Методика динамического управления сетевыми ресурсами телекоммуникационной сети / С.Г. Семенов // Перспективи розвитку озброєння і військової техніки Сухопутних військ: мат. наук.-техн. конф. – Л: ЛІСВ НУ «ЛПІ». – 2009. – С. 132.

46. *Семенов С.Г.* Исследование потоковых свойств трафика, циркулирующего в телекоммуникационных сетях / С.Г. Семенов, Ю.О. Семеренко // Проблеми інформатики і моделювання: мат. IX міжнародн. наук.-техн. конф. – Харків: НТУ «ХПІ». – 2009. – С. 53.

47. *Семенов С.Г.* Сравнительные исследования и анализ алгоритмов управления очередями в многопротокольных узлах связи телекоммуникационной сети / С.Г. Семенов, В.В. Босько, Є.В. Мелешко // Новітні технології – для захисту повітряного простору: мат. наук.-техн. конф. – Харків: ХУ ПС. – 2010. – С. 132.

Здобувачем проведено аналіз алгоритмів росподілу доступу до ресурсів компьютерної мережі.

48. *Семенов С.Г.* Визначення ймовірності втрат запитів у мережах передачі даних інфокомунікаційних систем / С.Г. Семенов, О.В. Петров, Ю.Г. Бусигін // Перспективи розвитку озброєння і військової техніки Сухопутних військ: мат. наук.-техн. конф.– Л: ЛІСВ НУ «ЛПІ». – 2010. – С. 145.

Здобувачем проведено аналіз показників безпеки в мережах передачі даних.

49. *Семенов С.Г.* Аналіз вимог до якості зв'язку у комп'ютерних мережах систем критичного застосування / С.Г. Семенов, І.В. Ільїна, С.О. Загайнов // Інформаційні технології в навігації і управлінні: стан та перспективи розвитку: мат. наук.-техн. конф. – К: ДП «ЦНДІ НіУ», 2010. – С. 29.

Здобувачем проведено аналіз вимог безпеки зв'язку у компьютерних мережах критичного застосування.

50. *Semenov S* The method of processing and identification of telecommunication traffic based on *BDS*-tests / S. Semenov, A. Smirnov, E. Meleshko // Materials International Conference «Statistical Methods of Signal and Data Processing (SMSDP-2010)». – Kiev, Ukraine, National Aviation University "NAU-Druk" Publishing House, October 2010. C.166-168. – engl.

Здобувачем розробленометод структурной ідентифікації телекомунікаційного трафіку на основі BDS-тестування.

51. *Семенов С.Г.* Порівняльний аналіз та дослідження систем захисту електронних повідомлень / С.Г. Семенов, О.О. Сур // Новітні технології – для захисту повітряного простору: мат. наук.-техн. конф. – Харків: ХУ ПС. – 2011. – С. 165-166

Здобувачем проведено дослідження систем захисту електронних повідомлень.

52. *Семенов С.Г.* Выбор критерия параметрической идентификации информационной системы / С.Г. Семенов, В.В. Босько, І.А. Березюк // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: мат. наук.-техн. конф. – Харків: НТУ «ХПІ». – 2011. – С. 76

Здобувачем досліджени крітерії параметричної ідентифікації інформаційно-вимірювальних систем.

53. *Семенов С.Г.* Ідентифікація статистичних даних в інформаційних системах і консолідація часових рядів / С.Г. Семенов, С.О. Єнгаличев // Інформаційні технології в навігації і управлінні: стан та перспективи розвитку: мат. наук.-техн. конф. – К.: ДП «ЦНДІ НіУ. – 2011. – С. 30-31

Здобувачем здійснена ідентифікація статистичних даних в інформаційних системах.

54. *Семенов С.Г.* Инерционная динамическая модель информационной системы на основе структурно-информационного портрета / С.Г. Семенов, В.В. Давыдов // Проблеми інформатики і моделювання: мат. наук.-техн. конф. – Харків: НТУ «ХПІ». – 2011. – С. 67.

Здобувачем розроблено інерційну динамічну модель інформаційної системи на основі структурно-інформаційного портрету.

55. *Семенов С.Г.* Анализ факторов, влияющих на состояние защиты *NGN*-сетей / С.Г. Семенов, В.В. Босько, І.А. Березюк // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засоби управління: мат. наук.-техн. конф. – К.:ДП «ЦНДІ НіУ», Х.: ДП «ХНДІ ТМ», К.: КДАВТ. – 2011.. – С. 72.

Здобувачем проаналізовано фактори, що впливають на безпеку NGN-мереж.

56. *Семенов С.Г.* Структурная идентификация защищенных информационно-телекоммуникационных систем в процессе их моделирования / С.Г. Семенов // Новітні технології – для захисту повітряного простору:мат. наук.-техн. конф. – Харків: ХУПС. – 2012. – С. 174.

57. *Semenov S* Mathematical Modelling of the Spreading of Software Threats in Computer Network / S. Semenov, V. Davidov, S. Engalishev // Proceedings of the XIth International Conference TCSET’2012 «Modern problems of radio engineering, telecommunications and computer science». – Lviv – Slavske, 2012. C.329/

Здобувачем розроблено математичну модель розповсюдження зловмисного програмного забезпечення.

58. *Семенов С.Г.* Система биометрической аутентификации пользователей на основе анализа клавиатурного почерка / С.Г. Семенов, С.О. Енгаличев // Безопасность информации в информационно-телекоммуникационных системах: мат. наук.-техн. конф. – К: ООО «ИП ЭДЕЛЬВЕЙС», НИЦ «ТЕЗИС» НТУУ «КПИ», 22-25.05 2012. – С.96-97

Здобувачем проаналізовано напрями біометричної автентифікації користувачів компьютеризованих управляючих систем.

59. *Семенов С.Г.* Исследования структурно-идентификационных портретов информационно-телекоммуникационных систем в условиях неопределенности / С.Г. Семенов, Д.Ю. Задорожный // Інформаційні проблеми теорії акустичних, радіоелектронних та телекомунікаційних систем IPST-2012: мат. наук.-техн. конф. – Системи обробки інформації. – Харків: ХУ ПС. – 2012. –Вип. 6(104). – С.168.

Здобувачем досліджені структурно-ідентифікаційні портрети інформаційно-телекомунікаційних систем в умовах невизначеності

60. *Семенов С.Г.* Методы адаптивного управления безопасностью информации в компьютерных системах критического применения / С.Г. Семенов,

И.В. Ильина, А.И. Баленко // Современные направления развития информационно-телекоммуникационных технологий и средств управления: мат. III междунар. наук.-техн. конф. – Полтава.:ПНТУ, Белгород.: НИУ «БГУ», Кировоград.: КЛА НАУ. – 2013. – С. 62.

Здобувачем розроблено метод адаптивного управління безпекою в комп'ютеризованих інформаційно-вимірювальних управляючих системах

АНОТАЦІЇ

Семенов С.Г. Методи та засоби розподілу доступу і захисту даних в комп'ютеризованих інформаційних управляючих системах критичного застосування. – На правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Національний технічний університет «Харківський політехнічний інститут», м. Харків, 2013.

Дисертаційна робота присвячена вирішенню актуальної науково-технічної проблеми розробки методів та засобів розподілу доступу і захисту даних в КІУСКЗ для забезпечення гарантованого рівня безпеки в умовах зовнішніх впливів.

Проведено аналіз науково-технічної проблеми розподілу доступу та захисту даних в КІУСКЗ.

Розроблено метод оцінки захищеності КІУСКЗ, що відрізняється від відомих урахуванням особливостей структурної і функціональної побудови системи.

Розроблено мережевий метод дослідження параметрів КІУСКЗ на основі багатошарової *GERT*-мережі, який на відміну від відомих враховує, багаторівневість структурно-функціональної побудови КІУСКЗ.

Вдосконалено метод структурної ідентифікації стану КІУСКЗ, що враховує статистичні залежності в змінах стану системи в умовах зовнішніх впливів і відрізняється від відомих використанням, як параметрів стану системи, координат особливих точок квазістатичних циклів спостережуваних структурно-інформаційних портретів. Вдосконалено комплекс методів адаптивного управління безпекою КІУСКЗ, який на відміну від відомих, використовує інтелектуальний підхід щодо виявлення порушень безпеки на множині параметрів КІУСКЗ.

Вдосконалено метод підвищення скритності сигналів при передачі бінарних повідомлень в мобільному сегменті КІУСКЗ, який враховує особливості приховання інформації в сигналі, що представляє хаотичну послідовність;

Вдосконалено метод оптимального налаштування параметрів розподілу доступу в КІУСКЗ, який відрізняється від відомих урахуванням основних показників адміністрування сучасних операційних систем;

Проведена порівняльна оцінка ефективності застосування розроблених методів та засобів розподілу доступу та захисту даних в КІУСКЗ.

Ключові слова: комп'ютеризована информаційна управляюча система критичного застосування, захист даних, розподіл доступу, структурна

ідентифікація стану, функція чутливості, *GERT*-мережі, *BDS*-статистика, спостережуваний структурно-інформаційний портрет.

Семенов С.Г. Методы и средства распределения доступа и защиты данных в компьютеризированных информационных управляющих системах критического применения. – на правах рукописи.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.05. – компьютерные системы и компоненты. – Национальный технический университет «Харьковский политехнический институт», г. Харьков, 2013.

Диссертационная работа посвящена решению актуальной научно-технической проблемы разработки методов и средств распределения доступа и защиты данных в компьютеризированных информационных управляющих системах критического применения (КИУСКП) для обеспечения гарантированного уровня безопасности в условиях внешних воздействий.

Активное внедрение компьютерных технологий критического применения в ключевые сферы жизнедеятельности общества является характерной чертой существования современного государства. Однако события последних лет свидетельствуют, что современные средства обеспечения безопасности в КИУСКП не могут обеспечить гарантированного уровня защиты данных. Связано это во многом с тем, что массовое распространение компьютерных сетевых технологий существенно расширило возможности злоумышленников в использовании методов и средств несанкционированного доступа к информации. В то же время уровень развития средств диагностирования и реагирования на деструктивные изменения режимов функционирования и внутренних характеристик КИУСКП остается прежним, а методы обеспечения безопасности данных часто не имеют надлежащей теоретической основы, что не гарантирует их успешной работы в условиях широкого спектра внешних воздействий на систему.

В диссертационной работе проведен анализ требований безопасности данных, показателей и критериев оптимизации, моделей и методов защиты данных в КИУСКП.

Разработан и исследован комплекс моделей КИУСКП, учитывающих влияние управляющего и внешних деструктивных воздействий, а также малых возмущений и ошибок измерения параметров на выходные характеристики системы.

Разработан метод оценки защищенности КИУСКП, отличающийся от известных учетом особенностей структурного и функционального построения системы, что дало возможность определить уровень чувствительности системы к деструктивным воздействиям и оценить степень влияния нелинейности внешних воздействий и независимости внутренних возмущений на состояние системы в трехуровневом режиме функционирования. Это позволило до 15% повысить точность выявления внешних воздействий на компьютерную систему.

Разработан сетевой метод исследования параметров КИУСКП на основе многослойной *GERT*-сети, в отличие от известных, учитывающий многоуровневость структурно-функционального построения КИУСКП, что

позволило найти функции и плотности распределения вероятностей случайных характеристик внешних воздействий на систему и оценить ее основные вероятностно-временные характеристики..

Усовершенствован метод структурной идентификации состояния КИУСКП, отличающийся от известных комплексным использованием наблюдаемого структурно-информационного портрета и *BDS*-теста и учитывающий статистические зависимости в изменениях состояния системы в условиях внешних воздействий, отличающийся от известных использованием в качестве параметров состояния системы координаты особых точек квазистатических циклов, что позволило уменьшить время структурной идентификации состояния системы до 2 раз.

Усовершенствован комплекс методов адаптивного управления КИУСКП, которые в отличие от известных, используют интеллектуальный подход к обнаружению нарушений безопасности на множестве параметров КИУСКП, что позволит решать задачи выявления причин деструктивных изменений состояния системы и контроля параметров в соответствии с гарантированными требованиями безопасности и функциональной целостности КИУСКП.

Разработан метод повышения скрытности сигналов при передаче бинарных сообщений в мобильном сегменте КИУСКП, учитывающий особенности скрытия информации в сигнале, представляющем хаотическую последовательность, что приводит к нерегулярному поведению траектории сигнала в фазовом пространстве (плоскости), характерному для случайных процессов, делает неэффективным использование известных методов качественного и количественного анализа нелинейных динамических систем в фазовом пространстве и, как следствие, приводит к повышению скрытности сигналов при передаче бинарных сообщений до 2 раз.

Разработан метод оптимальной настройки параметров распределения доступа в КИУСКП, отличающийся от известных учетом основных показателей администрирования современных операционных систем, что позволило минимизировать сложность настроек распределения доступа в КИУС критического применения.

Проведена сравнительная оценка эффективности применения разработанных методов и средств защиты данных в КИУСКП.

Ключевые слова: компьютеризированная информационная управляющая система критического применения, защита данных, распределение доступа, структурная идентификация состояния, функция чувствительности, *GERT*-сеть, *BDS*-статистика, наблюдаемый структурно-информационный портрет.

Semenov S. Methods and means of access and distribution of data protection in emergency computerized information control system. – Manuscript.

The thesis towards a degree of doctor of science (Dr. of Sc.) in specialty 05.13.05 – Computer Systems and Components. – National Technical University "Kharkiv Polytechnic Institute", Kharkov 2013.

The thesis isd devoted to solving important scientific and technical problem of development of methods and means for access distribution and data protection in

emergency computerized information control system (ECICS) to provide a guaranteed level of security in the context of external influences.

Active implementation of computer technology for critical applications to key areas of public life is characteristic feature of modern society. However, recent events witness that existed security means in ECICS can not provide a guaranteed level of data protection. This is due largely to the fact that the mass distribution of computer networking technology greatly increased the possibility of malicious users in the use of methods and means of unauthorized access to information. At the same time the level of diagnostics means and response to disruptive changes in modes of operation and the internal characteristics of ECICS remains the same, and methods of data security often do not have adequate theoretical background that does not guarantee their success in a wide range of external influences on the system .

This thesis analyzes the security requirements to the data, indices and criteria for optimization, models and methods of data protection in ECICS.

The complex of ECICS models is developed and investigated that takes into account the influence of manager biheviour and external destructive activities, as well as small disturbances and measurement errors on the output characteristics of the system.

Developed is the method for estimation of security level of ECICS, that differs from the known ones with considering the peculiarities of structural and functional layout of the system.

Developed is the network method for research of the ECICS parameters on the base of the multilayer GERT-network, allowing to take into account multilevel structural and functional layout of ECICS.

Improved is the method for the structural identification of the ECICS state, taking into account the statistical dependencies in the changes of the system under external influences.

Improved is the complex for adaptive control of the ECICS that uses an intelligent approach to the detection of security breaches on the set of the ECICS parameters.

Developed is the method of increasing secrecy in the transmission of binary signals in the mobile communications segment of the ECICS, taking into account the peculiarities of information hiding in the signal that is a chaotic sequence.

Developed is the method for optimal tuning parameters for the access distribution in the ECICS that differs from the well-known ones with considering the major indices of the administration in modern operating systems.

A comparative evaluation of the effectiveness of the developed models and methods of data protection in ECICS is implemented.

Keywords: emergency computerized information control system, data protection, access distribution, structural identification of a state, sensitivity function, GERT-network, BDS-statistics, the observed structural and informational portrait.

Підписано до друку 01.10.2013 р. Формат 60×84 $^{1}/_{16}$. Папір офсетний.
Гарнітура Times New Roman. Друк ризографічний. Ум. друк. арк. 2,09.
Тираж 100 пр. Зам. № 2/20–2013

Видавець і виготівник
Харківський університет Повітряних Сил
імені Івана Кожедуба
61023, Харків-23, вул. Сумська, 77/79.
Свідоцтво суб'єкта видавничої справи
ДК № 2535 від 22.06.2006.