НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

АЛЕКСАНДЕР Марек Богуслав

УДК 004.056.53:004.492.3

МЕТОДИ ТА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

Спеціальність 05.13.21 – «Системи захисту інформації»

Автореферат

дисертації на здобуття наукового ступеня

доктора технічних наук

Київ – 2016

Дисертацією є рукопис.

Робота виконана на кафедрі безпеки інформаційних технологій Національного авіаційного університету Міністерства освіти і науки України.

Наукові консультанти: доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки **Корченко Олександр Григорович**, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету (м. Київ, Україна);

доктор технічних наук, професор **Карпінський Микола Петрович**, завідувач кафедри інформатики та автоматики Університету у Бєльсько-Бялій (м. Бєльсько-Бяла, Польща).

Офіційні опоненти: доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки **Васіліу Євген Вікторович,** директор Навчально-наукового інституту радіо, телебачення та інформаційної безпеки Одеської національної академії зв'язку ім. О.С. Попова (м. Одеса, Україна);

доктор технічних наук, професор **Лужецький Володимир Андрійович**, завідувач кафедри захисту інформації Вінницького національного технічного університету (м. Вінниця, Україна);

доктор технічних наук, професор **Хома Володимир Васильович,** професор кафедри систем керування та систем прийняття рішень Інституту автоматики та інформатики Опольської Політехніки (м. Ополе, Польща).

Захист відбудеться «30» серпня 2016 р. о $13^{\underline{00}}$ годині на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03680, Київ, пр. Космонавта Комарова, 1, корпус 11, аудиторія 111.

З дисертацією можна ознайомитись в науково-технічній бібліотеці Національного авіаційного університету за адресою: 03680, Київ, пр. Космонавта Комарова, 1.

Автореферат розісланий «28» липня 2016 р.

Учений секретар
спеціалізованої вченої ради
к.т.н., доцент С.О. Гнатюк

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Інтернет речей (Internet of Things, IoT) допомагає мільярдам людей об'єднати об'єкти (речі), які потрібно використовувати у повсякденному житті. Тисячі розумних підключених пристроїв відкривають нові можливості для людей в усьому світі та значно знижують витрати. Однією з базових технологій побудови IoT є використання безпроводових сенсорних мереж (БСМ), які почали застосовуватися ще в кінці минулого сторіччя і довели свою ефективність для розв'язання таких завдань як виявлення можливих відмов різноманітних механізмів за рахунок контролю базових параметрів, віддалений контроль доступу до систем об'єкта моніторингу в режимі реального часу, забезпечення енерго- та ресурсозберігаючих технологій, контроль екологічних параметрів навколишнього середовища, моніторинг стану пацієнтів в телемедичних системах тощо. Мережі БСМ мають низку переваг – це, зокрема, можливість розміщення у складно доступних місцях (зокрема у місцях, в яких складно чи дуже дорого використовувати мережі іншого типу), надійність мережі в цілому (у випадку виходу з ладу одного з елементів інформація передаватиметься через сусідні), оперативність та зручність розгортання й обслуговування, можливість корегування кількості елементів у мережі (додавання або віднімання будь-якої кількості елементів), відносно тривалий час роботи без заміни елементів живлення, а також високий рівень проникнення через перешкоди й стійкість до електромагнітних завад та ін.

Серед основних недоліків БСМ можна, перш за все, виділити недостатню їх захищеність (зокрема критичним є безпека комунікацій, пристроїв, систем управління пристроями, побудова нових моделей довіри), що все більш чітко проявляється зі зростанням підключених у БСМ пристроїв.

Дослідженню БСМ, зокрема підвищенню їх ефективності та захищеності, приділили увагу у своїх працях такі вітчизняні і закордонні вчені: К. Аккая, П. Агварал, Т. Альхмєдат, Л. Бароллі, А. Букерче, В. Ванг, М. Віноградов, Д. Естрін, М. Карпінський, О. Кільменінов, Р. Колодій, О. Корченко, Д. Куллер, Х. Муфта, Р. Одарченко, Д. Рагозін, С. Райба, С. Толюпа, Р. Шорей, Л. Шу та ін.

Переважна більшість відомих робіт присвячено розробці ефективних протоколів та архітектур БСМ, методів оптимізації їх структури та експлуатації, а також нових підходів і галузей застосування з урахуванням їх специфіки. Проте широке використання БСМ саме у концепції IoT зумовлює особливу актуальність створення нових методів та моделей безпечної їх комунікації, зокрема забезпечення захисту від визначених кіберзагроз їх базовим характеристикам безпеки (конфіденційності, цілісності та доступності). Таким чином, ціла низка завдань та проблем, вирішення яких має важливе наукове та практичне значення, залишаються невирішеними. З цих позицій, розробка та дослідження методів і моделей захисту БСМ та їх компонентів від різного роду кіберзагроз, спрямованих на порушення базових характеристик безпеки, *є актуальною науково-технічною проблемою,* що має теоретичне і практичне значення.

Зв'язок роботи з науковими програмами, планами, темами. Тематика дисертаційної роботи та одержані результати безпосередньо пов'язані з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014-2018 роки», Стратегією національної безпеки України від 26 травня 2015 року № 287/2015, Стратегією кібербезпеки України від 15 березня 2016 року №96/2016.

Результати роботи відображені у звітах держбюджетних науково-дослідних робіт Національного авіаційного університету «Організація систем захисту інформації від

кібератак» (д.р. № 0111U000171), «Новітні технології криптографічного захисту інформації» (реєстраційний номер № 100/14.01.06) та Кіровоградського національного технічного університету «Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах» (д.р. № 0115U003103), у яких здобувач брав участь у якості виконавця.

Мета і задачі дослідження. Метою дисертаційної роботи є забезпечення захисту безпроводових сенсорних мереж від кіберзагроз, що впливають на їх базові характеристики інформаційної безпеки.

Для досягнення поставленої мети необхідно розв'язати такі **основні задачі:**

1. Провести аналіз БСМ в концепції IoT щодо особливостей їх архітектури, протоколів та систем забезпечення захисту інформації.

2. Розробити математичні моделі інформаційних структур ймовірності загроз визначеного класу DoS-атак для оцінювання рівня впливу показників кіберзагроз щодо БСМ.

3. Розробити модель захищеної комунікації «клієнт-сервер-шлюз-вузол» для ідентифікації класу реалізованої кібератаки на БСМ та визначення відповідних контрзаходів.

4. Розробити метод відновлення повідомлення для забезпечення їх цілісності в умовах реалізації відповідних кіберзагроз БСМ.

5. Удосконалити метод ймовірнісного маркування пакетів у БСМ для здійснення їх моніторингу та відстежування джерела атак.

6. Розробити структурно-аналітичні моделі забезпечення доступності інформаційно-управляючих систем (ІУС) БСМ для здійснення вибору ефективної стратегії обслуговування гарантоздатної ІУС за показниками готовності технічного та інформаційного станів відносно сформованої множини дефектів.

7. Удосконалити технології обчислень на еліптичних кривих для збільшення швидкості криптографічної обробки даних у пристроях ІУС БСМ.

8. Розробити структурно-аналітичні моделі обчислювачів на еліптичних кривих у пристроях ІУС для досягнення мінімальних розмірів еліптичних кривих, що можуть бути застосовані для забезпечення необхідного рівня безпеки ІУС БСМ.

9. Розробити структурно-аналітичні моделі обчислення дискретного логарифму для кривих над полем $GF(2^m)$ для побудови високопродуктивних криптографічних пристроїв на еліптичних кривих і пришвидшення виявлення криптоаналітичних атак на ІУС БСМ.

Об'єктом дослідження є процес захисту безпроводових сенсорних мереж та їх окремих компонентів від кіберзагроз.

Предметом дослідження є методи та моделі забезпечення захисту безпроводових сенсорних мереж від визначених кіберзагроз, що впливають на їх базові характеристики інформаційної безпеки.

Методи дослідження базуються на теорії ймовірності та математичної статистики (розробка математичних моделей інформаційних структур ймовірності кіберзагроз та моделі захищеної комунікації «клієнт-сервер-шлюз-вузол»), а також на основі мережевих методів захисту інформації (розробка методу ймовірнісного маркування пакетів у БСМ, структурно-аналітичних моделей забезпечення живучості ІУС БСМ), інформаційної безпеки (розробка методу відновлення повідомлення), математичного моделювання (розробка моделі захищеної комунікації «клієнт-сервер-шлюз-вузол»), теорії алгебри та теорії криптографії (розробка технології обчислень на еліптичних кривих, структурно-аналітичних моделей обчислювачів на еліптичних кривих у пристроях ІУС БСМ, структурно-аналітичних моделей обчислення дискретного логарифму для кривих над полем $GF(2^m)$).

Наукова новизна одержаних результатів полягає у такому:

1. Вперше запропоновані нові математичні моделі інформаційних структур ймовірності загроз визначеного класу DoS-атак, які за рахунок сформованої базової множини характерних показників і відповідних вагових коефіцієнтів та взаємозв'язків визначених матриць активності мережі і встановленої інтенсивності впливу різних класів атак, дозволяють визначити рівень впливу показників кіберзагроз щодо безпроводових сенсорних мереж.

2. Отримала подальший розвиток модель захищеної комунікації «клієнт-сервер-шлюз-вузол», яка за рахунок сформованої базової множини залежностей можливих шляхів «точка доступу → точка призначення» із врахуванням впливу величин ймовірностей компрометації вузлів і вирахуваних вагових коефіцієнтів, дає можливість ідентифікувати клас реалізованої атаки на безпроводові сенсорні мережі та визначити відповідні заходи протидії.

3. Отримав подальший розвиток метод відновлення повідомлення, який за рахунок процедури підстановочного сортування *b*-бітних блоків лексикографічними значеннями, інтерпретації значення відповідно до формату зберігання блоків в IP-заголовку, *i*-індексним впорядкуванням контрольних сум та двохфазової відновлювальної схеми, дає можливість забезпечити цілісність повідомлень в умовах реалізації відповідних кіберзагроз безпроводовим сенсорним мережам.

4. Удосконалено метод ймовірнісного маркування пакетів у безпроводовій сенсорній мережі, який за рахунок доповнення пакетів вектором ідентифікації номерів вузлів (записаних в його координатах), правила формування ймовірності успішного міжвузлового переходу, процедури обмеження вибірки пакетів за мінімаксним критерієм та запропонованого методу відновлення повідомлення, дозволяє здійснювати моніторинг безпроводових сенсорних мереж та відстежувати джерела кібератак.

5. Отримали подальший розвиток структурно-аналітичні моделі забезпечення живучості інформаційно-управляючих систем безпроводових сенсорних мереж, які за рахунок побудованого направленого графу інформаційно-технічних станів $MS_{ПС}$, $MS_{ЧП}$, $MS_{НБС}$ і $MS_{НС}$ з комбінацією кодованих показників дефектів зовнішніх впливів за ознаками ймовірності та детермінованості, дають можливість здійснювати вибір ефективної стратегії обслуговування гарантоздатної інформаційно-управляючої системи за показниками готовності технічного та інформаційного станів відносно сформованої множини дефектів, що впливають на базову характеристику безпеки – доступність.

6. Удосконалено технології обчислень на еліптичних кривих, які за рахунок запропонованого способу заміни операцій множення за модулем в алгоритмі Крестенсона еквівалентним перетворенням на основі операції додавання з відображенням на відповідну обчислювальну архітектуру, дозволяє збільшити швидкість криптографічної обробки даних у пристроях інформаційно-управляючих систем безпроводових сенсорних мереж.

7. Отримали подальший розвиток структурно-аналітичні моделі обчислювачів на еліптичних кривих у пристроях інформаційно-управляючих систем, які за рахунок запропонованих структурно-аналітичних моделей забезпечення живучості та реалізації паралельних обчислень на основі теоретико-числових базисів Радемахера-Крестенсона в розроблених обчислювальних архітектурах, дозволяють досягти мінімальних розмірів еліптичних кривих, що можуть бути застосовані для забезпечення необхідного рівня доступності та безпеки інформаційно-управляючих систем безпроводових сенсорних мереж.

8. Отримали подальший розвиток структурно-аналітичні моделі обчислення дискретного логарифму для кривих над полем $GF(2^m)$, які за рахунок використання розроблених моделей обчислювачів на еліптичних кривих і з урахуванням теоретико-числових базисів Радемахера-Крестенсона для паралельного сумування чисел великої розрядності та паралельної реалізації операцій на підставі ро-методу Полларда, дають можливість будувати високопродуктивні криптографічні пристрої на еліптичних кривих і пришвидшити виявлення криптоаналітичних атак, що впливають на конфіденційність інформаційно-управляючих систем безпроводових сенсорних мереж.

Практичне значення одержаних результатів. Отримані в дисертаційній роботі результати можуть бути використані для створення інструментальних засобів у вигляді програмних або програмно-апаратних модулів для забезпечення захищеності БСМ та їх компонентів. *Практична цінність полягає у такому:*

– створено апаратно-програмну систему для ІУС, що працює на програмованих матрицях FPGA та ПК, дія якої ґрунтується на основі модифікованої моделі обчислень, причому на підставі досліджень побудованого суматора точок на програмованих матрицях FPGA Stratix III EP3SL150F1152I4SL одержано збільшення швидкості шифрування методом Ель-Гамаля приблизно втричі в порівнянні з традиційним підходом сумування точок;

– створено апаратно-програмну систему для ІУС, що реалізує ро-алгоритм Полларда, використовуючи технологію обчислень на ТЧБ Крестенсона, та ґрунтується на аналогічних апаратних засобах. За результатами дослідження роботи паралельної системи на декількох програмованих матрицях FPGA для розв'язання логарифма для ЕК різного розміру та проведених вимірювань визначено, що застосування «шляхів пошуку» алгоритму, який реалізовано на одній програмованій матриці FPGA, зумовлює трикратне збільшення швидкості роботи алгоритму в порівнянні з системою, побудованою на базі процесора Itanium 2.

Результати дисертаційної роботи впроваджені та отримали використання у навчальному процесі Університету в Бєльсько-Бялій (Польща) (акт впровадження від 24 листопада 2015 року) та Національного авіаційного університету (акт впровадження від 18 травня 2016 року) згідно з Угодою про співробітництво між університетами №336 від 15 травня 2014 року.

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. З друкованих праць, що опубліковані у співавторстві, у роботі використовуються результати, отримані особисто здобувачем. У роботах, опублікованих у співавторстві, здобувачеві належать: [1,5,6,15,16,27-30,32] – побудова захищеної топології БСМ; розробка алгоритмів синтезу БСМ з існуючими інформаційними інфраструктурами; [2,4,8,11-14,19,31,33,34] – розробка методів і засобів криптографічного захисту БСМ; застосування еліптичних кривих для досягнення необхідного рівня криптостійкості компонентів БСМ; розробка структурно-аналітичних моделей обчислення дискретного логарифму для кривих над полем $GF(2^m)$ для побудови високопродуктивних криптографічних пристроїв на еліптичних кривих; [3,20-22,25] – розробка методів забезпечення живучості БСМ у контексті забезпечення їх доступності; розробка стратегії обслуговування гарантоздатної інформаційно-управляючої системи за показниками готовності технічного та інформаційного станів відносно сформованої множини дефектів; [7,17,26] – розробка на базі запропонованих методів і моделей інструментальних засобів для забезпечення захищеності БСМ та їх компонентів; [9,10,35] – аналіз

уразливостей архітектури Інтернету речей (та БСМ як її основи) та стійкості до різних типів кібератак.

Апробація результатів роботи. Основні положення дисертаційної роботи доповідалися та обговорювалися на міжнародних науково-технічних конференціях та семінарах, серед яких 9th International Workshop on Computational Problems of Electrical Engineering (CPEE) (2008, Alushta, Crimea, Ukraine), 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (2015, Warsaw, Poland), 2nd International Conference «Renewable Energy Sources: Engineering, Technology, Innovations» (2015, Krynica, Poland), Междунар. науч.-техн. конф. «Приборостроение» (2014, Минск, Республика Беларусь), Міжвідомчий міжрегіональний семінар Наукової Ради НАН України «Технічні засоби захисту інформації» (2013-2014), Міжнар. наук.-практ. конф. «Інформаційні технології та безпека в управлінні» (ITSM) (2011, Севастополь, Крим, Україна), Міжнар. наук.-практ. конф. «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації» (CICSIS) (2015-2016 рр., Верхній Студений, Закарпаття, Україна), наук.-практ. конф. «Проблеми експлуатації та захисту інформаційно-комунікаційних систем» (2016 р., Київ, Україна) та ін.

Публікації. Основні положення дисертації опубліковано у 35 наукових працях, у тому числі 3 монографіях, 26 статтях фахових вітчизняних та закордонних рецензованих наукових виданнях (5 з яких входять до наукометричної бази Scopus), 1 патенті України на корисну модель та 5 матеріалах міжнародних конференцій.

Структура роботи та її обсяг. Дисертація складається зі вступу, п'яти розділів, загальних висновків, додатків, списку використаних джерел і має 198 сторінок основного тексту, 46 рисунків, 43 таблиці, 15 сторінок додатків. Список літератури містить 176 найменувань і займає 12 сторінок. Загальний обсяг роботи 225 сторінок.

ОСНОВНИЙ ЗМІСТ

У **вступі** представлена загальна характеристика роботи, обгрунтована актуальність наукової теми, сформульовані мета і задачі дослідженя, відображено наукову новизну та практичну цінність отриманих результатів і висновків, наведено дані щодо їх апробації та впровадження.

У **першому розділі** проведений аналіз сучасного стану розвитку концепції IoT як обчислювальної мережі фізичних об'єктів, оснащених вбудованими сенсорними технологіями для взаємодії один з одним або з зовнішнім середовищем.

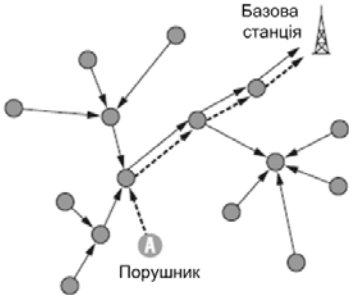

Рис.1. Схема потенційної DoS-атаки в БСМ

У результаті проведеного аналізу щодо можливості реалізації різного типу кібератак було виявлено такі проблеми IoT, як уразливість до DoS-атак (рис.1), можливість порушення конфіденційності шляхом прослуховування вузлів та їх захоплення, а також необхідність забезпечення цілісності ресурсів та фізична безпека сенсорів – тобто в IoT актуальним є захист інформації від множини кіберзагроз, що порушують їх базові характеристики безпеки. Також визначено, що реалізація порушником таких загроз може привести до втрати або нелегітимної модифікації інформації сенсорів. Наслідки DoS-атак (направлених, в першу чергу, на порушення доступності) щодо збірних сенсорних вузлів транзитного і верхнього

рівнів можна поділити на такі категорії: ушкодження базових станцій, ушкодження збірних сенсорних вузлів транзитного рівня (рівень шкоди залежить від конкретних додатків сенсорних давачів, наприклад, моніторингу шуму, світла, забруднення навколишнього середовища тощо). За рівнями моделі OSI ці атаки можна диференціювати відповідно до табл. 1.

Таблиця 1

Розподіл кібератак за рівнями моделі OSI

Рівень OSI	Тип кібератаки	Контрзаходи
Фізичний	Jamming (глушіння)	Розширення спектру, пріоритизація повідомлень, картування областей.
	Tampering (підробка)	Випробувальні пакети проти підробки, використання нечутливих до відмов протоколів.
Канальний	Колізії	Корегувальне кодування.
	Виснаження	Обмеження швидкості передавання даних.
	Збір інформації	Захисту проти повторних відправлень, сувора аутентифікація на канальному рівні.
Мережевий	Фальсифікація маршрутної інформації	Аутентифікація, використання захисту проти повторних відправлень.
	Селективне просування	Використання різних маршрутів, підтвердження доставки.
	Sinkhole атака	Перевірка надмірності.
	Sybil атака	Аутентифікація, надмірність, моніторинг.
Транспортний	Flood атака	Клієнтські пазли.
	Розсинхронізація	Аутентифікація.
Прикладний	DoS атака на базі маршруту	Аутентифікація, використання захисту проти повторних відправлень.
	Перепрограмування	

Встановлено, що БСМ, як одна із базових технологій IoT, є вразливою до DoS-атак, які спрямовані на легітимні послуги (порушення доступності ресурсів інформаційних систем). Такі атаки компрометують вузли в БСМ, використовують їхні обчислювальні ресурси для реалізації алгоритму кібератаки. Можливим також є створення на їх основі ботнетів, що стануть джерелом різноманітних типів кіберзагроз (наприклад Sinkhole, Sybil, Wormhole, Flood тощо), направлених на порушення базових характеристик безпеки БСМ та інших ресурсів. Це зумовлює необхідність забезпечення високих вимог до вибору стійких архітектур «клієнт-сервер-шлюз-вузол» в БСМ. Для відстеження основного джерела кібератаки або після її реалізації необхідно розробити відповідні методи контролювання пакетів на маршрутизаторах (координаторах) БСМ. Важливим є визначення виду кібератак на комунікації клієнтів (вузлів БСМ) і сервери, що компрометують вузли та можливі шляхи від точок доступу до точок призначення. Необхідно визначати і контролювати технічні параметри, що регулюють обсяг пакетів, переданих кожним каналом зв'язку окремо, і загальний обсяг пакетів БСМ. Для ефективності локалізації джерела кібератаки доцільно зменшувати чинник невизначеності ресурсу БСМ шляхом запобігання фальсифікації пакетів.

Таким чином, як показав проведений аналіз, БСМ є уразливими до різного роду кіберзагроз і саме тому розробка та дослідження методів і моделей захисту БСМ та їх компонентів від кіберзагроз, спрямованих на порушення базових характеристик безпеки, є актуальною науковою проблемою, яка потребує вирішення.

Другий розділ присвячений розробці моделей інформаційних структур ймовірності кіберзагроз визначеного класу DoS-атак та захищеної комунікації «клієнт-сервер-шлюз-вузол». БСМ фактично є розподіленими мережами, які самоорганізовуються та

складаються із мікроконтролерів, прийомопередавачів, елементів живлення і великої кількості сенсорів та виконавчих пристроїв, об'єднаних між собою за допомогою радіоканалу, для вимірювання параметрів навколишнього середовища, наприклад, температури, освітленості, вібрації, тиску, рівня шуму та інших (рис. 2).

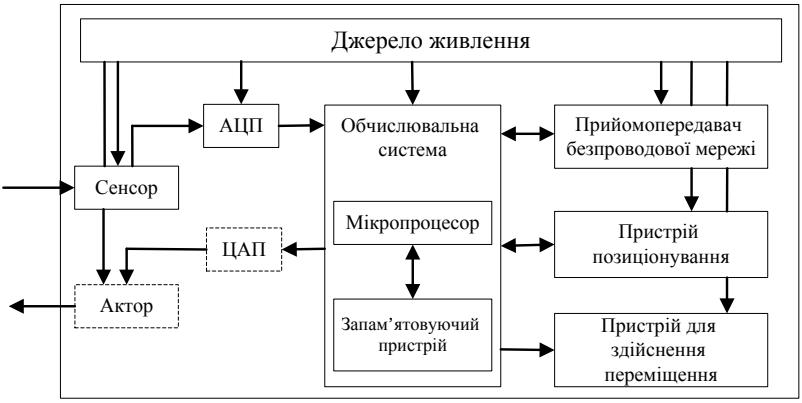

Рис. 2. Архітектура сенсорного (сенсорно-акторного) вузла БСМ

Для визначення рівня впливу показників атак на БСМ запропоновані нові *математичні моделі інформаційних структур ймовірності кіберзагроз визначеного класу DoS-атак на БСМ:*

$$\begin{cases} P_{інф.загр.} = \alpha_1 P_{конф.} + \alpha_2 P_{ціл.} + \alpha_3 P_{доступ.} \\ P_{конф.} = < K_{В.К.С.З.}, K_{\text{I.K.B.I.}} < K_{К.В.П.}\ K_{В.І.Ч.К.} >> \\ P_{ціл.} = \begin{bmatrix} K_{Вид.інф.} \\ \left\langle K_{В.Н.К.С.} < K_{В.З.А.}, K_{П.Л.З.Д.З.С.}, K_{П.Л.}, K_{С.С.П.}, K_{С.А.П.П.}, K_{А.С.} >, \right. \\ \left. K_{Вір.}, K_{Т.П.}, K_{П.З.} \right\rangle \\ K_{Зам.інф.} \end{bmatrix}, \\ P_{дост.} = \begin{bmatrix} K_{В.Д.П.П.Я.} \\ \left\langle K_{В.К.П.З.І.С.} \right\rangle \\ K_{К.Д.З.} \end{bmatrix} \end{cases} \quad (1)$$

де α_i – вагові коефіцієнти впливу показників конфіденційності, цілісності та доступності на результуючий показник кіберзагроз, причому $\sum_{i=1}^{3} \alpha_i = 1$, $P_{інф.загр.}$ – показники кіберзагроз, $P_{конф.}$ – показник конфіденційності інформації, $P_{ціл.}$ – показник цілісності інформації, $P_{дост.}$ – показник доступності інформації, $K_{В.К.С.З.}$ – коефіцієнт втрати контролю над системою захисту, $K_{I.K.B.I.}$ – коефіцієнт існування каналів витоку інформації, $K_{К.В.П.}$ – коефіцієнт каналу витоку за пам'яттю, $K_{В.І.Ч.К.}$ – коефіцієнт витоку інформації за часовим каналом, $K_{вид.інф.}$ – коефіцієнт видалення інформації, $K_{зам.інф.}$ – коефіцієнт заміни інформації, $K_{В.Н.К.С.}$ – коефіцієнт випадкової або навмисної критичної ситуації, $K_{Вір.}$ – коефіцієнт вірусів, $K_{Т.П.}$ – коефіцієнт «троянських програм», $K_{П.З.}$ – коефіцієнт програмних закладок, $K_{В.З.А.}$ – коефіцієнт відмови і збоїв в апаратурі,

$K_{П.Л.З.Д.З.С.}$ – коефіцієнт перешкод на лініях зв'язку від дій зовнішнього середовища, $K_{П.Л.}$ – коефіцієнт помилок людини, $K_{С.С.П.}$– коефіцієнт схемних і схемотехнічних помилок, $K_{С.А.П.П.}$ – коефіцієнт структурних, алгоритмічних і програмних помилок, $K_{А.С.}$ – коефіцієнт аварійних ситуацій, $K_{В.Д.П.П.Я.}$ – коефіцієнт випадкових дій, пов'язаних з випадковими явищами, $K_{Н.Д.З.}$ – коефіцієнт навмисних дій зловмисників, $K_{В.К.П.З.І.С.}$ – коефіцієнт великої кількості помилкових запитів до серверів.

Проаналізувавши класифікацію DoS-атак, запропоновано формалізовану математичну модель, яка дозволяє визначити рівень впливу показників кібератак на БСМ:

$$\begin{aligned} P_{DoS} &= \beta_1 P_{Smurf} + \beta_2 P_{Fraggle} + \beta_3 P_{SYNFlood} + \beta_4 P_{DNS}, \\ P_{DDoS} &= \delta_1 P_{Trinoo} + \delta_2 P_{TFN/TFN2K} + \delta_3 P_{Stacheldraht}, \\ P_{DRDoS} &= \mu_1 P_{Smurf} + \mu_2 P_{Fraggle} + \mu_3 P_{DNS} + \mu_4 P_{SNMP}, \end{aligned} \quad (2)$$

де β_i, δ_i, μ_i – вагові коефіцієнти впливу показників різного класу DoS-атак, причому $\sum_{i=1}^{4}\beta_i = 1$, $\sum_{i=1}^{3}\delta_i = 1$, $\sum_{i=1}^{4}\mu_i = 1$.

Вагові коефіцієнти визначають внесок основних видів DoS-атак в БСМ та дають змогу врахувати зазначені кібератаки при розробці та експлуатації систем захисту інформації (рис. 3). Дослідження показали, що всі види кібератак рівноймовірно впливають на роботу БСМ. Із збільшенням ймовірностей різновидів атак імовірність кіберзагроз, що відповідають типу DoS-атак, лінійно зростають. Запропоновані моделі за рахунок сформованої базової множини характерних показників і відповідних вагових коефіцієнтів та взаємозв'язків визначених матриць активності мережі і встановленої інтенсивності впливу різних класів кібератак, дозволяють визначити рівень впливу показників та критеріїв кіберзагроз щодо БСМ.

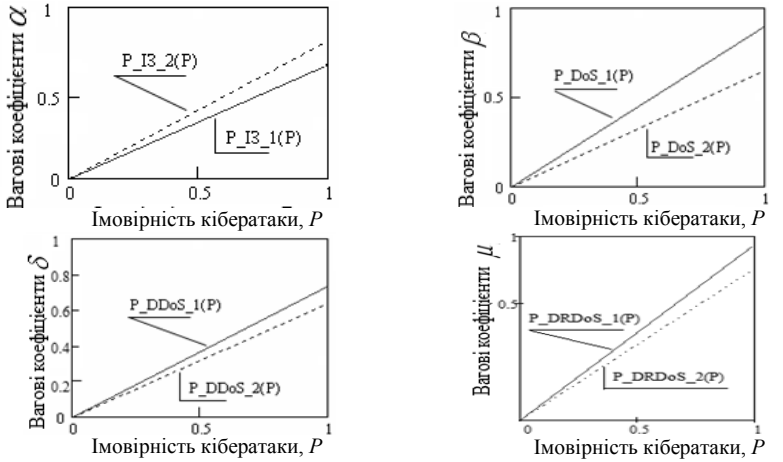

Рис. 3. Залежність вагових коефіцієнтів від ймовірності загроз реалізації DoS-атак

Отримала подальший розвиток *модель захищеної комунікації «клієнт-сервер-шлюз-вузол»,* яка дала можливість ідентифікувати клас реалізованої кібератаки на БСМ та визначити відповідні заходи протидії. Модель використовує метод вагових коефіцієнтів, які можна визначити експериментальним шляхом для кожної конкретної БСМ.

Тобто, спроектувати архітектури мереж і встановити інтенсивність різного виду кібератак на БСМ. За допомогою спрощеної моделі комунікації «клієнт-сервер-шлюз-вузол» і математичних моделей (1) та (2) визначаються матриці активності мережі БСМ (3), згідно з якими формується висновок про здійснення виду кібератаки:

$$\alpha_{інф.загр.}=\begin{bmatrix}\alpha_1^a & \alpha_2^a & \alpha_3^a\\ \alpha_1^b & \alpha_2^b & \alpha_3^b\\ \alpha_1^c & \alpha_2^c & \alpha_3^c\\ \alpha_1^d & \alpha_2^d & \alpha_3^d\\ \alpha_1^e & \alpha_2^e & \alpha_3^e\\ \alpha_1^f & \alpha_2^f & \alpha_3^f\\ \alpha_1^g & \alpha_2^g & \alpha_3^g\end{bmatrix},\beta_{DoS}=\begin{bmatrix}\beta_1^a & \beta_2^a & \beta_3^a & \beta_4^a\\ \beta_1^b & \beta_2^b & \beta_3^b & \beta_4^b\\ \beta_1^c & \beta_2^c & \beta_3^c & \beta_4^c\\ \beta_1^d & \beta_2^d & \beta_3^d & \beta_4^d\\ \beta_1^e & \beta_2^e & \beta_3^e & \beta_4^e\\ \beta_1^f & \beta_2^f & \beta_3^f & \beta_4^f\\ \beta_1^g & \beta_2^g & \beta_3^g & \beta_4^g\end{bmatrix},$$

$$\delta_{DDoS}=\begin{bmatrix}\delta_1^a & \delta_2^a & \delta_3^a\\ \delta_1^b & \delta_2^b & \delta_3^b\\ \delta_1^c & \delta_2^c & \delta_3^c\\ \delta_1^d & \delta_2^d & \delta_3^d\\ \delta_1^e & \delta_2^e & \delta_3^e\\ \delta_1^f & \delta_2^f & \delta_3^f\\ \delta_1^g & \delta_2^g & \delta_3^g\end{bmatrix},\mu_{DRDoS}=\begin{bmatrix}\mu_1^a & \mu_2^a & \mu_3^a & \mu_4^a\\ \mu_1^b & \mu_2^b & \mu_3^b & \mu_4^b\\ \mu_1^c & \mu_2^c & \mu_3^c & \mu_4^c\\ \mu_1^d & \mu_2^d & \mu_3^d & \mu_4^d\\ \mu_1^e & \mu_2^e & \mu_3^e & \mu_4^e\\ \mu_1^f & \mu_2^f & \mu_3^f & \mu_4^f\\ \mu_1^g & \mu_2^g & \mu_3^g & \mu_4^g\end{bmatrix}. \quad (3)$$

Основним коефіцієнтом ефективності архітектур БСМ є коефіцієнт емерджентності, за допомогою якого доцільно провести аналіз моделей комунікації «клієнт-сервер-шлюз-вузол». Отже, взявши загальну кількість кібератак за 100%, можна визначити скільки процесів буде належати кожному виду кібератак. З проведених досліджень і з врахуванням аналітичних виразів (3), слідує:

$$\begin{aligned}&\alpha_1^a=\frac{n_{Конф.}^a}{100\%},\alpha_2^a=\frac{n_{Ціл.}^a}{100\%},\alpha_3^a=\frac{n_{Дост.}^a}{100\%},\\ &\beta_1^a=\frac{n_{Smurf}^a}{100\%},\beta_2^a=\frac{n_{Fraggle}^a}{100\%},\beta_3^a=\frac{n_{SYNFlood}^a}{100\%},\beta_4^a=\frac{n_{DNS}^a}{100\%},\\ &\delta_1^a=\frac{n_{Trinoo}^a}{100\%},\delta_2^a=\frac{n_{TFN/TFN2K}^a}{100\%},\delta_3^a=\frac{n_{Stacheldraht}^a}{100\%},\\ &\mu_1^a=\frac{n_{Smurf}^a}{100\%},\mu_2^a=\frac{n_{Fraggle}^a}{100\%},\mu_3^a=\frac{n_{DNS}^a}{100\%},\mu_4^a=\frac{n_{SNMP}^a}{100\%},\end{aligned} \quad (4)$$

де $n_{Конф.}^a$, $n_{Ціл.}^a$, $n_{Дост.}^a$ – кількість показників кіберзагроз на комунікацію «клієнт-сервер-шлюз-вузол», n_{Smurf}^a, $n_{Fraggle}^a$, $n_{SYNFlood}^a$, n_{DNS}^a – кількість показників кібератак виду DoS на комунікацію «клієнт-сервер-шлюз-вузол», n_{Trinoo}^a, $n_{TFN/TFN2K}^a$, $n_{Stacheldraht}^a$ – кількість показників атак виду DDoS на комунікацію «клієнт-сервер-шлюз-вузол», n_{Smurf}^a, $n_{Fraggle}^a$, n_{DNS}^a, n_{SNMP}^a – кількість показників атак виду DRDoS на комунікацію «клієнт-сервер-шлюз-вузол».

З урахуванням (3), можна визначити дані вагові коефіцієнти, які встановлюють міру впливу DoS-атак на комунікацію «клієнт-сервер-шлюз-вузол». З проведених

досліджень і з врахуванням (4) та емерджентності моделі комунікації «клієнт-сервер-шлюз-вузол» отримано конкретні значення вагових коефіцієнтів:

$$\alpha_1^{\alpha}=\frac{3}{8}\cdot\frac{1}{k_e^{\alpha}}=0{,}375,\ \alpha_1^{b}=\frac{3}{8}\cdot\frac{1}{k_e^{b}}=0{,}15,\ \alpha_1^{c}=\frac{3}{8}\cdot\frac{1}{k_e^{c}}=0{,}15,$$

$$\alpha_1^{d}=\frac{3}{8}\cdot\frac{1}{k_e^{d}}=0{,}125,\alpha_1^{e}=\frac{3}{8}\cdot\frac{1}{k_e^{e}}=0{,}15,\ \alpha_1^{f}=\frac{3}{8}\cdot\frac{1}{k_e^{f}}=0{,}15,$$

$$\alpha_1^{g}=\frac{3}{8}\cdot\frac{1}{k_e^{g}}=0{,}75,\ \alpha_2^{\alpha}=\frac{1}{8}\cdot\frac{1}{k_e^{\alpha}}=0{,}125,\ \alpha_2^{b}=\frac{1}{8}\cdot\frac{1}{k_e^{b}}=0{,}05,$$

$$\alpha_2^{c}=\frac{1}{8}\cdot\frac{1}{k_e^{c}}=0{,}05,\ \alpha_2^{d}=\frac{1}{8}\cdot\frac{1}{k_e^{d}}=0{,}375,\alpha_2^{e}=\frac{1}{8}\cdot\frac{1}{k_e^{e}}=0{,}05, \qquad (5)$$

$$\alpha_2^{f}=\frac{1}{8}\cdot\frac{1}{k_e^{f}}=0{,}05,\alpha_2^{g}=\frac{1}{8}\cdot\frac{1}{k_e^{g}}=0{,}0625,\alpha_3^{\alpha}=\frac{1}{2}\cdot\frac{1}{k_e^{\alpha}}=0{,}5,$$

$$\alpha_3^{b}=\frac{1}{2}\cdot\frac{1}{k_e^{b}}=0{,}2,\ \alpha_3^{c}=\frac{1}{2}\cdot\frac{1}{k_e^{c}}=0{,}2,\ \alpha_3^{d}=\frac{1}{2}\cdot\frac{1}{k_e^{d}}=0{,}166,$$

$$\alpha_3^{e}=\frac{1}{2}\cdot\frac{1}{k_e^{e}}=0{,}2,\ \alpha_3^{f}=\frac{1}{2}\cdot\frac{1}{k_e^{f}}=0{,}2,\ \alpha_3^{g}=\frac{1}{2}\cdot\frac{1}{k_e^{g}}=0{,}25.$$

Коефіцієнти (5) визначені експериментально, шляхом розробки архітектури, і дозволяють визначити інтенсивність кібератак на БСМ. На основі використання методу вагових коефіцієнтів розроблено математичну модель комунікації «клієнт-сервер-шлюз-вузол» для диференціації кібератак у БСМ, яка містить імовірність компрометації вузла та кількість можливих шляхів від точок доступу до точок призначення:

$$\mathrm{I}\alpha_i^{a}=\frac{1}{k_e^{a}}\left[P_{AP}^{1}+P_{AP}^{2}\right],\ \mathrm{II}\alpha_i^{b}=\frac{1}{k_e^{b}}\left[2P_{AP}^{1}+P_{AP}^{2}\right],\ \mathrm{III}\alpha_i^{c}=\frac{1}{k_e^{c}}\left[P_{AP}^{1}+2P_{AP}^{2}\right],$$

$$\mathrm{IV}\alpha_i^{d}=\frac{1}{k_e^{d}}\left[2P_{AP}^{1}+2P_{AP}^{2}\right],\ \mathrm{V}\alpha_i^{e}=\frac{1}{k_e^{e}}\left[2P_{AP}^{1}+P_{AP}^{2}\right],\ \mathrm{VI}\alpha_i^{f}=\frac{1}{k_e^{f}}\left[P_{AP}^{1}+2P_{AP}^{2}\right] \qquad (6)$$

$$\mathrm{VII}\alpha_i^{g}=\frac{1}{k_e^{g}}\left[P_{AP}^{1}+P_{AP}^{2}\right]$$

де $\alpha_i^{a},\alpha_i^{b}$, α_i^{c}, α_i^{d}, α_i^{e}, $\alpha_i^{f},\alpha_i^{g}$ – вагові коефіцієнти, *a, b, c, d, e, f, g* – тип моделі комунікації, *i* – види DoS-атак, k_e^{a}, k_e^{b}, k_e^{c}, k_e^{d}, k_e^{e}, k_e^{f}, k_e^{g} – коефіцієнти емерджентності в комунікації «клієнт-сервер-шлюз-вузол». Проведено експеримент згідно з математичною моделлю (6), який відображено на рис. 4.

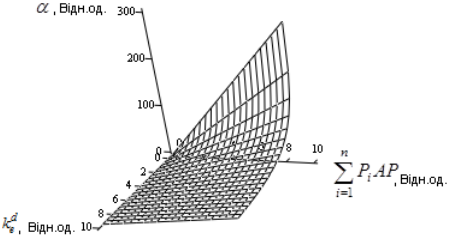

Рис. 4. Залежність вагових коефіцієнтів від імовірності скомпрометованих точок доступу і кількості можливих шляхів «клієнт-сервер-шлюз-вузол»

Результати експериментів показали, що для значення емерджентності $k_e^d = 3$ і сумарної імовірності скомпрометованих точок доступу, яка дорівнює 4,2354, ваговий коефіцієнт комунікації «клієнт-сервер-шлюз-вузол» зростає до значення 17 відносних одиниць. Проаналізувавши спрощені архітектури комунікації «клієнт-сервер-шлюз-вузол», коефіцієнти їх емерджентості можна поділити на 4 групи: $K_e = 1$, $K_e = 2$, $K_e = 2{,}5$, $K_e = 3$. На основі коефіцієнтів емерджентості для спрощеної моделі комунікації «клієнт-сервер-шлюз-вузол» знайдено критерій $K_{зе}$ (табл. 2) забезпечення певного рівня захисту для спрощеної моделі комунікації «клієнт-сервер-шлюз-вузол».

Таблиця 2

Показники критерію забезпечення рівня захисту для спрощеної моделі комунікації «клієнт-сервер-шлюз-вузол»

$K_з$ \ K_e	1	2	2,5	3
10	0,100	0,200	0,250	0,300
9	0,111	0,222	0,3125	0,333
8	0,125	0,250	0,4375	0,375
7	0,143	0,286	0,357	0,428
6	0,166	0,333	0,416	0,500
5	0,200	0,400	0,500	0,600
4	0,250	0,500	0,625	0,750
3	0,333	0,666	0,833	1,000
2	0,5	1,000	1,250	1,500
1	1,000	2,000	3,500	3,000

За допомогою аналізу коефіцієнта емерджентності для розподілених комп'ютерних систем та мереж визначено коефіцієнт стійкості $K_{зе}$ для архітектури комунікації «клієнт-сервер-шлюз-вузол» БСМ (рис. 5).

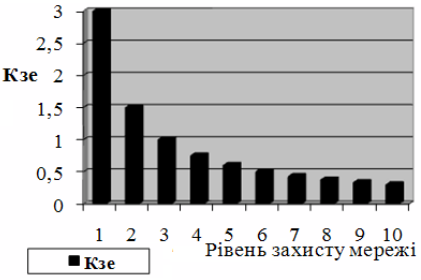

Рис. 5. Коефіцієнт стійкості для спрощеної моделі комунікації «клієнт-сервер-шлюз-вузол»

Результати досліджень показали, що для забезпечення необхідного рівня захисту інформації в БСМ, необхідно вибирати таку модель комунікації «клієнт-сервер-шлюз-вузол», для якої відношення коефіцієнта захищеності до емержентності БСМ близьке до 1. Слід врахувати небезпеку DoS-атак, яка полягає в тому, що ці атаки проявляють себе тоді, коли обчислюваного ресурсу БСМ стає недостатньо. Моніторинг трафіку БСМ є необхідною умовою для нормального функціонування БСМ, в основу якого покладено критерій мінімального обсягу мережевих даних.

Визначено параметри, які регулюють обсяг пакетів, переданих кожним каналом зв'язку окремо, і загальний обсяг пакетів, що передані за час поновлення таблиць маршрутизації. Загальний обсяг трафіка *V* визначається згідно моделі:

$$V = \frac{T_{sys}}{\Delta t_{sys}} \sum_{i,j=1}^{N} P_i Q_j \,, \tag{7}$$

де Δt_{sys} – час одного такту системи, Q_j – обсяг інформації, переданої за один такт за кожним окремим каналом в БСМ, N – кількість вузлів БСМ, P_i – ступінь компрометації вузла, T_{sys} – час, на протязі якого при зміні топології БСМ вузли розповсюджують повідомлення про поновлення маршрутів. Результати експериментів за виразом (7) представлено на рис. 6.

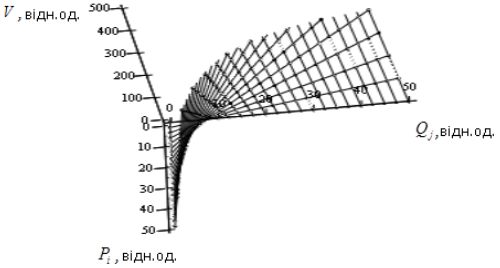

Рис.6. Залежність обсягу трафіка від ступеня компрометації вузла

Експерименти показали, що під час кібератаки стрімко збільшується загальний обсяг трафіку БСМ, причому він досягає значення 470 відн. од. Для $Q_j = 10$ відн. од. і ступеня компрометації 0,05 обсяг трафіка стрімко зростає.

Третій розділ присвячений розробці методів відновлення повідомлень та ймовірнісного маркування пакетів у БСМ.

Удосконалено *метод ймовірнісного маркування пакетів у БСМ*, який дозволяє здійснювати моніторинг БСМ та відстежувати джерела кібератак. Проведено моделювання системи захисту для комунікації «клієнт-сервер-шлюз-вузол», результати якого показали необхідність дослідження чинника невизначеності трафіку з використанням методу імовірнісного маркування пакетів на маршрутизаторах:

$$\mathrm{I\,m_a} = \sum_{i=1}^{M} \frac{(1-p)^{d_i^a}}{p(1-p)^{d_i^a-1}}, \mathrm{II\,m_b} = \sum_{i=1}^{M} \frac{(1-p)^{d_i^b}}{p(1-p)^{d_i^b-1}}, \mathrm{III\,m_c} = \sum_{i=1}^{M} \frac{(1-p)^{d_i^c}}{p(1-p)^{d_i^c-1}},$$

$$\mathrm{IV\,m_d} = \sum_{i=1}^{M} \frac{(1-p)^{d_i^d}}{p(1-p)^{d_i^d-1}}, \mathrm{V\,m_e} = \sum_{i=1}^{M} \frac{(1-p)^{d_i^e}}{p(1-p)^{d_i^e-1}}, \mathrm{VI\,m_f} = \sum_{i=1}^{M} \frac{(1-p)^{d_i^f}}{p(1-p)^{d_i^f-1}}, \tag{8}$$

$$\mathrm{VII\,m_g} = \sum_{i=1}^{M} \frac{(1-p)^{d_i^g}}{p(1-p)^{d_i^g-1}}$$

де $d_i^a, d_i^b, d_i^c, d_i^d, d_i^e, d_i^f, d_i^g$ – кількість вузлів на шляху кібератаки, p – імовірність зміни маркування пакетів ініціатором кібератак, M – маркування пакетів БСМ, відповідно.

Проведено експеримент згідно з емпіричною моделлю ресурсу БСМ (8), результати якого узагальнено на рис. 5 для комунікації «клієнт-сервер-шлюз-вузол» БСМ. Результати експерименту показали, що під час DoS-атаки, при зростанні кількості скомпрометованих вузлів в комунікації «клієнт-сервер-шлюз-вузол» збільшується фактор невизначеності m та витрат на обробку даних, понесених користувачем для відстеження кібератак. Показано, що для запобігання DoS-атаки ефективним є метод

імовірнісного маркування пакетів з різною імовірністю їх маркування на маршрутизаторах та із використанням процедури *TTL*, застосовування якого дає змогу виявляти та відтворювати схему організації кібератаки у найпродуктивніший спосіб.

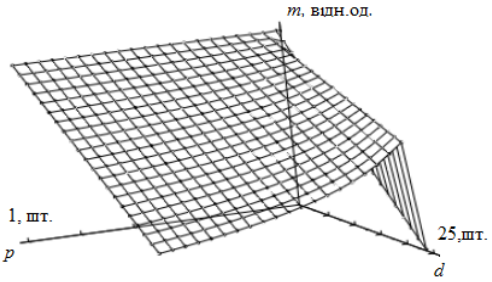

Рис. 7. Результати моделювання DoS-атаки: *m* – чинник невизначеності, *p* – імовірність зміни маркування пакета ініціатором атак, *d* – кількість вузлів на шляху DoS-атаки

Алгоритм маркування пакетів БСМ. Якщо блоки $b_0, b_1, \ldots, b_{l-1}$ призначені для повідомлення M_X, тоді можна розпочати маркування пакетів. Нехай p $(p = 20)$ – параметр імовірності. Подія відбудеться з імовірністю $(1-p)$, якщо маршрутизатор *X* пересилає пакет за призначенням. В іншому випадку, маршрутизатор *X* випадково вибирає один з блоків b_i, поміщає b_i в багаторазові біти цього пакету, тоді оновлюється контрольна сума заголовку в міру необхідності, потім передає переглянутий пакет за призначенням. Процес маркування триває до тих пір, поки не змінюється повідомлення M_X. Якщо повідомлення M_X змінюється, то маршрутизатор *X* повторює обчислення для b_i блоків для нового повідомлення. Потім маршрутизатор повторює алгоритм імовірнісного маркування пакетів для нового набору блоків. Для маршрутизатора не потрібно зберігати блоки $b_0, b_1, \ldots, b_{l-1}$, оскільки швидко генерується випадково блок b_i.

Отримав подальший розвиток *метод відновлення повідомлення,* який дає можливість забезпечити цілісність повідомлень в умовах реалізації відповідних кіберзагроз БСМ. Оскільки фрагментація повідомлення на невеликі блоки індексується з великою статистично випадковою контрольною сумою, то це може бути ефективним підходом для відправлення повідомлень користувачеві за розміром більшим, ніж *b* біт. Зокрема, фрагментації сполучаються в два, чотири або вісім фрагментів слова та можуть бути ефективним способом для відправлення середнього розміру повідомлень користувачеві (наприклад, від 48 біт до 96 біт). Проте, якщо є більшого розміру повідомлення (наприклад, порядку 128 біт або 192 біт), вісім фрагментів можуть бути недостатніми, щоб надати повідомлення і використати велику контрольну суму, яка є необхідною для безпеки та відновлення повідомлення. Тоді доцільно повторити метод випадкового посилання для відправлення великих за розміром повідомлень. Отже, повідомлення *M* доцільно розділити на слова *l*, $M_0, M_1, M_2, \ldots, M_l$. Цей розподіл повинен бути зроблений таким чином, щоб зберегти в кожному слові M_i таку ж ступінь випадковості, як і в повідомленні *M*. Якщо повідомлення *M* достатньо велике, то можна помітити, що кожне слово M_i є занадто велике для того, щоб його перенести в блок даних з

великим ступенем достеменності. Тоді, кожне слово M_i можна розділити на m підслів $M_{i,0}, M_{i,1}, M_{i,2}, \ldots, M_{l,m}$. Значення m і розмір підслів можна позначити числом c_1 контрольної суми бітів для відправлення підслів, за умови однакового розміру b біт в блоку.

Доцільно відвести ($b - c_1 - \lceil \log m \rceil$) біт для даних в кожному підслові $M_{i,j}$. Таким чином можна скласти підслова у великі блоки розміром ($m(b - c_1 - \lceil \log m \rceil)$) біт. Для того, щоб великі блоки мали такий самий рівень захисту, як і малі за розміром блоки, то розмір кожної випадкової контрольної суми має бути ($c_2 = c_1 - \lceil \log m \rceil$) біт. Цей фактор пов'язаний з тим, що ймовірність зіткнення між двома різними пакетами в першій фазі становить $1/m2^{c_1}$ і ця імовірність в другій фазі дорівнює $1/lm2^{c_2}$, поки кожне слово другої фази не стане m підсловами першої фази. Крім того, доцільно виділити $\lceil \log l \rceil$ біт для фрагменту числа кожного індексу i. Тоді, для кожного слова M_i обчислюється c_2 -біт контрольної суми для досягнення високої довіри передачі повідомлень кожного слова (рис. 8).

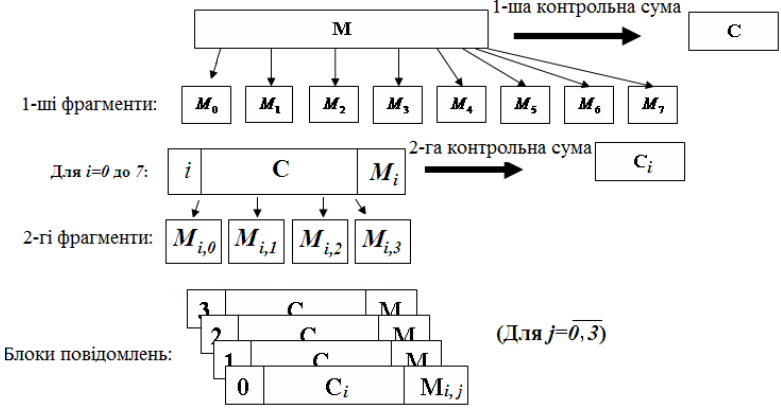

Рис. 8. Схема двофазної фрагментації повідомлення БСМ

У дворівневій схемі передача даних відбувається подібно однорівневій схемі. Крім того, маршрутизатор вирішує вставляти повідомлення в пакет, вибираючи один з багатьох його $M_{i,j}$ підслів. Відновлення повідомлення відбувається у два етапи. На першому етапі відновлюються всі кандидати слова M_i, а на другому етапі – всі повідомлення кандидата. Таким чином, час роботи для відновлення повідомлення в двофазній схемі $T_{ДС}$ пропорційний до наступного виразу:

$$T_{ДС} = N + \sum_{C} \prod_{i=0}^{m} M_{C,i} + \sum_{C} \prod_{i=0}^{l} N_{C,i}, \qquad (9)$$

де N – загальна кількість пакетів користувача, для відновлення повідомлення.

На рис.8 $M_{C,i}$ – це кількість окремих пакетів з набору контрольних сум C і фрагментів індексу i в першій фазі блоку відновлення повідомлення; $N_{C,i}$ – кількість

окремих пакетів з набору контрольних сум *C* і фрагментів індексу *i* в другій фазі блоку відновлення повідомлення. Ці величини можуть бути цілком прийнятними за умови достатньої кількості бітів у контрольній сумі *C*.

Четвертий розділ присвячено розробці структурно-аналітичних моделей забезпечення живучості ІУС БСМ, технології обчислень та моделей обчислювачів на еліптичних кривих.

Отримали подальший розвиток структурно-аналітичні моделі забезпечення доступності ІУС БСМ, які дають можливість здійснювати вибір ефективної стратегії обслуговування гарантоздатної ІУС за показниками готовності технічного та інформаційного станів відносно сформованої множини дефектів, що впливають на характеристику безпеки – доступність. Розроблення структурної моделі підвищення живучості ІУС проведено з врахуванням дефектів ДВ (дефекти диференційовано на три групи: ДР – розроблення або проектування, ДФ – фізичні та ДВ –зовнішні впливи), що дає можливість сформулювати завдання вибору (пошуку) оптимальної стратегії обслуговування гарантоздатної ІУС за показниками готовності технічного та інформаційного станів відносно всієї множини дефектів. При цьому взято до уваги зміну інформаційно-технічних станів, в одному з восьми яких може перебувати ІУС. Скористаємося напрямленим графом інформаційно-технічних станів (рис. 9):

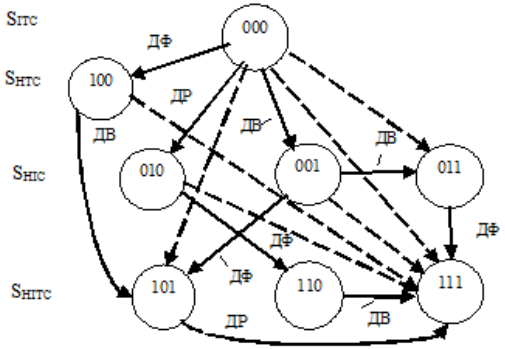

Рис.9. Напрямлений граф інформаційно-технічних станів ІУС БСМ

На рис. 9 позначено: S_{ITC} – інформаційно-технічний стан, $S_{НТС}$ – непрацездатний технічний стан, S_{HIC} – непрацездатний інформаційний стан, S_{HITC} – несправний (непрацездатний, небезпечний) інформаційно-технічний стан ІУС. Кожному стану та відповідній вершині графу станів надано трирозрядний код, який описує наявність відповідних дефектів ДФ, ДР і ДВ (1 – дефект присутній, 0 – відсутній). Переходи на графі, на яких виникають два або три дефекти різних типів, показані пунктиром як менш ймовірні. Приміром, у множину S_{HITC} входять підмножини S_{HITC1}(101), S_{HITC2}(110), S_{HITC3}(111), залежно від комбінації дефектів ДР і ДВ, за наявності ДФ, причому в розглянутих автором ІУС, включно з вбудованими криптографічними пристроями на еліптичних кривих (ІУСЕК), та їх моделях враховуються лише ДВ. Модель живучості ІУС, зокрема ІУСЕК можна представити сукупністю відповідної кількості часткових моделей різного призначення, в яких для опису процесів застосовуються як детерміновані, так і імовірнісні методи. Введемо позначення для множини *MS* інформаційно-технічних станів ІУСЕК: *ПС* – працездатний стан, *ЧП* – частково працездатний стан, *НБС* – працездатний безпечний стан, *НС* – небезпечний стан.

Один із підходів оцінювання гарантоздатності ґрунтується на розробленні та аналізуванні структурних моделей та схем живучості системи. Згідно чинних стандартів можна отримати об'єднання підмножин елементів ІУС, включно з елементами на ЕК, відмови яких призводять до її переходу в інший стан, для різних вихідних станів системи, а саме:

$$E_{ПС} = E_{ПС,ПС} \cup E_{ПС,ЧП} \cup E_{ПС,НБС} \cup E_{ПС,НС},$$
$$E_{ЧП} = E_{ЧП,ЧП} \cup E_{ЧП,НБС} \cup E_{ЧП,НС}, \quad (10)$$
$$E_{НБС} = E_{НБС,НБС} \cup E_{НБС,НС}.$$

Приміром, перше із співвідношень стосується випадку перебування ІУС у працездатному (вихідному) стані, для котрого множину її елементів $E_{ПС}$, включно з криптографічними на ЕК, можна подати у вигляді об'єднання підмножин елементів, відмови яких призводять до її переходу в інший працездатний стан – $E_{ПС,ПС}$, частково працездатний стан – $E_{ПС,ЧП}$, непрацездатний безпечний стан – $E_{ПС,НБС}$, і небезпечний стан – $E_{ПС,НС}$. Тоді для кожної із груп станів $MS_{ПС}$ і $MS_{ЧП}$ ІУС згідно з виразом (10) запропоновано побудувати відповідні структурні моделі живучості, враховуючи наявність криптографічних елементів на ЕК і беручи до уваги оцінювання живучості за станом системи та результатами виконання завдання: 1) для станів $MS_{ПС}$ схему живучості утворено елементами підмножин $E_{ПС,ПС}$ і $E_{ПС,ЧП}$ з можливим паралельним ввімкненням, $E_{ПС,НБС}$ і $E_{ПС,НС}$ з послідовним ввімкненням, модулем 1 оцінювання живучості ІУС за її станом, модулем 2 оцінювання живучості ІУС за результатами виконання нею завдання, моделлю прийняття рішення (ІІР) про способи підвищення живучості (включно із змінами структури та параметрів ІУС, а також додатковим удосконаленням пасивних та активних засобів забезпечення живучості), якщо оцінки вказують на її незадовільний рівень (рис. 10 а); 2) для станів $MS_{ЧП}$ схему живучості утворено елементами підмножин $E_{ЧП,ЧП}$ з можливим паралельним ввімкненням, $E_{ЧП,НБС}$ і $E_{ЧП,НС}$ з послідовним ввімкненням, модулем 1 оцінювання живучості ІУС за її станом, модулем 2 оцінювання живучості ІУС за результатами виконання нею завдання, моделлю прийняття рішення (ІІР) про способи підвищення живучості, якщо оцінки вказують на її незадовільний рівень (рис. 10 б). У наведених на рис. 10 моделях дефекти ДВ можна подати у вигляді точкової та просторової моделі, якщо класифікувати їх за областю дії. У точкових моделях ДВ викликає відмову одного або декількох елементів. Для одноточкової області за наявності K елементів ІУС одним з можливих розподілів є рівномірний розподіл $\alpha_i = 1/K$, тоді як для багатоточкової області в моделях можна застосувати зрізаний біноміальний розподіл

$$\beta_i = C_K^i p^i (1-p)^{K-i} / (1- p^K), i = 1,\ldots, K, \quad (11)$$

та зрізаний розподіл Пуассона:

$$\beta_i = \frac{a^i}{i!} / \sum_{j=1}^{K} \frac{a^j}{j!}, a = -\ln p\ , \quad (12)$$

де p – ймовірність виживання одиничного елемента в точковій моделі.

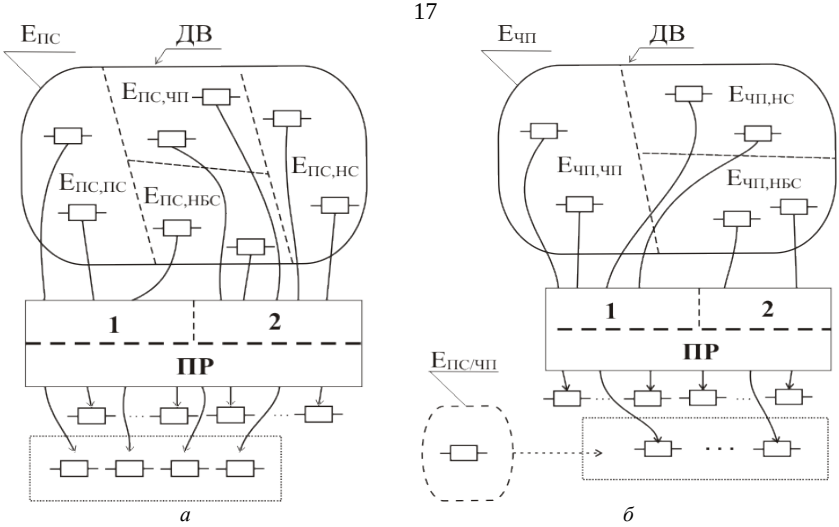

Рис.10. Структурна модель живучості ІУСЕК для вихідного стану: а) $MS_{ПС}$ б)$MS_{ЧП}$

У просторових моделях можна задати двомірний розподіл декартових координат епіцентру ДВ $p_2(x_0, y_0)$ і розподіл радіуса круга $p_0(r_0)$, в якому діє ДВ. За законом розподілу інтенсивності ДВ можна врахувати в моделі дефекти з нескінченною інтенсивністю, з постійною інтенсивністю I за всією площею області дії та зі спадною від епіцентру за певним законом $I(r,\varphi)$ інтенсивністю, зокрема, за законом Релея:

$$I(r, \varphi) = I_0 \exp(-r^2 / a r_0^2), \qquad (13)$$

де I_0 – максимальна інтенсивність в епіцентрі, r_0 – радіус круга - області дії ДВ, a – постійний параметр, r і φ – полярні координати точки при розташуванні початку координат в епіцентрі.

Удосконалено *технології обчислень на еліптичних кривих,* які дозволяють збільшити швидкість криптографічної обробки даних у пристроях ІУС БСМ. Результати проведеного теоретичного дослідження свідчать про те, що перспективною вбачається реалізація технології обчислень для прискореного виконання основних операцій на еліптичних кривих над полем вищих порядків $GF(p)$ на базі вбудованих модулів VIRTEX. При цьому точки на еліптичних кривих ще перед початком виконання операції додавання записано у проективних координатах, що дозволило уникнути необхідності обчислення оберненості. Операція обчислень на числах великої розрядності ґрунтується на модулярних додаванні, відніманні та множенні. Архітектура операційного пристрою для додавання точок базується на двох суматорах/віднімачах і двох помножувачах (рис. 11).

Операцію множення методом Монтгомері здійснено за допомогою алгоритму Radix-4. У скороченому вигляді множення двох k-бітних чисел X та Y відповідно до цього алгоритму можна подати так:

$$A = X \cdot Y = \{2^{k-1}x_{k-1} + 2^{k-2}x_{k-2} + x_{k-3,k-4}\} \times \{2^{k-1}x_{k-1} + 2^{k-2}y_{k-2} + y_{k-3,k-4}\}. \qquad (14)$$

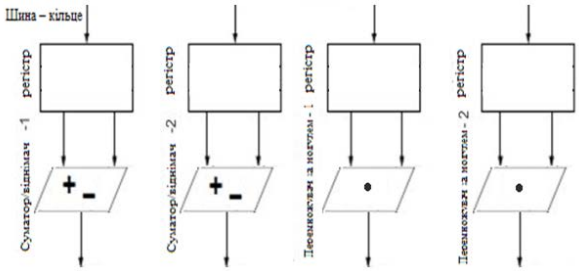

Рис. 11. Схема операційного пристрою для додавання точок на еліптичних кривих

Графічне представлення операції множення проілюстровано на рис. 12:

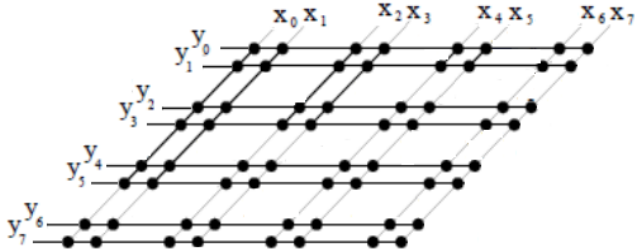

Рис. 12. Схема множення на основі алгоритму Radix-4

Дослідження показали, що час, необхідний для виконання одного додавання, в залежності від довжини модуля еліптичної характеристики, приймає значення, наведені в табл. 3.

Таблиця 3

Час виконання операції додавання двох точок на кривій *GF*(p)

GF(*p*)	Час додавання двох точок, мкс
128	4,45
256	10,34

Доведено, що прискорення обчислень на ЕК може бути досягнуто шляхом подальшої імплементації відповідного методу для еліптичних кривих виду $GF(2^m)$. Додавання точок еліптичної кривої $GF(2^m)$ проведено в проективних координатах. Додавання двох елементів, що належать еліптичній кривій $GF(2^m)$, полягає на додаванні відповідних коефіцієнтів за модулем 2. З цією метою застосовано операцію XOR для відповідних коефіцієнтів. Додавання точок A і B, результат якого дорівнює C, можна подати моделлю, представленою наступною формулою:

$$C = \sum_{i=0}^{m-1} a_i + b_i \bmod 2, \quad (15)$$

якщо

$$A = (a_{m-1}a_{m-2} \dots a_1a_0) \quad (16)$$

та

$$B = (b_{m-1}b_{m-2}\dots b_1b_0). \quad (17)$$

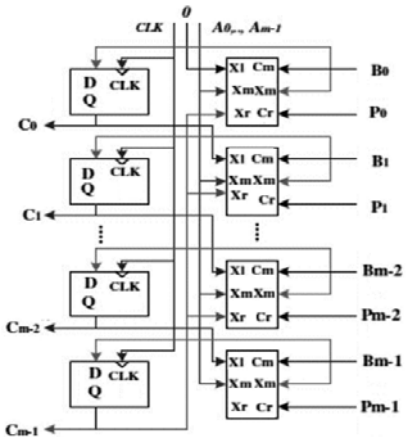

Рис. 13. Архітектура перемножувача за модулем для еліптичної кривої $GF(2^m)$

Передбачено множення двох елементів A і B за модулем третього елемента P, причому всі елементи представлено як і для випадку додавання. Множення виконується одночасно з обчисленням модуля. Схематично перемножувач за модулем наведено на рис. 13. Результати імплементації вищевказаних методів дозволили досягти виконання операції додавання двох точок на еліптичній кривій $GF(2^{163})$ протягом часу 3,05 мкс. Результати проведених досліджень доводять, що не повинна залишатися поза увагою науковців наявність ще однієї можливості реалізації методу паралельних обчислень, яка базується на використанні процесорів GPU.

Показано, що алгоритм LSB можна застосувати із задовільними результатами також для виконання операції множення елементів в програмованих матрицях FPGA (рис. 14).

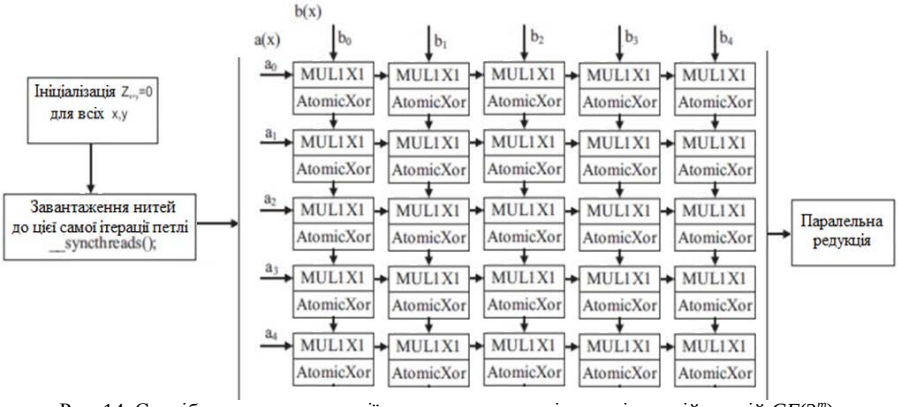

Рис. 14. Спосіб виконання операції множення елементів на еліптичній кривій $GF(2^m)$ із використанням алгоритму LSB

Це підтверджено результатами випробувань, проведених порівнюючи швидкодію функціонування операційних пристроїв, побудованих на основі процесорів GPU та імплементацій, здійснених в середовищі програмованих матриць FPGA.

Отримали подальший розвиток *структурно-аналітичні моделі обчислювачів на еліптичних кривих у пристроях ІУС,* які дозволяють досягти мінімальних розмірів еліптичних кривих, що можуть бути застосовані для забезпечення необхідного рівня доступності ІУС БСМ. В основу моделі для виконання основних операцій на еліптичних кривих покладемо продуктивність P для оцінювання стану ІУСЕК, базованих на пристроях, що реалізують криптографічні операції на еліптичних кривих, та введемо наступні позначення: p_{wwf} – ймовірність безвідмовної роботи ІУСЕК; f_s – функція живучості, тобто мінімальна підмножина функцій ІУСЕК з найвищим пріоритетом,

виконання яких необхідно для того, щоб система не перейшла до небезпечного стану; P_s – продуктивність ІУСЕК, необхідна для виконання функцій живучості та нижче за яку виникає аварія; m – загальна кількість функцій живучості; p_{ds} – ймовірність переходу ІУСЕК на часовому інтервалі t до небезпечного стану; n – загальна кількість процесорних пристроїв в ІУСЕК; $n_{КПЕК}$ – кількість пристроїв КПЕК у системі, що виконують криптографічні операції на еліптичних кривих; x – вектор стану ІУСЕК; X_{ds} – множина, яка відповідає небезпечним станам ІУСЕК; α_i та α_j – компоненти вектора x, які відповідають стану i-го процесорного пристрою та j-го КПЕК ($\alpha_i = \alpha_j = 0$ – для відмови; $\alpha_i = \alpha_j = 1$ – для працездатності); P_i та P_j – продуктивність i-го процесорного пристрою та j-го КПЕК; P_x – продуктивність ІУСЕК в стані, що відповідає вектору x.

У результаті отримуємо модель живучості ІУСЕК БСМ, представлену формулами:

$$P_x = \sum_{i=1}^{n-n_{КПЕК}} \alpha_i P_i + \sum_{j=1}^{n_{КПЕК}} \alpha_j P_j \le P_s ,$$

$$p_{ds}(t) = \sum_{x \in X_{ds}} p_x(t)\Big|_{\forall x \in X_{ds}} ,$$

де $p_x(t)\Big|_{\forall x \in X_{ds}} = \prod_{i=1}^{n} p_i^{\alpha_i}(1-p_i)^{1-\alpha_i} - \prod_{j=1}^{n-n_{КПЕК}} p_j^{\alpha_j}(1-p_j)^{1-\alpha_j}$, звідки можна обчислити ймовірність переходу ІУСЕК БСМ в часовому інтервалі t до небезпечного стану, викликаного зниженням її продуктивності внаслідок відмов КПЕК. Основна особливість моделі полягає в заміні операції модулярного множення великих цілих чисел додаванням за модулем, яке проводиться за допомогою базисів Крестенсона, а також застосуванням паралельного додавання чисел, що дає змогу прискорити виконання операції на відміну від традиційного підходу. Паралельне сумування полягає на поділі цих великих чисел на слова (довжина слова відповідає розміру регістра процесора), розмір яких дає змогу безпосередньо виконати операцію додавання за допомогою вбудованих в процесори суматорів з використанням стандартних типів даних. Віднімання чисел також виконується паралельним способом.

Розглянемо два числа X та Y і модуль n: $Z = X*Y \bmod n$. Модель передбачає подання чисел X і Y у вигляді двійкових послідовностей:

$$X = x_{r-1}2^{r-1} + x_{r-2}2^{r-2} + x_i 2^i + \ldots + x_1 2^1 + x_0 2^0 ,$$

$$Y = y_{r-1}2^{r-1} + y_{r-2}2^{r-2} + y_j 2^j + \ldots + y_1 2^1 + y_0 2^0 .$$

Для визначення результату їх множення побудовано матрицю, представлену в табл. 4, де $m_{ij} = 2^{i+j} / \bmod n$.

Таблиця 4

Матриця Крестенсона

…	…	…	…	…	2^{r-1}
…	$(2^{i+i}) \bmod n$	…	…	…	2^i
…	…	…	…	…	|
…	…	…	$(2^{1+1}) \bmod n$	…	2^1
…	…	…	…	…	2^0
2^{r-1}	2^j	…	2^1	2^0	

Добуток чисел X та Y можна отримати так: $X \cdot Y \bmod n = \sum_{s,k=1}^{r-1} m_{sk} \bmod n$, де $x_s, y_k = 1$, тобто m_{sk} знаходиться на перетині стовпця і рядка, для яких відповідні x_i

та y_j дорівнюють 1. Числа, які записано в таблицю, є меншими, ніж заданий модуль *n*. Сума чисел рядка або стовпця є меншою від подвійного модуля, тому для обчислення за модулем достатньо порівняння та віднімання за модулем. Виходячи з цього, надалі створено модель, за допомогою якої проводяться обчислення із використанням стандартних типів даних, що обслуговуються безпосередньо даним процесором.

Алгоритм обчислень зводиться до наступного:

1. Генерування матриці Крестенсона згідно з табл. 3 та її запис у тривимірному масиві (рис. 1), де третій вимір залежить від кількості слів, на які було поділено числа. Таким чином побудовано третій вимір масиву.

2. Додавання за модулем *n* рядків матриці Крестенсона відповідно до виразу $\sum_{i;\,j=1}^{j=r-1} m_{sk} \bmod n$. Додавання рядків відбувається в паралельному режимі, тобто в тому самому часі здійснюється додавання кожного з *i* рядків.

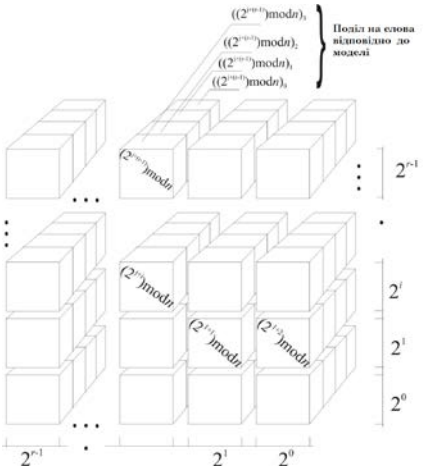

Рис 15. Алгоритм запису матриці Крестенсона в моделі

Розглянуте додавання відповідає методу, описаному в попередньому розділі. Єдина модифікація полягає у додаванні на першому кроці не двох слів, а *r-1* слів. Обчислення за модулем для кожного рядка лінії здійснюється відповідно до рис. 15.

Додавання вектора, наведеного на рис. 17, здійснюється згідно зі способом, подібним до додавання рядка, представленого вище. Єдиною відмінністю є те, що додаються всі елементи вектора. У результаті виконання цієї операції одержується добуток чисел *X* та *Y* за модулем *n*.

Рис. 16 ілюструє концепцію додавання рядків матриці. Результатом цієї операції є вектор розміру *r-1* сум для кожного рядка, що показано на рис. 16.

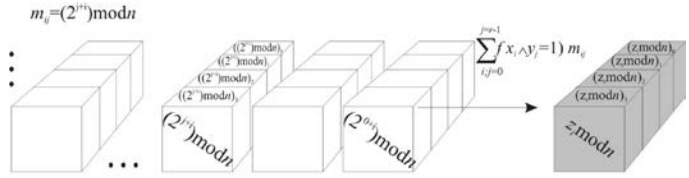

Рис. 16. Концепція додавання рядків матриці Крестенсона

Створено апаратний засіб, який реалізує «шляхи пошуку» з модифікацією трьох стартових сталих у реалізації ро-методу Полларда, а також його паралельну версію. Проведено аналіз впливу модифікованих моделей та технологій обчислень, реалізованих на основі базисів Радемахера-Крестенсона, на живучість ІУСЕК БСМ шляхом *розв'язання дискретного логарифма на еліптичній кривій над полем GF(*2^m*),* що дає можливість будувати високопродуктивні криптографічні пристрої на еліптичних кри-

вих і пришвидшити виявлення криптоаналітичних атак на ІУС БСМ. Здійснена реалізація створених моделей та апаратних імплементацій, які основані на базисах Крестенсона і паралельному додаванні та за допомогою яких впроваджено ро-метод Полларда розв'язання дискретного логарифма, завдяки чому побудовано продуктивніші шифрувальні системи, а також забезпечено ефективність розв'язання дискретного логарифма. Визначено області і технології, в яких застосування розроблених моделей, алгоритмів та методик зумовлює підвищення ефективності обчислень на кривих *GF(p)*. Такими середовищами є структури програмованих матриць FPGA, комп'ютерні системи з багатоядерними процесорами чи багатопроцесорні сервери та комп'ютерні кластери, а також системи з архітектурою CUDA NVIDIA.

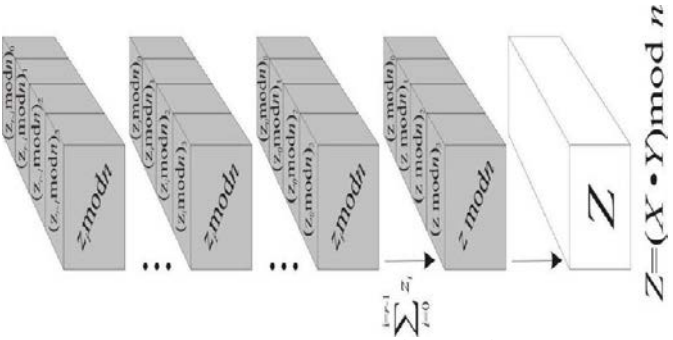

Рис. 17. Додавання вектора суми рядків матриці Крестенсона

Проведений аналіз свідчить, що *модель суматора точок на еліптичній кривій* може бути побудована з одинадцяти незалежних множників, двох суматорів та п'яти перемножувачів. Такий спосіб може виявитися неможливим для фізичної реалізації суматора в програмованих матрицях, оскільки для побудови такої складної системи не вистачило б необхідної логіки. Другий спосіб полягає у використанні логічного пристрою, який керує виконанням операцій в потрібній послідовності, як це показано на рис. 18.

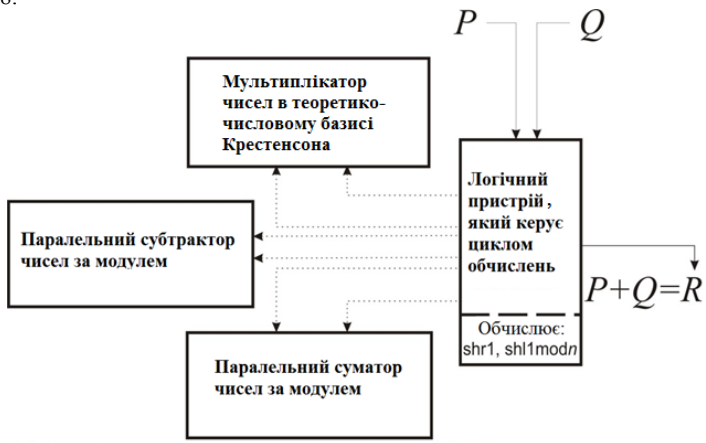

Рис.18. Модель суматора точок на еліптичній кривій

Крім цього, цей пристрій керування виконує операції правого та лівого зсуву бітів shl1 і shr1, що відповідає множенню та діленню даного числа на 2, а також є тривіальним за рахунок використання чисел у вигляді двійкових векторів. Слід звернути увагу на припущення, яке було прийняте при створенні моделі та передбачає, що суматор і перемножувач є незалежними пристроями або процесорами, які можуть працювати незалежно. Виходячи з цього, модель суматора точок схематично може бути представлено в спосіб, як це наведено на рис. 18.

Для побудови *апаратної моделі додавання точок на еліптичній кривій GF(p)* використано складові фізичних моделей, запропонованих у попередніх розділах. Обидва блоки апаратної моделі для відповідної складової криптографічного пристрою ІУСЕК спроектовано таким чином, що працюють на даних того самого типу, зокрема як вхідні, так і вихідні дані мають тип Std_Logic_Vector, що дозволяє уникнути труднощів виконання перетворень під час конверсії.

Операційний пристрій додавання точок, що показаний на рис. 19, завантажує числа у вигляді двійкових векторів, причому вектори *a* та *b* є відповідними координатами точки *P*, а вектори *c* та *d* – це координати точки *Q*. Тоді як сума *R* вивантажується у вигляді двох векторів *x* та *y*. Операційний пристрій додавання точок описано за допомогою компонента gfmkadd_p, а саме:

```
entitygfkadd_pisport(
a, b, c, d : in std_logic_vector(91 downto 0);
clk, rst, next : in std_logic;
x, y : out std_logic_vector(91 downto 0));
end gfkadd_p;
```

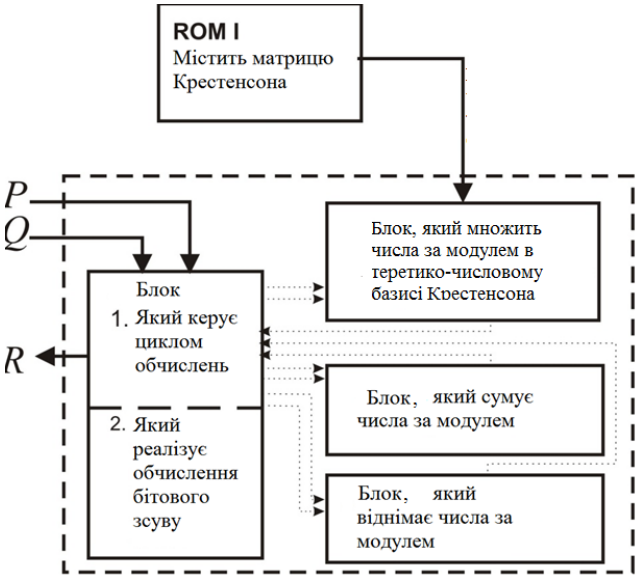

Рис. 19. Модель апаратного суматора точок

Обчислення результату множення та ділення на 2, тобто зсув бітів для випадку запису у вигляді векторів, є тривіальним і згідно з визначенням таких дій полягає у зсуві значень окремих бітів. Обчислення модуля для випадку множення здійснюється відповідно до попереднього опису.

Модель обчислень дискретного логарифма із застосуванням теоретико-числових базисів Радемахера-Крестенсона та паралельного додавання на підставі ро-методу Полларда зображено на рис. 20, апаратно-програмна модель паралельної реалізації ро-методу Полларда з використанням теоретико-числового базису Крестенсона наведена на рис. 21.

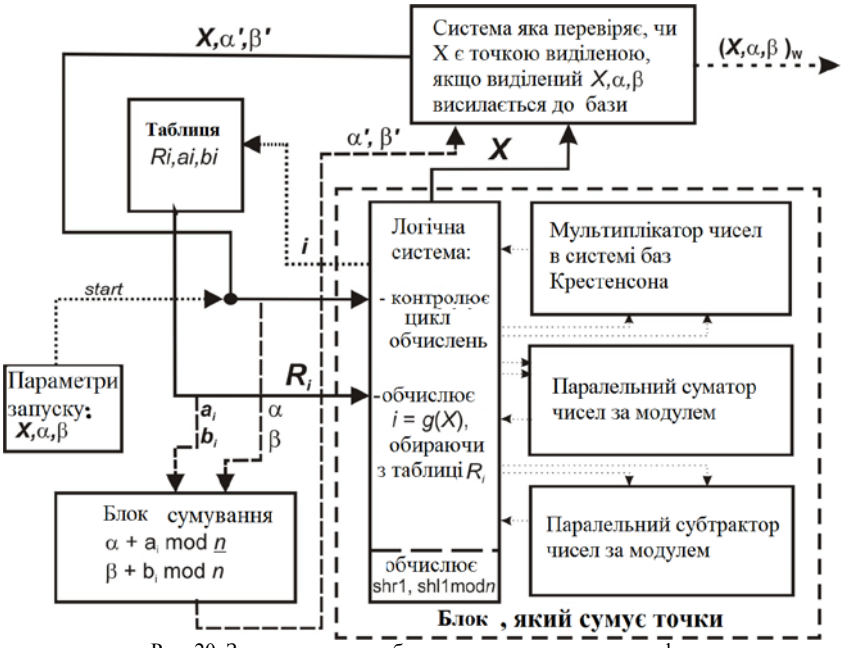

Рис. 20. Загальна модель обчислень дискретного логарифма

Характерна особливість моделі паралельної реалізації ро-методу Полларда полягає у застосуванні багатьох шляхів випадкового блукання, що здійснюються паралельно. Суть його функціонування зводиться до використання багатьох компонентів, які реалізують свої власні «шляхи пошуку» та записують дані до спільної бази даних. Усі компоненти, які здійснюють «шляхи пошуку», отримують та завантажують однакові таблиці точок R_i та таблиці значень a_i і b_i.

Побудова кожного компонента є ідентичною, єдина відмінність полягає в наборі трьох стартових параметрів. Це дає змогу побудувати продуктивні криптографічні пристрої на еліптичних кривих ECCD ІУСЕК та підвищити ефективність розв'язання дискретного логарифму, а тим самим пришвидшити виявлення криптоаналітичних кібератак.

П'ятий розділ присвячено експериментальним дослідженням запропонованих у роботі методів та моделей забезпечення захисту БСМ.

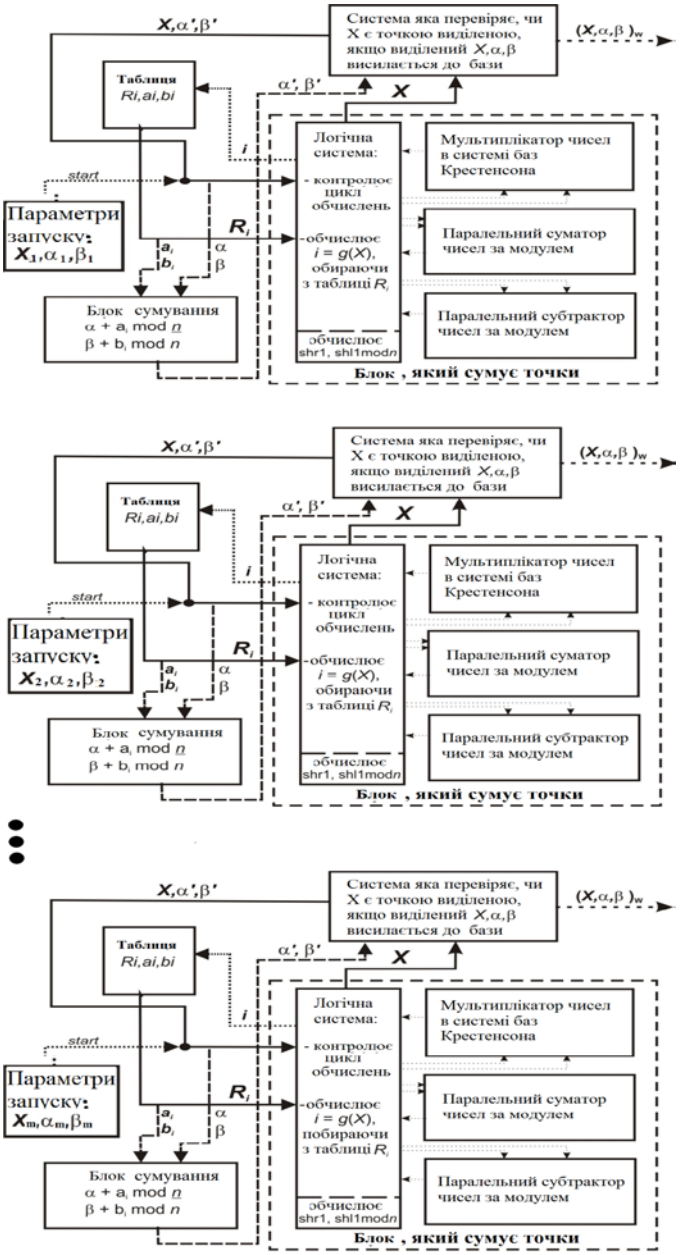

Рис. 21. Апаратно-програмна модель паралельної реалізації ро-методу Полларда для БСМ з використанням теоретико-числового базису Крестенсона

Проведено симуляційні дослідження методу відновлення повідомлення для відслідковування DoS-атак в середовищі TRMSim-WSN. Промодельовано засіб локалізації DoS-атак на основі використання методу імовірнісного маркування пакетів на стійкій БСМ до DoS-атак, який проілюстровано на рис. 22.

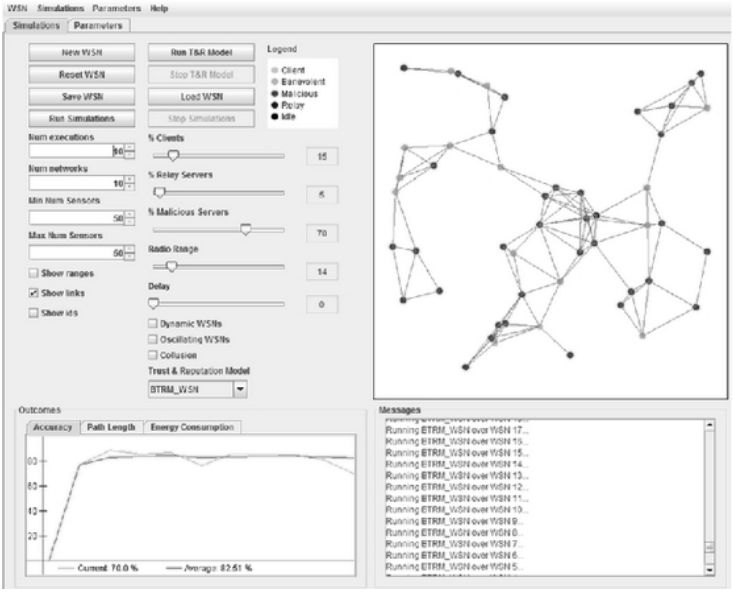

Рис. 22. Результати комп'ютерного моделювання в середовищі TRMSim-WSN

Проведені компіляційні дослідження показують, що за допомогою запропонованого методу імовірнісного маркування пакетів відсіюються немарковані пакети в межах 140-170 с. Отже, цей метод можна застосувати для покращення захисту БСМ від DoS-атак в заходах протидії, які ґрунтуються передусім на перевірці характерних номерів портів та аналізі мережевого трафіка з використанням аналізаторів, вбудованих в системи IDS, а також на блокуванні доступу до Інтернету пакетам з підробленою адресою джерела та пакетам, що надані до даної БСМ з IP – адресою за межами цієї БСМ. Можна також визначити власні правила, на підставі яких відома програма Snort, наприклад, виявлятиме несанкціонований трафік в БСМ з повідомленням про атаки відмови в обслуговуванні типу DDoS, перезапускатиме або блокуватиме підозрілі з'єднання. Результативним є поєднання запропонованого методу імовірнісного маркування пакетів з іншим програмним захистом від атак DDoS, зокрема такими програмами, як ZombieZapper, Wtrinscan або DDoSPing.

Здійснено симуляцію роботи моделей та технологій обчислень, запропонованих в попередньому розділі. Проведено аналіз симуляції роботи апаратно-програмних систем для розв'язування дискретного логарифма, який є підставою для оцінювання живучості ІУСЕК. На основі результатів розв'язування дискретного логарифма для кривих різних розмірів здійснено оцінювання живучості ІУСЕК БСМ.

Схему алгоритму додавання чисел X та Y за модулем n наведено на рис. 23. Обчислення суми двох чисел, яке складається з чотирьох слів, вимагає виконання семи

кроків. Під час додавання проводиться також операція паралельного віднімання. При цьому слід відзначити, що порівнюється не ціле число, а окремі слова, щоб на підставі порівняння всіх слів здійснити порівняння чисел. Паралельне сумування чисел в поєднанні з відніманням за модулем дозволяє зменшити кількість кроків, які повинні бути виконані для того, щоб додати числа за модулем.

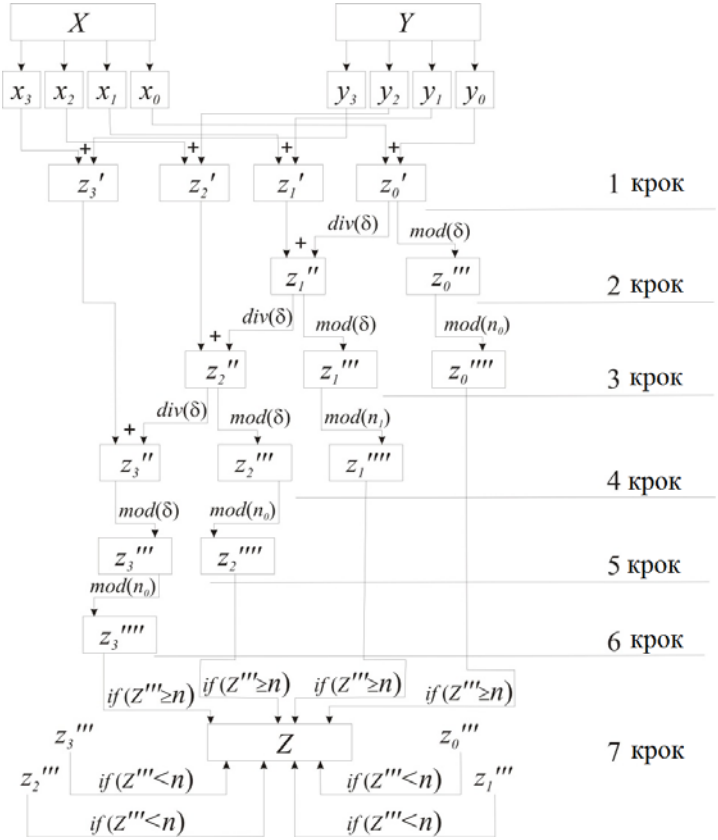

Рис. 23. Схема алгоритму додавання двох чисел за модулем *n*

Проаналізовано випадок зміни складності обчислень для більших чисел, які поділено не на чотири, а на п'ять, шість і т.д. слів. Доведено, що якщо в схему алгоритму, зображену на рис.23, ввести додатково одне слово, то тоді потрібно збільшити кількість кроків на два, модифікуючи п'ятий крок, і після нього додати додатково два кроки. Звідси випливає, що для випадку поділу числа на п’ять слів кількість необхідних кроків потрібно збільшити до дев'яти.

Аналіз роботи суматора, реалізованого в програмованих структурах системи, здійснено на підставі результатів досліджень обчислювальних засобів, побудованих на програмованих матрицях FPGA. Логічний синтез апаратної моделі, виконаної на про-

грамованій матриці фірми Altera типу Stratix III, дав змогу забезпечити робочу частоту на рівні 366 МГц.

Робота на такій частоті дозволила виконати 45,75 млн. додавань за секунду для чисел, які складаються з чотирьох слів. Швидкодія сумування для числа, яке складається з п'яти слів, становить 35 млн. додавань за секунду для частоти 350 МГц, а для шести слів – 27,9 млн. додавань. Можна зауважити майже лінійне зменшення швидкості обчислень в залежності від збільшення кількості слів, що є важливим для забезпечення живучості ІУСЕК. Протестовано побудовану в третьому розділі модель перемноження великих чисел. Схема алгоритму, зображеного на рис. 5, відображає дії, необхідні для обчислення добутку двох чисел за модулем, виконуючи відповідні сумування елементів матриці Крестенсона. Проведено симуляцію для апаратної моделі, яку передбачено для обчислень, що здійснюються на великих числах. Відповідне генерування і синтез операційного пристрою проведено для програмованої матриці FPGA типу Stratix III. При цьому отримано тактову частоту на рівні 44 МГц. Додавання значень всіх рядків матриці здійснюється паралельним способом, причому обчислення суми рядків отримується протягом виконання семи кроків. Сумування рядка здійснюється аналогічно тому, що описано попередньо для випадку суматора, проте єдиним винятком є сумування на першому кроці багатьох чисел. На наступному кроці виконано сумування вектора, що показаний («затемненим») на рис. 24, також аналогічним чином протягом 7 кроків. Для того щоб обчислити добуток двох чисел, поділених на чотири слова, потрібно виконати 14 кроків.

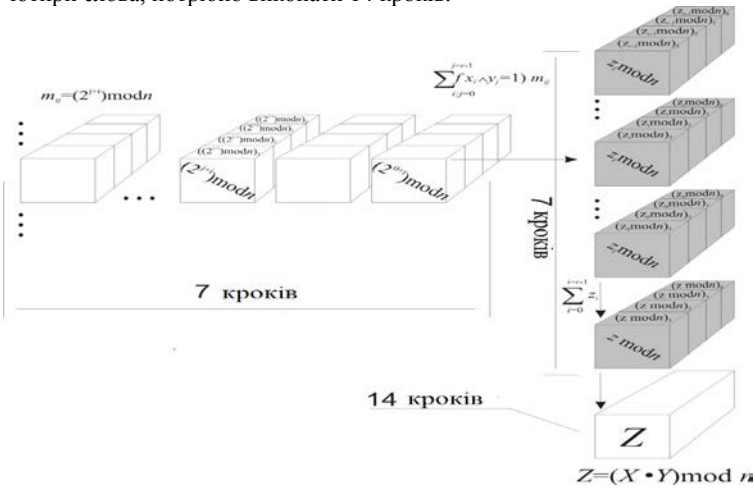

Рис. 24. Схема алгоритму виконання операції множення в базисах Крестенсона

Проведено аналіз роботи суматора точок на еліптичній кривій із застосуванням обчислень в базисах Радемахера-Крестенсона та паралельного додавання. Додавання точок у суматорі складається із виконання операцій додавання та множення чисел. Сумування точок у змішаному поданні зводиться до виконання наступних операцій над числами: 11-ти множень, 2-ох додавань, 5-ти віднімань та 2- ох бітових зсувів.

Вся операція сумування точок змішаним способом може бути здійснена протягом 11 кроків, застосовуючи відповідний підхід до вибору порядку обчислень. Симуляцію процесів здійснено на апаратній моделі суматора точок *GF(p)*. Симуляцію проведено

для програмованої матриці FPGA типу Stratix III EP3SL150F1152I4SL. Результати симуляції дозволили отримати тактову частоту на рівні 44 МГц. Проведено аналіз функціональних характеристик суматора точок на еліптичній кривій при реалізації алгоритму шифрування Ель-Гамаля в компонентах ІУСЕК. У табл. 5 наведено результати роботи системи, основаної на традиційних підходах до додавання точок на еліптичній кривій (для файлу об'ємом 1024 кБ).

Таблиця 5

Швидкість шифрування файлу методом Ель-Гамаля в компонентах ІУСЕК із використанням стандартних алгоритмів додавання точок на еліптичній кривій

Крива *GF*(*p*)	89	97	109	131	163	191
Час, *с*	104	131	145	243	339	440

Симуляція алгоритму Ель-Гамаля, до якого було впроваджено алгоритм додавання точок на еліптичних кривих на основі базису Крестенсона, дала змогу отримати для тих же кривих час шифрування, значення якого наведені у табл. 6.

Таблиця 6

Швидкість шифрування файлу методом Ель-Гамаля в компонентах ІУСЕК із використанням стандартних алгоритмів сумування точок на еліптичній кривій на основі системи залишків Радемахера-Крестенсона

Крива *GF*(*p*)	89	97	109	131	163	191
Час, *с*	37	40	43	79	111	127

З аналізу даних таблиць можна зробити висновок, що введення додавання на основі базисів Крестенсона у відповідному середовищі ІУСЕК БСМ збільшує швидкість шифрування приблизно вдвічі порівняно з традиційним підходом.

Здійснено аналіз живучості ІУС БСМ, базуючись на розв'язанні дискретного логарифма модифікованим ро-методом Полларда. Симуляцію роботи здійснено на базі програмованої матриці типу Stratix III EP3SL150F1152I4SL. У табл. 7 наведено результати дослідження процесів, які протікають у апаратно-програмній моделі для ЕК різного розміру.

Таблиця 7

Кількість ітерацій алгоритму для різних кривих *GF(p)*

Крива *GF(p)*	69	92	115	138	161	184
Кількість ітерацій / с	321678,3	235294,1176	186147,2	149090,9	125391,8	107438

Для визначення середнього очікуваного часу знаходження дискретного логарифма за допомогою ро-методу Полларда $\sqrt{\pi n}/2$, в табл. 8 показано приблизний прогнозований час обчислення дискретного логарифма для еліптичних кривих різного розміру.

Таблиця 8

Прогнозований час знаходження дискретного логарифма в компонентах ІУСЕК для різних еліптичних кривих *GF(p)*

Крива	*GF(69)*	*GF(92)*	*GF(115)*	*GF(138)*	*GF(161)*	*GF(184)*
Час, дні	0,84	3295	$12*10^{6}$	$4,2*10^{10}$	$1,7*10^{14}$	$5,8*10^{17}$

Проведено дослідження процесів в апаратній моделі реалізації ро-методу Полларада для підтримки системи криптоаналізу, спрямованого на відповідні компоненти ІУСЕК БСМ. Цю модель застосовано складовим компонентом для підтримки функці-

онування криптографічної системи, що ґрунтується на програмному рішенні. Процеси як у апаратно-програмній, так і програмній моделях симульовано в різних середовищах. Одні з них – процесорами Itanium 2 тактової частоти 1,5 ГГц, інші – на основі мікропроцесора Pentium IV 2,8 ГГц. Результати роботи, які ілюструють наведені в табл. 9 дані, відносяться до кількості ітерацій, необхідних для реалізації одного «шляху пошуку». Крім цього, в таблиці додатково подано кількість ітерацій для апаратного рішення на базі програмованої матриці FPGA.

Таблиця 9

Залежність кількості ітерацій алгоритму для різних кривих *GF(p)* в залежності від обчислювальних середовищ в ІУСЕК

Обчислювальне середовище \ крива *GF*(*p*)	69	92	115	138	161	184
Itanium2	109169	67142	53791	47921	42052	32543
Pentium IV	117496	73157	56045	48659	41274	31235
FPGA	321678	235294	186147	149091	125392	107438

Як випливає з даних, наведених в табл. 8, швидкість обчислення на заданій еліптичній кривій при застосуванні апаратно-програмної моделі збільшується принаймні втричі в порівнянні з обчисленнями, виконаними в програмній моделі. Застосування апаратної моделі обчислень з використанням базисів Крестенсона дає реальне збільшення швидкості обчислень на еліптичній кривій і значно пришвидшує продуктивність ро-методу Полларда. Реалізація алгоритму паралельного блукання полягає на створенні J компонентів, за допомогою яких реалізуються окремі «шляхи пошуку». Для випадку впровадження до обчислень більшої кількості компонентів ІУСЕК, що реалізують шляхи випадкового блукання, кількість ітерацій алгоритму збільшується пропорційно до кількості впроваджених компонентів. Розглянемо випадок заімплементування моделі, яка дає змогу реалізувати паралельний ро-метод Полларда, на кластері програмованих матриць FPGA типу COPACOBANA. В результаті проведених досліджень визначено, що для застосованих 120 «шляхів пошуку», які виконуються паралельно, є можливість оцінити час, необхідний для розв'язку дискретного логарифма для кривих *GF(p)* різного розміру (табл. 10). Продуктивність обчислювальної системи визначається кількістю ітерацій за секунду та для зазначеного рішення зростає до значень, наведених в табл. 10.

Таблиця 10

Продуктивність обчислювальної системи для різних кривих *GF(p)* під час реалізації 120 шляхів пошуку

Крива *GF*(*p*)	69	92	115	138	161	184
Кількість ітерацій / с	38601398	28235294	22337662	17890909	15047022	12892562

Отримані результати досліджень дали змогу оцінити час, який необхідний для розв'язку дискретного логарифма для кривих *GF(p)* різного розміру при використанні 120 «шляхів пошуку» (табл. 11)

Таблиця 11

Прогнозний час знаходження дискретного логарифма для різних еліптичних кривих *GF*(p) при 120 програмувальних компонентах

Крива	*GF*(69)	*GF*(92)	*GF*(115)	*GF*(138)	*GF*(161)	*GF*(184)
Час, дні	0,007	27	100790	$3{,}5*10^{8}$	$1{,}4*10^{12}$	$4{,}9*10^{15}$

Беручи до уваги кібератаку на алгоритм, забезпечення живучості інтегрованих ІУС на основі еліптичних кривих *GF(p)* залежить від розміру застосованої ЕК. Мінімальний час, протягом якого БСМ забезпечено захист і цілісність даних під час кібератаки, наведено в табл. 11.

У **додатках** вміщено акти впровадження результатів дисертаційної роботи та фрагменти кодів програм, що відображають практичну частину дисертаційного дослідження.

ВИСНОВКИ

Результатом виконаної роботи є вирішення актуальної науково-технічної проблеми створення нових методів та моделей захисту безпроводових сенсорних мереж та їх компонентів від різного роду кібератак, спрямованих на порушення конфіденційності, цілісності та доступності їх інформаційних ресурсів.

У процесі виконання дисертаційної роботи отримані такі вагомі результати:

1. Проведено аналіз безпроводових сенсорних мереж (архітектури, протоколів), який вказав на їх уразливість до різного класу DoS-атак, а також до інших кібератак, що порушують конфіденційність і цілісність інформаційних ресурсів цих мереж. Цей аналіз дозволив сформулювати завдання щодо розробки ефективних методів та моделей забезпечення захисту безпроводових сенсорних мереж.

2. Запропоновані нові математичні моделі інформаційних структур ймовірності загроз визначеного класу DoS-атак, які за рахунок сформованої базової множини характерних показників і відповідних вагових коефіцієнтів та взаємозв'язків визначених матриць активності мережі і встановленої інтенсивності впливу різних класів кібератак, дозволяють оцінювати рівень впливу показників кіберзагроз щодо безпроводових сенсорних мереж.

3. Отримала подальший розвиток модель захищеної комунікації «клієнт-сервер-шлюз-вузол», яка за рахунок сформованої базової множини залежностей можливих шляхів «точка доступу → точка призначення» за врахуванням впливу величин ймовірностей компрометації вузлів і вирахуваних вагових коефіцієнтів, дає можливість ідентифікувати клас реалізованої кібератаки на безпроводові сенсорні мережі та визначити відповідні заходи протидії.

4. Отримав подальший розвиток метод відновлення повідомлення, який за рахунок процедури підстановочного сортування *b*-бітних блоків лексикографічними значеннями, інтерпретації значення відповідно до формату зберігання блоків в IP-заголовку, *i*-індексним впорядкуванням контрольних сум та двохфазової відновлювальної схеми, дає можливість на 11% ефективніше забезпечити цілісність повідомлень в умовах реалізації відповідних кіберзагроз безпроводовим сенсорним мережам.

5. Удосконалено метод ймовірнісного маркування пакетів у безпроводовій сенсорній мережі, який за рахунок доповнення пакетів вектором ідентифікації номерів вузлів (записаних в його координатах), правила формування ймовірності успішного міжвузлового переходу, процедури обмеження вибірки пакетів за мінімаксним критерієм та запропонованого методу відновлення повідомлення, дозволяє здійснювати моніторинг безпроводових сенсорних мереж та відстежувати джерела кібератак точніше на 17%.

6. Отримали подальший розвиток структурно-аналітичні моделі забезпечення живучості інформаційно-управляючих систем безпроводових сенсорних мереж, які за рахунок побудованого направленого графу інформаційно-технічних станів $MS_{ПС}$, $MS_{ЧП}$, $MS_{НБС}$ і $MS_{НС}$ з комбінацією кодованих показників дефектів зовнішніх впливів за ознаками ймовірності та детермінованості, дають можливість здійснювати вибір

ефективної стратегії обслуговування гарантоздатної інформаційно-управляючої системи за показниками готовності технічного та інформаційного станів відносно сформованої множини дефектів, що впливають на базову характеристику безпеки – доступність.

7. Удосконалено технології обчислень на еліптичних кривих, які за рахунок запропонованого способу заміни операцій множення за модулем в алгоритмі Крестенсона еквівалентним перетворенням на основі операції додавання з відображенням на відповідну обчислювальну архітектуру, дозволяють забезпечити високу швидкість криптографічної обробки даних у пристроях інформаційно-управляючих систем безпроводових сенсорних мереж.

8. Отримали подальший розвиток структурно-аналітичні моделі обчислювачів на еліптичних кривих у пристроях інформаційно-управляючих систем, які за рахунок запропонованих структурно-аналітичних моделей забезпечення живучості та реалізації паралельних обчислень на основі теоретико-числових базисів Радемахера-Крестенсона в розроблених обчислювальних архітектурах, дозволяють досягти мінімальних розмірів еліптичних кривих, що можуть бути застосовані для забезпечення необхідного рівня доступності інформаційно-управляючих систем безпроводових сенсорних мереж.

9. Отримали подальший розвиток структурно-аналітичні моделі обчислення дискретного логарифму для кривих над полем $GF(2^m)$, які за рахунок використання розроблених моделей обчислювачів на еліптичних кривих і з урахуванням теоретико-числових базисів Радемахера-Крестенсона для паралельного сумування чисел великої розрядності та паралельної реалізації операцій на підставі ро-методу Полларда, дають можливість будувати високопродуктивні криптографічні пристрої на еліптичних кривих і збільшити швидкість виявлення криптоаналітичних атак, що впливають на конфіденційність інформаційно-управляючих систем безпроводових сенсорних мереж, мінімум у 10^2 разів.

10. Розроблено програмні засоби захисту інформації і рекомендації щодо практичного застосування запропонованих методів і моделей у безпроводових сенсорних мережах. На базі отриманих теоретичних результатів створено спеціалізоване програмне забезпечення виявлення різного класу DoS-атак на безпроводові сенсорні мережі.

11. Створено дві апаратно-програмні системи для інформаційно-управляючих систем:

– перша працює на програмованих матрицях FPGA та ПК, дія якої ґрунтується на основі модифікованої моделі обчислень, причому на підставі досліджень побудованого суматора точок на програмованих матрицях FPGA Stratix III EP3SL150F1152I4SL одержано збільшення швидкості шифрування методом Ель-Гамаля приблизно втричі в порівнянні до традиційного підходу сумування точок;

– друга реалізує ро-алгоритм Полларда, використовуючи технологію обчислень на ТЧБ Крестенсона, та ґрунтується на аналогічних апаратних засобах. За результатами дослідження роботи паралельної системи на декількох програмованих матрицях FPGA для розв’язання логарифма для ЕК різного розміру та проведених вимірювань визначено, що застосування «шляхів пошуку» алгоритму, який реалізовано на одній програмованій матриці FPGA, зумовлює трикратне збільшення швидкості роботи алгоритму в порівнянні з системою, побудованою на базі процесора Itanium 2.

12. Результати дисертаційної роботи впроваджені та отримали використання у навчальному процесі Університету в Бєльсько-Бялій (Польща) (акт впровадження від 24 листопада 2015 року) та Національного авіаційного університету (акт впровадження від 18 травня 2016 року) згідно з Угодою про співробітництво між університетами №336 від 15 травня 2014 року.

ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Bezpieczeństwo bezprzewodowych sieci spontanicznych i sensorowych / M. Aleksander, J. Kinach, G. Litawa, W. Karpiński, A. Chominczuk // Bezpieczeństwo informacji / edited by M. Karpiński. – Warszawa: Wydawnictwo Pomiary Automatyka Kontrola. – 2012. – R. 2. – S. 82-129. – ISBN 978-83-930505-3-6. (розділ у монографії).

2. Aleksander M., Litawa G. Bezpieczeństwo kryptosystemów opartych na krzywych eliptycznych / M. Aleksander, G. Litawa // Bezpieczeństwo informacji / edited by M. Karpiński. – Warszawa: Wydawnictwo Pomiary Automatyka Kontrola. – 2012. – R. 5. – S. 183-196. – ISBN 978-83-930505-3-6 (розділ у монографії).

3. Reliability basics of information systems / edited by A. Petrov; authors A. Petrov, V. Khoroshko, L. Scherbak, A. Petrov, M. Aleksander. – Kraków: AGH University of Sceince and Technology Press, 2016. – 246 p. – ISBN: 978-83-7464-859-2 (монографія).

4. Karpinski M., Aleksander M., Litawa G., Karpinskyi V. The security of data transmission over telecommunication networks based on advanced data encryption methods // Electrical Review. – 2009. – 85 (4). – P. 19-21 (Scopus).

5. Kurytnik I., Karpinski M., Aleksander M., Mikulski M. Algorithms of topology building in the Wireless Sensor Networks // Electrical Review. – 2009. – 85 (4). – P. 22-24 (Scopus).

6. Palamar M., Aleksander M., Pohrebennyk V., Strembickyy M. Synthesis and Optimization of Neural Network Parameters for Control Non-linear Objects // Electrical Review. – 2014. – 90 (5). – P. 207-210 (Scopus).

7. Aleksander M.B., Dubchak L., Chyzh V., Naglik A., Yavorski A., Yavorska N. Software-defined networking Technologies Implementation in Wireless Sensor Networks; The 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 24-26 September 2015, Warsaw, Poland. – P. 448-452 (Scopus).

8. Aleksander M., Litawa G., Karpinskyi V. Distributed computing system which solve an elliptic curve discrete logarithm problem; 10th International Conference The experience of designing and application of cad systems in microelectronics, 24-28 February 2009, Polyana, Ukraine. – P. 378-380 (Scopus).

9. Аналіз загроз та механізмів забезпечення інформаційної безпеки в сенсорних мережах / О. Корченко, М. Александер, Р. Одарченко, А. Наджі, О. Петренко // Захист інформації. 2016. – Т. 18, №1. – С. 48-56.

10. Дослідження вразливостей сенсорних підмереж архітектури інтернету речей до різних типів атак / М. Александер, О. Корченко, М. Карпінський, Р. Одарченко // Безпека інформації. 2016. – Т. 22, №1. – С. 12-19.

11. Aleksander M., Karpinskyy M., Litawa G. Calculation of GF (p) Elliptic Curves in FPGA // Computing. – 2011. – Vol. 10. – Issue 2. – P. 91-96.

12. Functional safety and survivability of information control elliptic-curve-based systems:models and methods / M. Aleksander, M. Karpinski, G. Litawa // Безпека інформації. – 2013. – Т. 19, № 1. – С. 51-56.

13. Karpinski M., Aleksander M., Litawa G., Karpinskyi V. Cryptographic system security level based on elliptic curves // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2008. – № 8 (126). – С. 94-98.

14. Aleksander M., Karpinski M., Litawa G. Implementation and testing of methods parallel computation on elliptic curves GF(p) // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2011. – № 7 (161). – С. 304-310.

15. Minin V., Skopa O., Aleksander M. Binomial model TEST survivability protected information channels // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2012. – № 7. – С. 42-58.

16. Aleksander M., Petrov A., Serhiyenya K. Methods for Troubleshooting of Corporate Network Fault Tolerance // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2012. – № 8. – С. 348-355.

17. Aleksander M., Boldarev A. Research process running applications in the operating system environment Windows // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2013. – № 15 (204), ч. 1. – С. 18-27.

18. Aleksander M.A. Features of Denial-of-Service Attacks in Information Systems / M.A. Aleksander, M.P. Karpinski, U.O. Yatsykovska // Інформатика та математичні методи в моделюванні. – 2012. – Т. 2, № 2. – С. 129-133.

19. Aleksander M., Karpinski M., Litawa G. Implementation in FPGA of Computations on Elliptic Curves GF(p) based on Rademacher-Krestenson's Bases // Інформаційна безпека. – 2012. – № 1 (7). – С. 12-17.

20. Modeling survivable information network / O. Petrov, A. Minin, M. Aleksander, E. Mikvabiya // Інформаційна безпека. – 2013. – № 1. – С. 117-123.

21. Prediction reliability of information systems / M. Aleksander, O. Petrov, A. Minin, L. Scherbak, A. Petrov // Інформаційна безпека. – 2013. – № 2. – С. 123-134.

22. Assessment of the survivability of network information aystems using neural network model / O.S. Petrov, A.V. Mìnìn, M. Aleksander // Інформаційна безпека. – 2013. – № 3. – С. 130-138.

23. Realization of the metod of attacks visualization in wireless sensor networks / M. Aleksander, B. Borowik, P. Evtukh, V. Karpinskyi, M. Karpinski // Вісник Національного університету «Львівська політехніка». Серія: Радіоелектроніка та телекомунікації. – 2012. – № 738. – С. 112-116.

24. Атаки на відмову в обслуговуванні комп'ютерних мереж / М. Карпінський, У. Яциковська, А. Балик, М. Александер // Вісник Національного університету «Львівська політехніка». Серія: Комп'ютерні системи та мережі. – 2014. – № 806. – С. 94-98.

25. Petrov A., Aleksander M., Petrov A. Methods and models of reliable software protection systems // Autobusy. – 2016. – №6. – P. 37-46.

26. Petrov A., Aleksander M., Petrov A. Creating of automated fault-tolerant system based on http anonymizers that allows access to forbidden web-sites // Autobusy. – 2016. – №6. – P. 378-383.

27. Aleksander M.B., Karpiński M., Khlaponin Yu., Kozlovskyi V., Mischenko A. Generalized Algorithm for Synthesis of Protective Coating against Electromagnetic Radiation // Technika Transportu Szynowego. – 2015. – №12. – P. 95-98.

28. Aleksander M.B., Kulyk M., Karpiński M., Khlaponin Yu., Mischenko A. Intelligent Technologies in Information Security Management // Technika Transportu Szynowego. – 2015. – №12. – P. 2357-2360.

29. Tereykovskaya L., Petrov O., Aleksander M. Prospects Of Neural Networks In Business Models // Technika Transportu Szynowego. – 2015. – №12. – P. 1539-1545.

30. Спосіб візуалізації параметрів сигналів інформаційних вузлів: патент на корисну модель № 103955: МПК H04W 12/12 / Александер М.Б., Чиж В.М., Карпінський В.М., Балабан С.М., Карпіньскі М.П.; власники патенту Тернопільський національний технічний університет імені Івана Пулюя (Україна) та Університет в Бєльсько-Бялій. – № u201505858; заявл. 15.06.15; опубл. 12.01.2016, Бюл. № 1. – 6 с.

31. Aleksander M., Karpinski M., Litawa G. Implementation and testing of methods parallel computation on elliptic curves GF(p) // VIII International Science Practical Conference on Information Technologies and Security in Administration (ITSM'2011), September 12-16, 2011, Sevastopol, Crimea, Ukraine. – P. 11.

32. Kurytnik I., Karpinski M., Aleksander M., Mikulski M. Algorithms of topology building in the Wireless Sensor Networks // Proceedings of the 9th International Workshop «Computational Problems of Electrical Engineering» (CPEE'08) (September 16-20, 2008, Alushta (Crimea), Ukraine). – P. 95-97.

33. Karpiński M. Bezpieczeństwo przekazu informacji w sieciach oparte na metodach szyfrowania bazujących na krzywych eliptycznych / M. Karpiński, M. Aleksander, G. Litawa // III Międzynarodowa Konferencja Naukowa z cyklu «Informatyka w dobie XXI wieku», 2009. – P. 1-3.

34. Aleksander M., Karpinski M., Litawa G. Elliptic curve cryptography in security sensor networks // Актуальні питання забезпечення кібернетичної безпеки та захисту інформації: Міжнародна наук.-практ. конф. CICSIS-2015, 25-28 лютого 2015 р.: Збірн. наук. пр. конф. – К.,: Вид-во Європейського ун-ту, 2015. – С. 9-13.

35. Одарченко Р. Аналіз вразливостей архітектури Інтернету речей / Р. Одарченко, М. Александер // Проблеми експлуатації та захисту інформаційно-комунікаційних систем: наук.-практ. конф., 7-9 червня 2016 р.: тези доп. – К., 2016. – С. 117-118.

АНОТАЦІЯ

Александер М.Б. Методи та моделі забезпечення захисту безпроводових сенсорних мереж. – Рукопис.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – Системи захисту інформації. – Національний авіаційний університет, Київ, 2016.

Дисертаційна робота присвячена розв'язанню актуальної науково-практичної проблеми створення нових методів та моделей захисту безпроводових сенсорних мереж (БСМ) та їх компонентів від різного роду кібератак, спрямованих на порушення конфіденційності, цілісності та доступності їх інформаційних ресурсів.

У роботі проведено аналіз БСМ (архітектури, протоколів), який вказав на їх уразливість до різного роду кібератак, що порушують конфіденційність, цілісність і доступність інформаційних ресурсів. Запропоновані нові математичні моделі інформаційних структур ймовірності загроз визначеного класу DoS-атак, які дозволяють оцінювати рівень впливу показників загроз щодо БСМ. Отримала подальший розвиток модель захищеної комунікації «клієнт-сервер-шлюз-вузол», яка дає можливість ідентифікувати клас реалізованої кібератаки на БСМ та визначити відповідні заходи протидії. Отримав подальший розвиток метод відновлення повідомлення, який дає можливість на 11% ефективніше забезпечити цілісність повідомлень в умовах реалізації відповідних кіберзагроз БСМ. Удосконалено метод ймовірнісного маркування пакетів у БСМ, який дозволяє здійснювати моніторинг БСМ та відстежувати джерела кібератак точніше на 17%. Отримали подальший розвиток структурно-аналітичні моделі забезпечення живучості інформаційно-управляючих систем БСМ, які дають можливість здійснювати вибір ефективної стратегії обслуговування гарантоздатної інформаційно-управляючої системи за показниками готовності технічного та інформаційного станів відносно сформованої множини дефектів. Удосконалено технології обчислень на еліптичних кривих, які дозволяють забезпечити високу швидкість криптографічної обробки даних у пристроях інформаційно-управляючих систем БСМ. Отримали подальший розвиток структурно-аналітичні моделі обчислювачів на еліптичних кривих у

пристроях інформаційно-управляючих систем, які дозволяють досягти мінімальних розмірів еліптичних кривих, що можуть бути застосовані для забезпечення захисту інформаційно-управляючих систем БСМ. Отримали подальший розвиток структурно-аналітичні моделі обчислення дискретного логарифму для кривих над полем $GF(2^m)$, які дають можливість будувати високопродуктивні криптографічні пристрої на еліптичних кривих і збільшити швидкість виявлення криптоаналітичних атак на інформаційно-управляючі системи БСМ мінімум у 10^2 разів. Розроблено програмні засоби захисту інформації і рекомендації щодо практичного застосування запропонованих методів і моделей у БСМ.

Ключові слова: безпроводова сенсорна мережа, захист інформації, кібератака, модель захищеної комунікації, інформаційно-управляюча система, еліптичні криві, ймовірнісне маркування пакетів.

АННОТАЦИЯ

Александер М.Б. Методы и модели обеспечения защиты беспроводных сенсорных сетей. – Рукопись.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.21 – Системы защиты информации. – Национальный авиационный университет, Киев, 2016.

Диссертационная работа посвящена решению актуальной научно-практической проблемы создания новых методов и моделей защиты беспроводных сенсорных сетей (БСС) и их компонентов от различных кибератак, направленных на нарушение конфиденциальности, целостности и доступности их информационных ресурсов.

В работе проведен анализ БСС (архитектуры, протоколов), который указал на их уязвимость к разному классу DoS-атак, а также к другим кибератакам, нарушающим конфиденциальность и целостность информационных ресурсов этих сетей. Анализ позволил сформулировать задачу относительно разработки эффективных методов и моделей обеспечения защиты БСС. Предложенные новые математические модели информационных структур вероятности угроз определенного класса DoS-атак, которые за счет сформированного базового множества характерных показателей и соответствующих весовых коэффициентов, и взаимосвязей определенных матриц активности сети, а также установленной интенсивности влияния разных классов кибератак, разрешают оценивать уровень влияния показателей киберугроз относительно БСС. Получила дальнейшее развитие модель защищенной коммуникации «клиент-сервер-шлюз-узел», которая за счет сформированного базового множества зависимостей возможных путей «точка доступа → точка назначения» с учетом влияния величин вероятностей компрометации узлов и высчитанных весовых коэффициентов, дает возможность идентифицировать класс реализованной кибератаки на БСС и определить соответствующие мероприятия для противодействия. Получил дальнейшее развитие метод восстановления сообщений, который за счет процедуры подстановочной сортировки b-битных блоков лексикографическими значениями, интерпретации значения соответственно формату хранения блоков в IP-заголовке, *i*-индексным приведением в порядок контрольных сумм и двухфазной схемы возобновления, дает возможность на 11% эффективней обеспечить целостность сообщений в условиях реализации соответствующих киберугроз БСС. Усовершенствован метод вероятностного маркирования пакетов в БСС, который за счет дополнения пакетов вектором идентификации номеров узлов (записанных в его координатах), правил формирования вероятности успешного узлового перехода, процедуры ограничения выборки пакетов по мини-

максному критерию и предложенного метода восстановления сообщения, позволяет осуществлять мониторинг БСС и отслеживать источник кибератак на 17% точнее. Получили дальнейшее развитие структурно-аналитические модели обеспечения живучести управляющих систем БСС, которые за счет построенного направленного графа информационно-технических состояний $MS_{ПС}$, $MS_{ЧП}$, $MS_{НБС}$ и $MS_{НС}$ с комбинацией кодированных показателей дефектов внешних влияний по признакам вероятности и детерминированности, дают возможность осуществлять выбор эффективной стратегии обслуживание информационно-управляющей системы по показателям готовности технического и информационного состояний относительно сформированного множества дефектов, которые влияют на базовую характеристику безопасности – доступность.

Усовершенствованы технологии вычислений на эллиптических кривых, которые за счет предлагаемого способа замены операций умножения по модулю в алгоритме Крестенсона эквивалентным преобразованием на основе операции добавления с отображением на соответствующую вычислительную архитектуру, разрешают обеспечить высокую скорость криптографической обработки данных в устройствах управляющих систем БСС. Получили дальнейшее развитие структурно-аналитические модели вычислителей на эллиптических кривых в устройствах управляющих систем, которые за счет предложенных структурно-аналитических моделей обеспечения живучести и реализации параллельных вычислений на основе теоретико-числовых базисов Радемахера-Крестенсона в разработанных вычислительных архитектурах, позволяют достичь минимальных размеров эллиптических кривых, которые могут быть применены для обеспечение необходимого уровня доступности управляющих систем БСС. Получили дальнейшее развитие структурно-аналитические модели вычисления дискретного логарифма для кривых над полем $GF(2^m)$, которые за счет использования разработанных моделей вычислителей на эллиптических кривых и с учетом теоретико-числовых базисов Радемахера-Крестенсона для параллельного суммирования чисел большой разрядности и параллельной реализации операций на основании ро-метода Полларда, дают возможность строить высокопроизводительные криптографические устройства на эллиптических кривых и увеличить скорость выявления криптоаналитических атак, которые влияют на конфиденциальность управляющих систем БСС, минимум в 10^2 раз. Разработаны программные средства защиты информации и рекомендации относительно практического применение предложенных методов и моделей в БСС. На базе полученных теоретических результатов созданы специализированное программное обеспечение выявления разного класса DoS-атак на БСС. Создано две аппаратно-программных системы: первая работает на программированных матрицах FPGA и ПК, действие которой основывается на основе модифицированной модели вычислений, причем на основании исследований построенного сумматора точек на программированных матрицах FPGA Stratix III EP3SL150F1152I4SL получено увеличение скорости шифрования методом Ель-Гамаля приблизительно в три раза по сравнению с традиционным подходом суммирования точек; вторая система реализует ро-алгоритм Полларда, используя технологию вычислений на ТЧБ Крестенсона, и основывается на аналогичных аппаратных средствах. По результатам исследования работы параллельной системы на нескольких программированных матрицах FPGA для решения логарифма для эллиптических кривых определено, что применение «путей поиска» алгоритма, который реализовано на одной программированной матрице FPGA, предопределяет трехкратное увеличение скорости работы алгоритма в сравнении с системой, построенной на базе процессора Itanium 2. Результаты диссертационной работы внедрены и получили использование в образовательном процессе Универ-

ситета в Бельско-Бялой (Польша) (акт внедрения от 24 ноября 2015 года) и Национального авиационного университета (акт внедрения от 18 мая 2016 года) согласно Соглашению о сотрудничестве между университетами №336 от 15 мая 2014 года.

Ключевые слова: беспроводная сенсорная сеть, защита информации, кибератака, модель защищенной коммуникации, информационно-управляющая система, эллиптические кривые, вероятностное маркирование пакетов.

ABSTRACT

Aleksander M.B. Methods and models to provide wireless sensor networks security – Manuscript.

Thesis for a Doctor of Technical Science degree in specialty 05.13.21 – Information security systems. – National Aviation University, Kyiv, 2016.

Thesis is devoted to applied scientific research problem to develop new methods and models for wireless sensor networks (WSN) and its components security against cyberattacks directed on information resources confidentiality, integrity and availability violation.

In the work the analysis of WSN (architecture, protocols) was carried out and it was pointed on WSN vulnerabilities against cyberattacks that violate information resources confidentiality, integrity and availability. New mathematical models for information structures of Dos-attacks threats probabilities were proposed and these give possibilities to assess level of influence by threats parameters of WSN. The model of secured communication «client-server-gateway-node» was developed and it allows cyberattack (directed on WSN) type identifying and countermeasures defining. Also the method of message reconstruction was developed and it gives a possibility to provide messages integrity 11% on favor of known methods in conditions of WSN cyberthreats realization. The method of probability packet marking in WSN was improved and it allows to monitor WSN and define cyberattack sources accurately on 17%. The structural and analytical model of information and control systems of WSN survivability that provide effective service strategy choosing by technical and informative readiness relatively to defects. The computation technologies based on elliptic curves and provide high cryptographic performance in information and control systems of WSN. The structural and analytical models of calculators based on elliptic curves in information and control systems that allow to minimize elliptic curves for the security of information and control systems of WSN. And also the structural and analytical models for discrete logarithm calculation for curves on field $GF(2^m)$ that allow high performance cryptographic devices construction based on elliptic curves and these models also provide high detection rate (more than 10^2 of times) of cryptanalytic attacks on information and control systems of WSN. Software for information security and practical recommendations for proposed methods and models implementation were also created.

Key words: wireless sensor network, information security, cyberattack, secured communication model, information & control system, elliptic curves, probability packet marking.