

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ

УДК 681.518.54



Тези доповідей

Міжнародної науково-практичної конференції

**“Інформаційна безпека та інформаційні
технології”**

**“Information Security and Information
Technologies”**

24–25 квітня 2019 р.

Харків 2019

УДК 681.518.54

Матеріали Міжнародної науково-практичної конференції “Інформаційна безпека та інформаційні технології”: тези доповідей, 24 – 25 квітня 2019 р. – Х.: ХНЕУ імені Семена Кузнеця, 2019. – 68 с.

Наведені тези пленарних та секційних доповідей за теоретичними та практичними результатами наукових досліджень і розробок. Представлені результати теоретичних досліджень в галузях проектування інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

За достовірність викладених фактів, цитат та інших відомостей відповідальність несе автор.

© Харківський національний економічний університет імені Семена Кузнеця, 2019

ПОБУДОВА ГІБРИДНОЇ КРИПТО-КОДОВОЇ КОНСТРУКЦІЇ МАК-ЕЛІСА

Криптографічні системи на алгоритмах несиметричної криптографії (RSA, ECC, DSA) вразливі до атак “грубої сили” з використанням повномасштабного квантового комп’ютера. Тому основні дослідження і розробки криптографічних засобів захисту інформації (КЗЗІ) спрямовані на пошуки рішень, що не мали б вразливостей щодо квантових обчислень і були б одночасно стійкими до атак за допомогою звичайних комп’ютерів. Такі алгоритми відносяться до розділу квантово-стійкої криптографії.

Аналіз практичної реалізації алгоритмів шифрування / розшифрування в гібридній крипто-кодovій конструкції (ГККК) Мак-Еліса показує, що досягається зменшення поля до $GF(2^4)$ зі збереженням гарантованої стійкості за рахунок використання збиткових кодів та медоів багатоканальної криптографії. Алгоритм формування кодограми (криптограми) що реалізовується за допомогою відповідних пристроїв кодування, та полягає у виконанні наступних кроків:

1. Фіксування кінцевого поля $GF(q)$. Фіксування еліптичної кривої $y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$ і набір її точок $EC(GF(q)) : (P_1, P_2, \dots, P_N)$ над $GF(q)$. Фіксування підмножини точок $h(GF(q)) : (P_{x1}, P_{x2}, \dots, P_{xx})$, $h \subseteq EC(GF(q))$, h/x і зберігаємо його в секреті.

2. Фіксування вектору ініціалізації $IV = EC - h_j$, h_j – інформаційні символи рівні нулю, $h/x = \frac{1}{2}k$, т. то. $I_i = 0, \forall I_i \in h$;

3. За введеним інформаційним вектором I формування кодового слову c . Якщо (n, k, d) код над $GF(q)$ заданий породжувальною матрицею, то $c = I \cdot G$.

4. Формування випадкового вектору помилки e такий, що $w(e) \leq t$, $t = \lfloor (d-1)/2 \rfloor$. Отримання кодового слову шляхом додавання сформованого вектору до кодового слову: $c^* = c + e$.

5. Формування кодограми, шляхом видалення (укорочення) символів вектору ініціалізації, яка поступає на алгоритм MV2 [3]: $c_X^* = c^* - IV$.

6. Формування прапору $CH_D^i \| f(x)_i \|$ і залишку $CFT^i \| C(x)_i \|$ на основі алгоритму MV2:

$$C_j^* = C_j - C_{k-h_j}, E_{K_{MV2}} : C_j^* \rightarrow \| f(x)_i \| + \| C(x)_i \|.$$

Алгоритм розкодування кодограми (криптограми), що реалізовується за допомогою

відповідних пристроїв кодування, та полягає у виконанні наступних кроків:

1. Введення кодограми, що підлягає розкодуванню. Осмислення кодограми за алгоритмом MV2:

$$E_{K_{MV2}}^{-1} : \| f(x)_i \| + \| C(x)_i \| \rightarrow C_j.$$

2. Додавання нульових інформаційних символів до отриманої кодограми: $C_j^* = C_j + C_{k-h_j}$;

3. Розкодування отриманого вектору у відповідних пристроях за алгоритмом Берлекемпа-Мессі: $C = M_i \cdot (X^u)^T \cdot (G^{EC})^T + e \cdot (D^u)^{-1} \cdot (P^u)^{-1}$, кодограма – суть кодове слово з помилками еліптичного коду. Вага вектора помилок $w(e) \leq t$.

4. Формування інформаційного вектору. Для цього у відповідних пристроях отриманий результат розкодування $M_i \cdot (X^u)^T$ слід помножити на $(X^u)^{-1}$:

$$(M_i \cdot (X^u)^T) \cdot (X^u)^{-1} = M_i.$$

Таким чином використовуючи вектор ініціалізації при формуванні кодограми і універсальний механізм заподіяння збитку на основі алгоритму MV2 забезпечується суттєве зменшення довжини кодового слова який поступає в канал зв’язку, тим самим складність формування криптограми зменшується \approx в 12 разів і розкодування криптограми \approx в 20 разів зі збереженням стійкості несиметричної крипто-кодovої конструкції.

Список літератури

1. С. П. Євсєєв, “Використання кодів пошкоджень у крипто-кодovих системах”, *Інформаційні системи*, № 5 (151), с. 109–121, 2017.
2. С. П. Євсєєв, Г. П. Коц, С. В. Мінухін, О. Г. Король, та А. В. Холодкова, “Розробка методу багатofакторної аутентифікації на основі гібридних криптокодovих конструкцій на дефектних кодах”, *Східноєвропейський журнал передових технологій*, 5/9(89), с. 19 – 35, 2017.
3. С. П. Євсєєв, Г. П. Коц, та Є. С. Лекарев, “Розробка багатofакторного методу аутентифікації на основі модифікованої криптокодovої системи Нідеррайтера-Мак\еліса”, *Східноєвропейський журнал передових технологій*, 6/4(84), с. 1, 2010.

ЗМІСТ

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

РОЗРОБКА МЕТОДУ ДІАГНОСТИЧНОГО КОНТРОЛЮ ТЕХНІЧНОГО СТАНУ ДВИГУНІВ ЗАСОБІВ ВОДНОГО ТРАНСПОРТУ ДЛЯ ЗМЕНШЕННЯ ВИТРАТ НА ПЕРЕВЕЗЕННЯ ВАНТАЖІВ.....	3
МАТЕМАТИЧНИЙ ОПИС КРИПТОСИСТЕМИ ФРЕДГОЛЬМА.....	4
ОБҐРУНТУВАННЯ ПРИНЦИПІВ ПОБУДОВИ АВТОМАТИЧНИХ ПРИЛАДІВ ДЛЯ КОНТРОЛЮ ПАРАМЕТРІВ СИСТЕМ УПРАВЛІННЯ ТА НАВІГАЦІЇ ЗАСОБІВ ВОДНОГО ТРАНСПОРТУ.....	5
ПІДХОДИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ ОРГАНІЗАЦІЙ ПРИ ВИКОРИСТАННІ ВНУТРІШНІМИ СТЕЙКХОЛДЕРАМИ МОБІЛЬНИХ ПРИСТРОЇВ	6
МЕТОД СТВОРЕННЯ ЦИФРОВОГО ПІДПISУ НА ОСНОВІ УЗАГАЛЬНЕНОГО ПЕРЕТВОРЕННЯ ФУР'Є	7
СЕНСОРНІ МЕРЕЖІ ZIGBEE, WIFI ТА BLUETOOTH В КІБЕРФІЗИЧНИХ ТЕХНОЛОГІЯХ.....	8
ПОБУДОВА ГІБРИДНОЇ КРИПТО-КОДОВОЇ КОНСТРУКЦІЇ МАК-ЕЛІСА.....	9
ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ УМОВАХ ГОСПОДАРЮВАННЯ.....	10
ИССЛЕДОВАНИЕ И ОБОСНОВАНИЕ ВЫБОРА МЕТОДОВ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ	11
СПОСОБИ МОДЕЛЮВАННЯ КІБЕРАТАК У СУЧАСНОМУ КІБЕРПРОСТОРІ.....	12
ТОТАЛЬНА ОПТИМІЗАЦІЯ ЛОГІСТИЧНОГО БІЗНЕСУ ЯК ВАЖЛИВИЙ АНТИКРИЗОВИЙ І БЕЗПЕКОВИЙ ІНСТРУМЕНТ.....	13
АНАЛІЗ РОБОТИ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ.....	14
МОДЕЛЮВАННЯ ІНФОРМАЦІЙНОГО ВПЛИВУ В СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ НА ОСНОВІ СИСТЕМОЇ ДИНАМІКИ.....	15
ТЕХНОЛОГІЇ ДАТА-ЦЕНТРІВ ТА ОХОРОНА ДОВКІЛЛЯ	16
РОЗВИТОК МЕТОДІВ І МОДЕЛЕЙ ДЛЯ ОЦІНЮВАННЯ СТРАТЕГІЙ ІНВЕСТИВАННЯ В СИСТЕМИ КІБЕРБЕЗПЕКИ	17
ОБҐРУНТУВАННЯ ПРОПОЗИЦІЙ ЩОДО ЗАСТОСУВАННЯ СУЧАСНИХ СУПУТНИКОВИХ ТЕХНОЛОГІЙ ДЛЯ ТОПОГЕОДЕЗИЧНОГО ЗАБЕЗПЕЧЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ.....	18
ПОШУК КРИТИЧНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ В ЗАСОБАХ МАСОВОЇ ІНФОРМАЦІЇ.....	19
АНАЛІЗ ВРАЗЛИВОСТЕЙ WINDOWS-ПОДІБНИХ СЕРВЕРНИХ ОПЕРАЦІЙНИХ СИСТЕМ ТА ЗАГАЛЬНЕ ОПИСАННЯ МЕХАНІЗМІВ ЇХ ЗАХИСТУ.....	20
ГІБРИДНА КРИПТО-КОДОВА КОНСТРУКЦІЯ НІДЕРРАЙТЕРА НА ЗБИТКОВИХ КОДАХ	21
ДОСЛІДЖЕННЯ СТІЙКОСТІ СТЕГANOГРАФІЧНИХ МЕТОДІВ ВБУДОВУВАННЯ ДАНИХ В ВІДЕОФАЙЛИ ДО АТАК.....	22

СЕКЦІЯ 2 ПРОГРАМУВАННЯ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

ОЦЕНКА ПОМЕХОУСТОЙЧИВОСТИ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ КОДОВ С ПОСТОЯННЫМ ВЕСОМ.....	23
THE DECISION-MAKING PROBLEM IN CONDITIONS OF FUZZY INITIAL INFORMATION.....	24
РАСПРЕДЕЛЕНИЕ НАГРУЗКИ ПРИ ПОСТРОЕНИИ ОТЧЁТОВ И ЗАПРОСОВ С БОЛЬШИМ ОБЪЁМОМ ДАННЫХ.....	25
РЕЗУЛЬТАТИ ЧИСЕЛЬНОГО МОДЕЛЮВАННЯ НЕСТАЦІОНАРНИХ РЕЖИМІВ З ВИКОРИСТАННЯМ МЕТОДУ БРОЙДЕНА.....	26
ГЕНЕРУВАННЯ ФРАКТАЛЬНОГО ТРАФІКУ ЗА ДОПОМОГОЮ МОДЕЛІ ГЕНЕРАТОРА НА ГРАФІ.....	27
СЖАТИЕ ИЗОБРАЖЕНИЙ НА ОСНОВЕ АВТОМАТИЧЕСКОЙ И НЕЧЕТКОЙ КЛАССИФИКАЦИИ ФРАГМЕНТОВ.....	28
СИСТЕМА ПІДТРИМАННЯ ПРИЙНЯТТЯ РІШЕНЬ ДІЯЛЬНОСТІ КОМПАНІЙ У СФЕРІ ОБСЛУГОВУВАННЯ.....	29
ЗАСТОСУВАННЯ МОДЕЛІ ПРИЙНЯТТЯ РІШЕНЬ В УМОВАХ ПРОТИДІЇ КОНКУРЕНТІВ.....	30
СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ З УПРАВЛІННЯ ТРАНСПОРТНИМИ ПОТОКАМИ ВЕЛИКОГО МІСТА.....	31
МОДИФИЦИРОВАННЫЕ СПОСОБЫ ПОДСЧЕТА ДВОИЧНЫХ ЕДИНИЦ.....	32
РОЗРОБЛЕННЯ КОМП'ЮТЕРНОЇ ПРОГРАМИ "STAT TRACKER".....	33
ПІДСИСТЕМА УПРАВЛІННЯ ДАНИМИ КОРИСТУВАЧІВ ВЕБ-ЗАСТОСУНКУ НА БАЗІ ФРЕЙМВОРКУ DJANGO.....	34
СІТКОВІ 3D-ОБ'ЄКТИ ЇХ ОЦІНКА ТА ЯКІСТЬ ПРИ РІЗНИХ ШВИДКІСТЯХ ЦИФРОВОГО ПОТОКУ.....	35
ХМАРНИЙ СЕРВІС ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ОПТИМІЗАЦІЇ ТЕХНОЛОГІЧНОГО ПРОЦЕСУ ВІДНОВЛЕННЯ ТА ЗМІЦНЕННЯ ПОВЕРХОНЬ ЗІ СТАЛІ.....	36
ВИМОГИ ДО СЕРВІСІВ ДОСТАВКИ PUSH-СПОВІЩЕНЬ КОРИСТУВАЧАМ.....	37
СИСТЕМА ПІДТРИМАННЯ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ФОРМУВАННІ НАВИЧОК НАУКОВОЇ РОБОТИ.....	38
ОБҐРУНТУВАННЯ РОЗРОБКИ СИСТЕМИ ПІДТРИМАННЯ ПРИЙНЯТТЯ РІШЕНЬ НАДАННЯ РЕЛЕВАНТНИХ РЕКОМЕНДАЦІЙ ФІЛЬМІВ З ВРАХУВАННЯМ ОСОБИСТИХ ПОТРЕБ КОРИСТУВАЧА.....	39

СЕКЦІЯ 3 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ, МЕДИЦИНІ ТА ОСВІТІ

ПРИМЕНЕНИЕ АТМОСФЕРНОЙ ОПТИЧЕСКОЙ СВЯЗИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ.....	40
ОСНОВИ ТЕОРІЇ ОПТИМІЗАЦІЇ РАДІОЕЛЕКТРОННИХ ВИМІРЮВАЧІВ.....	41
RAILS CONDITION CONTROL SYSTEM FOR ENSURING TRAFFIC SAFETY OF TRAINS.....	42
INCREASING THE DETERMINATION ACCURACY OF THE SURFACE COLOR BY CALORIMETRIC METHOD.....	43
ДОСЛІДЖЕННЯ БАГАТОФАКТОРНОЇ МОДЕЛІ ОЦІНКИ ПОКАЗНИКІВ РОЗВИТКУ ІТ-ГАЛУЗІ ЗА РЕГІОНАМИ УКРАЇНИ.....	44

ОРГАНІЗАЦІЙНІ РІВНІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ.....	45
СИМВОЛІЧНІ МОДЕЛІ ФІЗИЧНИХ ПРОЦЕСІВ, ЩО ОПИСУЮТЬСЯ ІНТЕГРАЛЬНИМ РІВНЯННЯМ ФРЕДГОЛЬМА ПЕРШОГО РОДУ.....	46
КРИЗОВІ КОМУНІКАЦІЇ В СВІТОВІЙ ТУРИСТИЧНІЙ ІНДУСТРІЇ.....	47
ПОБУДОВА КОМІТЕТУ НЕЙРОПОДІБНИХ СТРУКТУР МПГП З ПОЛІНОМІАЛЬНИМ РОЗШИРЕННЯМ ВХОДІВ ДЛЯ ЗАДАЧ ВЕЛИКИХ ДАНИХ ..	49
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПОЗИЦІОНУВАННЯ БРЕНДУ.....	50
ОСОБЛИВОСТІ ВИКОРИСТАННЯ ГРАФІЧНОГО КОНТЕНТУ ДЛЯ ІНФОРМАЦІЙНОГО ВПЛИВУ НА АКТОРІВ СОЦІАЛЬНИХ МЕРЕЖ.....	51
РОЗВ'ЯЗАННЯ СИСТЕМНИХ ЗАДАЧ ЗА СЦЕНАРНО-ЦІЛЬОВИМ ПІДХОДОМ НА ОСНОВІ РОЗРОБКИ ЗНАННЯ-ОРІЄНТОВАНИХ СИСТЕМ.....	52
ЦИКЛ ПЕРЕТВОРЕННЯ ЗНАНЬ ЯК СКЛАДОВА ЧАСТИНА КОНЦЕПЦІЇ ВРМ.....	53
КОНЦЕПТУАЛІЗАЦІЯ ОРГАНІЗАЦІЙНО-ІНФОРМАЦІЙНОЇ ПІДТРИМКИ ФОРМУВАННЯ СИСТЕМИ ЗНАНЬ ПІДПРИЄМСТВА.....	54
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В МАРКЕТИНГОВІЙ ДІЯЛЬНОСТІ ПРОМИСЛОВИХ ПІДПРИЄМСТВ.....	55
ПЕРСОНАЛІЗОВАНИЙ ПІДХІД ЩОДО ОБРОБКИ ТА АНАЛІЗУ МЕДИЧНИХ ДАНИХ ПАЦІЄНТІВ.....	56
ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ.....	57
ВИКОРИСТАННЯ СЕРВІС-ОРІЄНТОВАНОЇ АРХІТЕКТУРИ ДЛЯ СИСТЕМИ РІВНЯ ENTERPRISE PERFORMANCE MANAGEMENT.....	58
КОНЦЕПТУАЛЬНІ ПОЛОЖЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ РОЗВИТКУ ПІДПРИЄМСТВА.....	59
МЕТОДИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ КЛАСТЕРНОГО АНАЛІЗУ НАДЗВИЧАЙНИХ СИТУАЦІЙ В СМАРТ-СІТІ	60
СТРАТЕГІЯ РІШЕНЬ НАДАННЯ ПРОФЕСІЙНОЇ МЕДИЧНОЇ ДОПОМОГИ В РАЙОНАХ ТЕХНОГЕННИХ КАТАСТРОФ НА БАЗІ ВИСОКИХ ТЕХНОЛОГІЙ	61
МІЖНАРОДНА ЕКОНОМІЧНА БЕЗПЕКА ДЕРЖАВИ В СУЧАСНИХ УМОВАХ.....	62
ДІГІТАЛІЗАЦІЯ ЯК ЧИННИК РОЗВИТКУ ВИЩОЇ ОСВІТИ	63
ІНФОРМАЦІЙНА ЗАБЕЗПЕЧЕНІСТЬ СИСТЕМИ ВЕРИФІКАЦІЇ ПЕРСОНАЛЬНИХ ДАНИХ.....	64

ТЕЗИ ДОПОВІДЕЙ
Міжнародної науково-практичної конференції
“Інформаційна безпека та інформаційні технології”
“Information Security and Information Technologies”

24–25 квітня 2019 р.

Відповідальний за випуск: *С.П. Євсєєв*

Комп'ютерна верстка: *А.А. Гаврилова*

Підписано до друку 30.03.2017. Формат 60×84/8. Папір офсетний.
Гарнітура «TimesNewRoman». Друк ризографічний. Ум.-друк. арк. – 8.6. Ціна договірна.
Наклад 250 прим.Зам. 0330/9-18

Видавництво «Цифрова друкарня №1»
Свідоцтво суб'єкта видавничої справи: серія ДК № 4354 від 06.07.2012 р.
61001, м. Харків, пл. Повстання, 7/8
e-mail: zebra-zakaz@mail.ru

Віддруковано з готових оригінал-макетів у друкарні ФОП Петров В.В.
Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців.
Запис № 2480000000106167 від 08.01.2009.
61144, м. Харків, вул. Гв. Широнінців, 79в, к. 137, тел. (057)778-60-34e-mail: bookfabric@rambler.ru