

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

## ГІБРИДНА КРИПТО-КОВОДА КОНСТРУКЦІЯ НІДЕРРАЙТЕРА НА ЗБИТКОВИХ КОДАХ

Вступ людства до ери високих технологій стимулює подальше розширення можливостей обчислювальних систем. Стрімке зростання і розширення функціональних можливостей корпоративних систем і соціальних мереж, дозволяє будувати інтегровані соціально-інформаційні мережі для вирішення різноманітного спектра завдань. Подальший розвиток технології передачі даних Ethernet формує глобальну ідеологію побудови телекомунікаційних мереж [1].

Використання модифікованої крипто-кової конструкції (МККК) Нідеррайтера з додатковими векторами ініціалізації (з множиною неприпустимих позиційних векторів вектора помилок і множиною позицій укорочення вектора помилки) вимагає збільшення швидкодії криптоперетворень системи в цілому. Для цього пропонується використовувати збиткові коди. Збиткові коди дозволяють збільшити швидкість кодових перетворень за рахунок зменшення потужності поля при нанесенні збитку відкритого тексту і зменшити обсяг переданих даних за рахунок нанесення шкоди шифртексту. Такий підхід дозволяє будувати гібридні крипто-ковові конструкції на основі синтезу модифікованих криптокодових конструкцій Нідеррайтера на модифікованих (укорочених або подовжених) кодах на еліптичних кривих з процедурами нанесення збитку. Суттєвою відмінністю від класичних гібридних (комплексних) криптосистем є використання несиметричної криптосистеми для забезпечення безпеки даних з швидкими процедурами криптоперетворень (формування та розкодування кодограми). Використання механізму нанесення збитку MV2 в крипто-кової конструкції Нідеррайтера на модифікованих еліптичних кодах в Інтернет-технологіях та мобільних мережах, забезпечення практичної реалізації на сучасних платформах та необхідної криптостійкості в умовах постквантової криптографії [2].

Розглянемо формальний опис гібридної математичної моделі несиметричної крипто-кової конструкції Нідеррайтера на збиткових кодах.

На основі рівноважного кодування формується закритий текст  $C_j \in C$  за введеним відкритим текстом  $M_i \in M$  і заданим ключем  $H_X^{ECu}$ ,  $u \in \{1, 2, \dots, s\}$ . Це здійснюється шляхом формування синдромної (в термінах завадостійкого

кодування) послідовності  $S_{X_j}$ , що відповідає рівноважній послідовності  $M_i = e = \{e_0, e_1, \dots, e_{n-1}\}$ :

$$S_{X_j} = \phi_u(M_i, H_X^{ECu}) = M_i \times (H_X^{ECu})^T, \text{ причому}$$

вага Гемінга (кількість ненульових елементів) вектора  $e$  не перевищує виправної здатності використовуваного алгебраїчного блокового  $(n, k, d)$  коду:

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

Потужність множин  $M$  та  $C$  визначається допустимим спектром ваг  $w(M_i)$ , тобто в загальному випадку (для всіх допустимих значень  $w(M_i)$ ) маємо:

$$m = \sum_{i=0}^t (q-1)^i \times C_n^i, \text{ де } C_n^i \text{ — біноміальний}$$

коефіцієнт,  $C_n^i = \frac{n!}{i!(n-i)!}$ .

Сформований закритий текст  $C_j \in C$  однозначно відповідає вектору  $M_i = \{e_0, e_1, \dots, e_{n-1}\}$ .

Відкритий ключ формується шляхом множення перевірконої матриці алгеброгеометричного коду на матриці маскування:

$$H_X^{ECu} = X^u \cdot H \cdot P^u \cdot D^u, \text{ } u \in \{1, 2, \dots, s\},$$

де  $H^{EC}$  — перевіркона  $n \times (n-k)$  матриця алгеброгеометричного блокового  $(n, k, d)$  коду з елементами з  $GF(q)$ .

В канал зв'язку поступає синдромна послідовність:  $S_{r-h_e}^* = (e_n - h_e) \times H_X^{ECT}$ .

### Список літератури

1. Ethernet и промышленные сети [Электронный ресурс]. Доступно: <https://www.osp.ru/lan/2013/09/13037411/>. Дата обращения: Март 23, 2019.
2. S. Yevseiev, O. Tsyhanenko, A. Gavrilova, V. Guzhva, O. Milov, V. Moskalenko, and et. al, "Development of Niederreiter hybrid crypto-code structure on flawed codes", *Eastern-European Journal of Enterprise Technologies*, 1 (9 (97)), pp. 27–38, 2019.

## 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-КОВОДОЇ 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-КОВОДА 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 VRM.....	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