ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації

СКУЦЬКОГО АРТЕМА БОРИСОВИЧА

на тему: «Метод і моделі системи захищеного інформаційного обміну з нероздільним факторіальним кодуванням даних»

для здобуття ступеня доктора філософії

за спеціальністю 123 – Комп'ютерна інженерія

Публічна презентація наукових результатів дисертації Скуцького Артема Борисовича відбулася на засіданні кафедри інформаційної безпеки та комп'ютерної інженерії (далі – ІБКІ) Черкаського державного технологічного університету (далі – ЧДТУ) 07 травня 2025 року, протокол № 12.

ПРИСУТНІ:

Базіло К.В., професор кафедри приладобудування, мехатроніки та комп'ютеризованих технологій;

Бойко А.І, завідувач кафедри філософських і політичних наук, професор;

Бондаренко М.О., завідувач кафедри приладобудування, мехатроніки та комп'ютеризованих технологій, професор;

Махиня Н.В., декан факультету гуманітарних технологій, професор кафедри іноземних мов та міжнародної комунікації;

Триус Ю.В., завідувач кафедри комп'ютерних наук та системного аналізу, професор;

Усик Л.М., доцент кафедри іноземних мов та міжнародної комунікації;

Фауре Е.В., проректор з науково-дослідної роботи та міжнародних зв'язків, професор кафедри ІБКІ, д.т.н., професор;

Бабенко В.Г., завідувач кафедри ІБКІ, д.т.н., професор;

Федоров Є.Є., професор кафедри ІБКІ, д.т.н., професор;

Миронець І.В., доцент кафедри ІБКІ, к.т.н., доцент;

Лавданський А.О., доцент кафедри ІБКІ, к.т.н., доцент;

Миронюк Т.В., доцент кафедри ІБКІ, к.т.н., доцент;

Нечипоренко О.В., доцент кафедри ІБКІ, к.т.н., доцент;

Сисоєнко С.В., доцент кафедри ІБКІ, к.т.н., доцент;

Розломій І.В., доцент кафедри ІБКІ, к.т.н., доцент;

Тазетдінов В.А., доцент кафедри ІБКІ, к.т.н., доцент;

Чепинога А.В., доцент кафедри ІБКІ, к.т.н., доцент;

Гресько С.О., ст. викладач кафедри ІБКІ;

Скуцький А.Б., здобувач ступеня доктора філософії за спеціальністю 123 «Комп'ютерна інженерія» 4-го року навчання;

Бондар В.В., здобувач ступеня доктора філософії за спеціальністю 123 «Комп'ютерна інженерія»1-го року навчання.

Тему дисертації «Метод і моделі системи захищеного інформаційного обміну з нероздільним факторіальним кодуванням даних» затверджено на засіданні вченої ради факультету інформаційних технологій і систем 27 березня 2025 року (протокол № 8). Науковий керівник: д.т.н., професор Фауре Еміль Віталійович – призначений наказом Черкаського державного технологічного університету від 06 серпня 2021 року № 243/01.

1. Актуальність теми дослідження.

Актуальність дисертаційного дослідження зумовлена потребою у забезпеченні захищеного інформаційного обміну в системах з нероздільним факторіальним кодуванням зашумленим каналом зв'язку. Зростання обсягів переданої конфіденційної інформації, розширення мереж бездротових сенсорних систем, військових, промислових та спеціалізованих засобів зв'язку потребують нових підходів до організації інформаційного обміну, здатних забезпечити стійкість до помилок, викликаних шумами, затримками або втратами даних. Особливої складності набуває задача встановлення синхронізму за невідомого початкового моменту передавання, що унеможливлює застосування відомих синхросхем та може призводити до хибного виявлення або збоїв у функціонуванні приймальної сторони.

Дисертантом розглянуто існуючі методи кадрової синхронізації на основі нероздільного факторіального кодування (НФКД), зокрема ті, що використовують кореляційну обробку або префіксно-суфіксну структуру. У роботі Скуцький А. Б обґрунтовує, що існуючі методи кадрової синхронізації на основі НФКД не враховують критично важливий фактор – невизначений початковий момент передавання даних. Що створює ризики хибних спрацювань або навіть аварій у випадках, коли синхрокомбінація фактично не надходить у канал, а шум сприймається як потенційна інформація. Ці обмеження є критичними. Відповідно постає потреба в нових або вдосконалених методах синхронізації з НФКД, здатних працювати в симплексному каналі за не визначеного початкового моменту приймання.

У цьому контексті перспективним є використання методу синхронізації НФКД з мажоритарною та кореляційною обробкою. Розроблений автором метод базується на методі кадрової синхронізації НФКД з кореляційною обробкою і додаванням показника серії спрацювань підсистеми синхронізації на основі ковзного вікна фіксованої довжини. Такий підхід дозволяє

інтегрувати в одній конструкції властивості надлишковості, завадостійкості та криптографічного захисту. Особливу наукову й прикладну цінність має поєднання НФКД з матричними структурами, зокрема з використанням скінченних полів квадратних матриць, що дозволяє реалізувати генерації перестановок ключів.

Таким чином, необхідність створення нових систем захищеного інформаційного обміну, здатних функціонувати в умовах невизначеності, зашумленості каналу та обмеженого обчислювального ресурсу, зумовлює актуальність дисертаційного дослідження. Запропоноване автором розв'язання спрямоване на підвищення достовірності та надійності передавання інформації в критичних умовах шляхом розвитку методів кадрової синхронізації з НФКД, а також теоретичному обґрунтуванні побудови скінченних полів матриць з метою інтеграції матричних структур разом з НФКД.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження, результати яких представлено в дисертаційній роботі, відповідають пріоритетному напряму розвитку науки і техніки України «Інформаційні та комунікаційні технології» та його тематичному напряму «Інформаційно-комунікаційні та радіоелектронні системи та технології, засоби радіоелектронної боротьби для забезпечення національної безпеки і оборони. Інформаційна безпека та кібербезпека» і виконувалися відповідно до програм і планів науково-дослідних робіт Черкаського державного технологічного університету, в тому числі в рамках держбюджетних науково-технічних (експериментальних) розробок молодих вчених, де автор був виконавцем:

- «Розробка завадозахищеної енергоефективної системи контролю та управління віддаленими безпілотними об'єктами на основі факторіального кодування даних» (№0125U000637);
- «Розробка методів, протоколів і засобів захищеного інформаційного обміну з використанням трьохетапного криптографічного протоколу на основі перестановок в умовах зашумленості каналів зв'язку» (№0123U100270);
- «Розробка мобільної системи захищеного інформаційного обміну для військових і цивільних підрозділів державних структур» (№0120U102607).

Метою дисертаційної роботи є забезпечення захищеного інформаційного обміну в системах з нероздільним факторіальним кодуванням даних і зашумленим каналом зв'язку.

Досягнення означеної мети передбачає виконання наступних завдань:

- розвинути метод кадрової синхронізації нероздільних факторіальних кодів для випадків невідомого моменту початку приймання синхрокомбінацій передавача;
- розвинути математичну модель процесу виявлення синхрокомбінації

систем передавання інформації з нероздільним факторіальним кодуванням даних за невідомого моменту початку приймання синхрокомбінацій передавача;

- розробити математичну модель скінченного поля квадратних матриць порядку 2 над скінченним полем простих чисел та розробити методику їх використання для узгодження ключів-перестановок;
- побудувати імітаційну модель системи інформаційного обміну, провести порівняльні експериментальні оцінки удосконаленого методу кадрової синхронізації.

Для вирішення поставлених завдань використано сукупність загальнонаукових і спеціальних методів. До спеціальних методів віднесено: методи теорії ймовірностей та математичної статистики; методи дискретної математики; методи теорії скінченних полів і лінійної алгебри; методи комп'ютерного моделювання; методи експериментального дослідження.

Об'єктом дослідження є процес захищеного передавання перестановок в умовах високої інтенсивності шуму в каналі зв'язку.

Предмет дослідження – метод і моделі системи захищеного інформаційного обміну з нероздільним факторіальним кодуванням даних.

2. Формулювання наукового завдання, нове розв'язання якого отримано в дисертації.

У дисертаційній роботі вирішено науково-технічну задачу, що полягає у забезпеченні захищеного інформаційного обміну в системах з нероздільним факторіальним кодуванням зашумленим каналом зв'язку

3. Наукові положення, розроблені особисто дисертантом, їхня новизна.

Дисертаційне дослідження містить у собі наступні наукові положення, розроблені особисто дисертантом:

– ***набув подальшого розвитку*** метод кадрової синхронізації нероздільних факторіальних кодів, що використовує як синхрокомбінацію перестановку чисел, яка має максимальне значення мінімальної відстані Хеммінга від її двійкового представлення до всіх її циклічних зсувів, а також кореляційну та мажоритарну обробку прийнятих фрагментів, де довжина фрагмента дорівнює довжині синхрокомбінації, який за рахунок використання ковзного вікна фіксованого розміру та врахування серії спрацювань підсистеми синхронізації дозволяє встановити кадрову синхронізацію приймальної та передавальної станцій системи інформаційного обміну за високої ймовірності бітової помилки та невідомого моменту початку приймання синхрокомбінацій передавача, забезпечуючи необхідні показники ймовірності правильної та хибної синхронізації;

– ***набула подальшого розвитку*** математична модель процесу виявлення синхрокомбінації систем передавання інформації з нероздільним факторіальним кодуванням даних, що використовують кореляційну та мажоритарну обробку прийнятих фрагментів, яка за рахунок дослідження механізмів перетворення синхрокомбінації в її зсув в умовах застосування приймачем ковзного вікна фіксованого розміру дозволяє оцінити ймовірності правильної та хибної кадрової синхронізації.

– ***вперше розроблено*** математичну модель скінченного поля квадратних матриць порядку 2 над скінченним полем простих чисел $\mathbb{Z}_p$, яка за рахунок збільшення порядку поля квадратних матриць до значення p^2, проте збереження порядку p поля $\mathbb{Z}_p$, в якому виконують операції перетворення, дозволяє підвищити стійкість криптографічних систем, які базуються на операціях у скінченому полі.

4. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій, які захищаються.

Наукові положення, висновки та рекомендації роботи обґрунтовано достатньою мірою. Обґрунтованість отриманих теоретичних результатів дисертації базується на використанні теорії систем передавання даних, теорії завадостійкого кодування, теорії ймовірностей і математичної статистики, статистичного аналізу, комбінаторики, функційного та об'єктно-орієнтованого програмування.

Для підтвердження висунутих наукових положень здобувачем виконано дослідні випробування на основі розроблених програмно-імітаційних моделях передавання даних, а також експериментів з використанням мови програмування MATLAB та його модуля Simulink для тестування розроблених методів і алгоритмів. Показано, що застосування запропонованих підходів забезпечує підвищення імовірності встановлення синхронізації, тим самим, підвищується стійкість комунікаційної системи в умовах впливу завад за умови не визначеного моменту приймання.

5. Рівень теоретичної підготовки здобувача, його особистий внесок у розв'язання конкретного наукового завдання. Рівень обізнаності здобувача з результатами наукових досліджень інших учених.

Дисертантом виконано змістовне дослідження предметної області, розглянуто основні методи забезпечення достовірного передавання інформації в комунікаційних системах. На основі опрацювання значної кількості літературних джерел, наукових публікацій, патентного пошуку автором роботи в максимальній мірі враховано наукові досягнення в обраному напрямку досліджень. Отримані результати свідчать про ґрунтовні теоретичні знання

дисертанта в області інформаційних технологій, комп'ютерних систем і мереж, математичного та комп'ютерного моделювання.

6. Наукове та практичне значення роботи.

У роботі запропоновано удосконалений метод кадрової синхронізації з нероздільним факторіальним кодуванням, який базується на використанні перестановки з максимальною мінімальною відстанню Хеммінга до її циклічних зсувів. Метод поєднує кореляційну та мажоритарну обробку фрагментів у межах ковзного вікна фіксованої довжини та враховує серію спрацювань, що забезпечує ефективну синхронізацію за умов високої ймовірності бітових помилок і невідомого моменту початку передавання. На основі методу розроблено алгоритм кадрової синхронізації з ковзним вікном та аналізом серії спрацювань, який забезпечує надійне встановлення синхронізму в симплексних каналах без узгодження початку передавання за високої ймовірності бітових помилок. Набула подальшого розвитку математична модель процесу виявлення синхрокомбінації, яка дозволяє оцінювати ймовірності правильної та хибної синхронізації в умовах шумового впливу. Вперше розроблено модель скінченного поля квадратних матриць другого порядку над полем простих чисел, що забезпечує підвищення криптостійкості систем, побудованих на факторіальному представленні. Запропоновано алгоритм перетворення квадратних матриць у перестановки, придатний для генерації ключів-перестановок у системах з НФКД. Створено макетний зразок системи обміну на базі мікроконтролера nRF52840 з використанням ISM-радіоканалу, який демонструє можливість стиснення та криптографічного захисту текстових повідомлень у вигляді перестановок. Розроблено програмний код для операцій над перестановками з використанням GPU (CUDA), що дозволяє пришвидшити криптографічні обчислення та адаптувати систему для реалізації на високопродуктивних обчислювальних платформах. Отримані результати можуть бути використані для побудови завадостійких та захищених систем інформаційного обміну без зворотного каналу зв'язку.

7. Використання результатів роботи.

Результати дисертаційного дослідження можуть бути впроваджені в практику побудови вбудованих та сенсорних систем зв'язку, де важлива синхронізація без зворотного каналу і забезпечення базового рівня криптографічного захисту, а також використані для розробки нових та удосконалення існуючих мережевих протоколів передавання даних в умовах високого рівня природних або штучних завад, трьохетапних криптографічних протоколів, зокрема, трьохетапного криптографічного протоколу на основі перестановок.

8. Повнота викладу матеріалів дисертації.

Основні результати дисертаційної роботи опубліковано в 11 наукових працях, серед яких: 8 наукових статей (з них 4 – у виданнях, індексованих у Scopus, і 4 – у фахових наукових виданнях України); 2 публікації у збірниках матеріалів міжнародних та всеукраїнських наукових конференцій; 1 підрозділ у колективній науковій монографії.

Повний перелік наукових публікацій:

[1] E. Faure, A. Baikenov, A. Skutskyi, D. Faure, і O. Abramkina, «Algorithms for reliable permutation transmission protocols in noisy communication channels», *CEUR Workshop Proceedings*, т. 3826, с. 40-49, 2024, doi: 10.5281/zenodo.15390412 (Scopus)

[2] E. Faure, A. Shcherba, A. Skutskyi, і A. Lavdanskyi, «A Finite Field of Square Matrices of Order 2», *CEUR Workshop Proceedings*, т. 3550, с. 306-312, 2023, doi: 10.5281/zenodo.15392022 (Scopus)

[3] E. Faure, A. Shcherba, A. Skutskyi, і A. Lavdanskyi, «A software model to generate permutation keys through a square matrix», *Вісник Черкаського державного технологічного університету*, т. 29, № 2, с. 10-23, 2024, doi: 10.62660/bcstu/2.2024.10

[4] E. Faure, A. Skutskyi, і A. Lavdanskyi, «Algorithms and simulation model for the synchronisation subsystem of the noise-resilient communication system based on permutations», *Вісник Черкаського державного технологічного університету*, т. 4, № 29, с. 62-74, 2024, doi: 10.62660/bcstu/4.2024.62

[5] A. Lavdanskyi, E. Faure, A. Skutskyi, і C. Bazilo, «Accelerating Operations on Permutations Using Graphics Processing Units», *Lecture Notes on Data Engineering and Communications Technologie*, т. 178, с. 3-12, 2023, doi: 10.1007/978-3-031-35467-0_1 (Scopus)

[6] A. Shcherba, E. Faure, A. Skutskyi, і O. Kharin, «Families of Square Commutative 2x2 Matrices», *CEUR Workshop Proceedings*, т. 3550, с. 289-296, 2023, doi: 10.5281/zenodo.15391901 (Scopus)

[7] А. О. Лавданський, Е.В. Фауре, С. Т. Тинимбаєв, і А. Б. Скуцький, «Система захищеного інформаційного обміну текстовими даними через радіоканал ISM-діапазону», *Вісник Черкаського державного технологічного університету*, т. 27, № 3, с. 41-48, 2022. doi: 10.24025/2306-4412.3.2022.267786

[8] Е. В. Фауре, А. Б. Скуцький, і А. О. Лавданський, «Імітаційна модель передавання текстових і аудіо повідомлень з використанням нероздільного факторіального кодування в середовищі Simulink», в *Challenges and threats to critical infrastructure*, Detroit, Michigan, USA:

NGO Institute for Cyberspace Research, 2023, с. 244-246. [Online]. Режим доступу: https://er.chdtu.edu.ua/bitstream/ChSTU/4539/1/Monograph-09-06-2023-Faure2.pdf

[9] Е. В. Фауре, А. Б. Скуцький, і А. О. Лавданський, «Імітаційна модель системи передавання інформації з нероздільним факторіальним кодуванням даних у середовищі Simulink», *Вісник Черкаського державного технологічного університету*, т. 27, № 4, с. 31-47, 2022, doi: 10.24025/2306-4412.4.2022.273385

[10] Е. В. Фауре і А. Б. Скуцький, «Розробка моделі трьохетапного криптографічного протоколу на основі перестановок», в *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доповідей XII Міжнародної науково-технічної конференції, Баку–Харків–Жиліна, 27–28 квітня 2022 року*, Харків: ХНУРЕ, 2022, с. 138. [Online]. Режим доступу: https://nure.ua/wp-content/uploads/conf-2022-akov/telecom_2022_volume_1.pdf

[11] Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, і О. О. Харін, «Протокол надійного передавання перестановок в умовах інтенсивних шумів у каналі зв'язку» в *Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2024): тези доповідей III Міжнародної науково-практичної інтернет-конференції*, Черкаси: ЧДТУ, 2024, с. 107. [Online]. Режим доступу : https://drive.google.com/file/d/15-8DffQpER_5F6TniHYNIDf2BjOPjehX/view?usp=drive_link

У друкованих працях, опублікованих у співавторстві, здобувачеві належать: [1], [11] – розвинуто математичну модель процесу виявлення синхрокомбінації із застосуванням ковзного вікна; [4] – набув подальшого розвитку метод кадрової синхронізації на основі кореляційної обробки з урахуванням ковзного вікна і серії спрацювань підсистеми синхронізації, досліджено ефективність застосування розробленого методу синхронізації в симплексному каналі передавання з імовірністю бітової помилки 0.4; [2], [6] – теоретично обґрунтовано принципи побудови скінченного поля квадратних матриць порядку 2 для криптографічних застосувань, визначено шість сімейств матриць із загальної лінійної групи порядку 2 над простим полем цілих чисел за модулем з комутативною операцією множення; [3] – розроблено та досліджено алгоритми перетворення квадратних матриць порядку 2 в перестановки, наведені статистичні властивості отриманих результатів перетворення, визначено найбільш ефективний алгоритм перетворення матриць у перестановки за критерієм рівномірності розподілу отриманих номерів

перестановок; [5] – досліджено ефективність виконання операцій над перестановками за допомогою графічних процесорів (GPU) в порівнянні з центральним процесором (CPU), перевірено стійкість трьохетапного протоколу на перестановках до атаки методом перебору ключових перестановок; [7] – створено систему захищеного інформаційного обміну текстовими даними через радіоканал ISM-діапазону на основі НФКД, наведено опис алгоритмів перетворення тексту в перестановки і навпаки; [8], [9] – розроблено та досліджено імітаційні моделі що використовують канал зв'язку з незалежними бітовими помилками для передачі текстової або аудіо інформації у вигляді перестановок; [10] – створено імітаційну модель трьохетапного криптографічного протоколу на основі перестановок.

Результати аналізу роботи, в тому числі за допомогою перевірки тексту дисертації з використанням системи UNICHECK на пошук та аналіз текстових збігів, свідчать про відповідність дисертації принципам академічної доброчесності

9. Апробація матеріалів дисертації відбувалась на наступних міжнародних наукових конференціях: XII Міжнародній науково-технічній конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» (Баку–Харків–Жиліна, 27–28 квітня 2022 року); Міжнародна науково-практична конференція «Information Technology for Education, Science and Technics» (ITEST 2022); II Міжнародна науково-практична конференція «Виклики та загрози об'єктам критичної інфраструктури» (Київ, 29-30 червня, 2023); Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II-2023), (Kyiv, 26 October 2023); Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2024), (Kyiv, 26 October 2024); III Міжнародній науково-практичній інтернет-конференції «Інновації та перспективні шляхи розвитку інформаційних технологій» (ІПШРІТ-2024), (Черкаси, 22 листопада 2024 року).

10. Оцінка мови та стилю дисертації.

Дисертацію написано з дотриманням норм і правил граматики, а стиль викладу в ній матеріалів досліджень, наукових положень, висновків і рекомендацій забезпечує легкість і доступність їх сприйняття.

Дисертація повною мірою відповідає пунктам 6–8 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради про присудження ступеня доктора філософії в Черкаському державному технологічному університеті». Робота містить нові науково обґрунтовані результати проведених здобувачем досліджень, які виконують конкретне наукове завдання, що має істотне значення для галузі знань 12 Інформаційні

технології.

Дисертацію виконано державною мовою та відповідно до наявних вимог щодо оформлення.

11. Відповідність змісту дисертації освітньо-науковій програмі, з якої вона подається до захисту.

Зміст дисертації повністю відповідає спеціальності 123 Комп'ютерна інженерія, освітньо-науковій програмі «Комп'ютерні системи та мережі».

12. Рекомендація дисертації до захисту.

Враховуючи рівень наукових досліджень, актуальність теми роботи та наукову новизну отриманих результатів, учасники фахового семінару кафедри інформаційної безпеки та комп'ютерної інженерії одноголосно ухвалили рішення затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Скуцького Артема Борисовича на тему: «Метод і моделі системи захищеного інформаційного обміну з нероздільним факторіальним кодуванням даних» для здобуття ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія галузі знань 12 Інформаційні технології та рекомендувати до захисту в разовій спеціалізованій вченій раді Черкаського державного технологічного університету для здобуття ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

У голосуванні брали участь 18 осіб. Результати голосування:

«ЗА» – 18,

«ПРОТИ» – немає,

УТРИМАЛИСЬ – немає.

Головуючий:
завідувач кафедри інформаційної безпеки
та комп'ютерної інженерії,
д.т.н, професор

Віра БАБЕНКО