модифікуються сингулярні числа блоків за допомогою бітової послідовності ЦВЗ, виконується зворотне відображення яскравості пікселів у фізичну область.

На рис.1, як приклад, зображено спеціальну схему: фігура – модельна область – область комплексного потенціалу.

Висновки. Запропонований підхід забезпечує високу робастність ЦВЗ до топологічних атак та стиснення JPEG. Використання конформної сітки як геометричного ключа забезпечує можливість надійно захищати приховану інформацію від вилучення.

1. Бомба А.Я., Бойчура М.В. Методи комплексного аналізу в задачах ідентифікації: монографія. Рівне: НУВГП, 2020. 188 с.
2. Liu R., Tan T. An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia*. – 2002. – V. 4, №1. – P. 121-128.

Проблематика узагальненої оцінки методів криптографічного захисту інформації

УДК 004.056.55

Віра Тітова[1], Володимир Анікін[2]

Хмельницький національний університет,
[1]titovav@khmnu.edu.ua, [2]anikin_volodymyr@khmnu.edu.ua

Існує значна розбіжність в підходах до узагальненої оцінки методів криптографічного захисту інформації (КЗІ). Аналіз досвіду проведення як вітчизняних, так і зарубіжних криптографічних конкурсів, в межах яких очевидною була необхідність строгого критеріального порівняння запропонованих методів-претендентів між собою, показує неузгодженість підходів до такої порівняльної оцінки. Часто таке порівняння методів криптографічного захисту фактично зводиться до порівняння засобів КЗІ, оскільки у якості критеріїв порівняння обирається, як приклад, швидкодія роботи, чи інша фізична величина, що емпірично вимірюється на прототипі засобу КЗІ. Подібний підхід простежувався, зокрема, у конкурсних процедурах, пов'язаних із вибором стандарту ДСТУ 7624:2014 «Калина», де поряд із криптографічними властивостями враховувалися також показники ефективності реалізацій.

З одного боку, такий підхід може бути виправданий з точки зору прикладної спрямованості порівняння, де той чи інший метод КЗІ не несе жодного практичного сенсу у суто теоретичному вимірі. Проте, з іншого боку, коли необхідність узагальненого порівняння виникає в ході певних науково-дослідних робіт, в межах яких, наприклад, є необхідність підібрати методи КЗІ як компонент деякої більш глобальної системи, а об'єктом оцінювання виступають не готові засоби, чи навіть їх прототипи, а виключно теоретичні абстракції, узагальнені характеристики яких необхідно порівняти, то згаданий емпірично-орієнтований підхід не може бути застосований.

Одним із аргументів, щодо принципової розбіжності у підходах порівняння методів та засобів КЗІ є те, що при дослідженні кількох різних реалізацій засобів

КЗІ, на базі одного і того ж самого методу, результати їх порівняння між собою можуть принципово відрізнятися. Це може бути зумовлено різними платформами, архітектурами, рівнями реалізацій, ступенями оптимізації та іншими чинниками, що є релевантними по відношенню до конкретного створеного засобу КЗІ.

Також в ході проєктування засобів КЗІ можуть бути створені додаткові вразливості, пов'язані із особливостями платформи, середовища чи будь-яких інших сторонніх каналів. Проте ці вразливості не будуть релевантні із теоретичними засадами функціонування методів КЗІ, що лежать в основі проблемних рішень.

Для вирішення зазначеної проблематики пропонується розробити критеріальну систему узагальненої оцінки методів КЗІ, яка б не опиралась в своїх розрахунках на ті чи інші емпіричні властивості прототипів, особливості реалізацій та інші практичні характеристики.

Принципово невірним було б рішення по створенню такої системи теоретичної оцінки виключно шляхом відкидання від інших загальноприйнятих систем оцінювання тих критеріїв, що базуються на емпіричних властивостях реалізацій засобів КЗІ, оскільки навіть суто теоретична узагальнена оцінка повинна зберігати широку різнобічність критеріїв, для того щоб результати такої оцінки були справді інформативними.

Для створення системи узагальненої оцінки методів КЗІ пропонується провести аналіз найбільш поширених критеріїв оцінки криптографічних примітивів, систем та протоколів, умовно розподілити їх на дві основних групи: ті, що спрямовані на теоретично-математичні властивості, та ті, що спрямовані на властивості конкретних реалізацій.

Перша група критеріїв може бути використана як базова складова запропонованого узагальненого методу оцінки.

Друга група потребує конвертації критеріїв у відповідники, що зберігають логічну сферу спрямування оцінки, проте опираються не на емпіричні властивості реалізації, а на деякі їх теоретично-математичні аналоги. Так, наприклад, критерій швидкодії роботи може бути приведено до критерію обчислювальної складності алгоритму тощо.

Для забезпечення гнучкості така критеріальна система може передбачати використання вагових коефіцієнтів. Вони можуть задаватися в усередненому варіанті або коригуватися відповідно до вимог конкретної задачі, якщо певний критерій має підвищену або знижену значущість.

Використання нормалізованих значень критеріїв і вагових коефіцієнтів дозволить отримати формалізований інтегральний показник, придатний для порівняння з іншими результатами, отриманими за тією самою процедурою.

Таким чином, проблематика узагальненої оцінки методів КЗІ є актуальною, в тому числі у вітчизняному науковому полі, оскільки станом на зараз є досить поширеною практика змішування оцінки методів та засобів КЗІ. Саме по собі таке змішування не є проблемою та може бути виправдане у вирішенні прикладних задач, в яких важливим є комплекс теоретичних та емпіричних властивостей об'єкту дослідження. Проте в інших задачах, наприклад у сфері теоретичного моделювання систем або протоколів КЗІ, де необхідна

узагальнена оцінка складових криптографічних елементів, без прив'язки до їх реалізацій, розділення підходів оцінки методів та засобів є необхідним. Наведені пропозиції щодо створення такої узагальненої системи оцінювання можуть лягти в основу окремого методу.

1. Prvulovic P, Radosavljevic N, Babic D, Drajic D. HERMEES: A Holistic Evaluation and Ranking Model for Energy-Efficient Systems Applied to Selecting Optimal Lightweight Cryptographic and Topology Construction Protocols in Wireless Sensor Networks. Sensors. 2025; 25(9):2732.
2. The concept of nonlinear cryptographic primitives, their steganographic applications, and related areas of use / Volodymyr Anikin, Serhii Lienkov, Ihor Muliar, Volodymyr Dzhulii, Oleksandr Sieliukov, Yaroslav Melnyk. EUREKA: Physics and Engineering. 2025. № 5. P. 190-204.

Сучасні підходи до безперервної автентифікації користувачів на основі динаміки рухів комп'ютерної миші

УДК 004.056.5:57.087.1

Олександр Корченко[1], Антон Герасименко[2], Імад Ірейфідж[3]

Державний університет інформаційно-комунікаційних технологій,
[1]agkorchenko@gmail.com, [2]anton.hrsmnk@gmail.com,
[3]dr.imad.education@gmail.com

Традиційні методи автентифікації (паролі, токени) стають вразливими до методів соціальної інженерії та витоку даних. Поведінкова біометрія пропонує концепцію безперервної автентифікації (Continuous Authentication), яка дозволяє верифікувати особу не лише в момент входу в систему, а протягом усієї сесії роботи. Рух миші є унікальним для кожної людини через індивідуальні особливості нейромоторної координації, що робить його перспективним об'єктом дослідження.

Методологія вилучення ознак (Feature Extraction) при автентифікації користувачів за рухом миші. Для ідентифікації користувача координати курсора x та y перетворюються на набір статистичних та кінематичних ознак. Основні параметри включають: швидкісні показники (миттєва швидкість v та прискорення a), траєкторні ознаки (кривизна руху, кутова швидкість та "джиттер", тобто мікротремтіння), часові ознаки (час реакції між появою стимулу та початком руху, тривалість пауз - dwell time), операційні ознаки (частота кліків, швидкість подвійного натискання, манера прокручування коліщатка).

Основні алгоритми машинного навчання та класифікації при автентифікації користувачів за рухом миші. Сучасні дослідження фокусуються на двох підходах до навчання моделей:

Однокласова класифікація (One-Class Classification): Модель навчається лише на даних легітимного користувача (наприклад, алгоритм Isolation Forest або One-Class SVM). Система шукає аномалії, які свідчать про те, що за комп'ютером перебуває інша особа.