розумного міста, екологічної безпеки та довіри населення. Подальші дослідження доцільно спрямувати на кількісне оцінювання ризиків, інтеграцію з SIEM/SOC-рішеннями та виявлення фальсифікованих або аномальних даних.

1. Bacco M., Delmastro F., Ferro E., Gotta A. Environmental monitoring for smart cities. IEEE Sensors Journal. 2017. Vol. 17(23). P. 7767-7774.
2. Zanella A. et al. Internet of Things for smart cities. IEEE Internet of Things Journal. 2014. Vol. 1(1). P. 22-32.
3. Sicari S. et al. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks. 2015. Vol. 76. P. 146-164.
4. Demertzi V., Demertzis S., Demertzis K. An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities. Applied Sciences. 2023. Vol. 13(2). Article 790.

Застосування методу PERT для оцінки трудомісткості задач у мобільних застосунках управління проєктами

УДК 004.42

Стасюк Сергій[1], Мудрик Іван[2]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]serhii_stasiuk1107@tntu.edu.ua, [2]i1mudryk@tntu.edu.ua

Управління сучасними IT-проєктами стикається з двома критичними викликами: проблемою точної оцінки трудомісткості задач та необхідністю гарантування конфіденційності проєктної інформації. Мобільні застосунки для трекінгу задач обробляють надзвичайно чутливі корпоративні дані (строки, розподіл ресурсів, архітектурні інсайти, бізнес-процеси). Відповідно, інструмент планування має не лише вирішувати проблему зриву дедлайнів, але й відповідати суворим вимогам інформаційної безпеки.

Точна оцінка трудомісткості задач є одним із ключових викликів у сучасному IT-проєктному менеджменті. Сучасні менеджери проєктів все частіше використовують мобільні застосунки для трекінгу задач та управління ресурсами. Однак, однією з найскладніших задач залишається точна оцінка трудомісткості на етапі планування або безпосередньо "на ходу" (наприклад, під час дейлі-мітингів чи зустрічей з клієнтами). Традиційні однопунктові методи систематично ігнорують невизначеність і ризики, що призводить до зривів термінів та перевитрати бюджету. Метод PERT (Program Evaluation and Review Technique) вирішує цю проблему через три сценарії для кожної задачі: оптимістичний (О), реалістичний (Р) та песимістичний (П). Очікуваний час (Т) обчислюється за формулою бета-розподілу:

$$T = \frac{О + 4Р + П}{6}$$

Така зважена оцінка враховує статистичний розподіл можливих результатів і є суттєво точнішою за однопунктове прогнозування [1].

Аналіз популярних інструментів (Trello, Jira, Asana) показує, що вони орієнтовані на хмарну синхронізацію, що розширює поверхню атаки (attack

surface) та створює ризики витоку даних через компрометацію мережевого трафіку або хмарних баз даних.

Аналіз наявних інструментів (Trello, Jira, Asana, Todoist) засвідчує відсутність вбудованої підтримки методу трьох точок як основного механізму планування, а також обмежені можливості захисту локальних даних. Більшість рішень орієнтовані на командну роботу з розгалуженою функціональністю, що робить їх надлишковими для індивідуального розробника чи малої команди [2].

Для вирішення цих прикладних проблем захисту інформації, пропонується децентралізована архітектура мобільного застосунку за патерном MVVM (Model-View-ViewModel), де логіка PERT інкапсульована незалежно від UI. Головною особливістю є "offline-first" підхід: усі три оцінки та метадані проєкту зберігаються виключно в реляційній базі даних на самому пристрої (наприклад, SQLite/Room для Android) без примусової прив'язки до хмарних сервісів. Це радикально мінімізує загрози, пов'язані з безпекою хмарних обчислень.

Зберігання даних локально вимагає надійного захисту кінцевої точки (endpoint security). Для протидії криміналістичному аналізу мобільних пристроїв та несанкціонованому вилученню даних (наприклад, у разі втрати смартфона) застосовуються методи прикладної криптології:

- Шифрування "Data at Rest": Використання бібліотек типу SQLCipher для повного AES-256 шифрування локальної бази даних SQLite.
- Захист ключів доступу: Інтеграція з апаратними сховищами ключів мобільних ОС (Android Keystore / Apple Secure Enclave) для генерації та безпечного зберігання криптографічних ключів.
- Біометричне розмежування доступу: Додатковий рівень аутентифікації на рівні самого застосунку для підтвердження особи користувача перед доступом до проєктних даних.

З точки зору інформаційної безпеки та захисту даних, мобільні застосунки для управління проєктами обробляють чутливі дані про терміни, ресурси та бізнес-процеси організації. Сучасні стандарти кібербезпеки (NIST, ISO/IEC 27001) вимагають шифрування локального сховища, розмежування прав доступу та захисту від несанкціонованого втручання. Інтеграція таких принципів на етапі проєктування застосунку дозволяє мінімізувати ризики витоку корпоративних даних [3].

Бізнес-аналітика на основі PERT-оцінок відкриває додаткові можливості для прийняття управлінських рішень. Накопичені статистичні дані про реальне та прогнозоване виконання задач дозволяють виявляти систематичні відхилення в плануванні, оцінювати продуктивність і коригувати майбутні оцінки. Такий підхід перетворює застосунок з інструменту планування на аналітичну платформу підтримки рішень.

Інтеграція вищезазначених принципів на етапі проєктування («Security by Design») дозволяє створити продукт, що відповідає сучасним стандартам кібербезпеки, зокрема концепціям NIST та ISO/IEC 27001 у частині розмежування прав доступу, захисту від несанкціонованого втручання та забезпечення конфіденційності інформаційних активів.

1. Wysocki, R. K. (2019). Effective Project Management: Traditional, Agile, Extreme, Hybrid. — New Jersey: Wiley. — 696 p.
2. Phillips, J. (2021). PMP Project Management Professional Study Guide. — New York: McGraw-Hill. — 592 p.
3. Ross, R. S., et al. (2020). Security and Privacy Controls for Information Systems and Organizations. — NIST SP 800-53 Rev. 5. — 492 p.
4. Bryk O., Mudryk I., Holubovskyi M., Stoianov Y. Machine learning models and methods aspects of processing unstructured data. Proceedings of the 1st International Workshop on Bioinformatics and Applied Information Technologies (BAIT 2024), Zboriv, Ukraine, 2024. 2024. P. 64–74.

Гібридний метод приховування ЦВЗ у цифрових зображеннях

УДК 004.056.5

Ірина Борисенко[1], Даніїл Стрельченко[2]

Національний університет «Одеська політехніка»,
[1]borisenko.i.i@op.edu.ua, [2]10182258@stud.op.edu.ua

Для побудови стійких систем ЦВЗ використовуються різні підходи перетворення контейнера, наприклад, дискретне перетворення Фур'є (ДПФ) та сингулярний розклад матриць (SVD), які демонструють високу ефективність у задачах спектрального аналізу та приховування даних. ДПФ дозволяє перейти у частотну область, забезпечуючи стійкість ЦВЗ до геометричних атак, SVD виділяє стабільний енергетичний кістяк зображення (сингулярні числа), який є надзвичайно стійким до стиснення алгоритмом JPEG та шумових перешкод.

Актуальність теми полягає в необхідності інтеграції переваг обох математичних апаратів у єдину комбіновану (гібридну) схему, яка забезпечуватиме максимальну стійкість захисту авторських прав до комплексних атак, зберігаючи при цьому високу візуальну якість зображення.

Метою роботи є розробка комбінованого стеганографічного алгоритму вбудовування ЦВЗ, що поєднує частотну декомпозицію на основі ДПФ і SVD перетворень та дослідження його стійкості до стеганоаналітичних атак.

Доведено [1], що перше (найбільше) сингулярне число S_{11} сингулярного розкладу матриці контейнера концентрує в собі основну енергію зображення, що робить його модифікацію надзвичайно стійкою до зовнішніх впливів, цю властивість будемо використовувати в алгоритмі вбудовування ЦВЗ.

Алгоритм вбудовування. Зображення-контейнер розбивається на незалежні блоки розміром 8×8 пікселів, для кожного блоку виконується ДПФ, до коефіцієнтів середньої частоти застосовується кільцева маска з радіусами R_{min} та R_{max}, яка виділяє коефіцієнти, які є найбільш оптимальними для приховування даних, після чого до виділеного кільця застосовується SVD. Значення S_{11} ділиться на коефіцієнт сили вбудовування α – одержуємо S'_{11}. Якщо секретний біт дорівнює 0, значення S'_{11} округлюється до найближчого парного числа, якщо 1 – до непарного. Отримуємо матрицю S_{new}. Далі робимо зворотні перетворення: $US_{new}V^T$ та зворотне ДПФ. Відновлюється повідомлення шляхом зворотних перетворень: ДПФ –> кільце з радіусами R_{min} та R_{max} –> SVD виділеного кільця частот; зчитується перше сингулярне число,