МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

РАДІОТЕХНІКА

Всеукраїнський
міжвідомчий науково-технічний збірник

Засновано в 1965 р.

В И П У С К 2 0 6

Харків
Харківський національний
університет радіоелектроніки
2021

УДК 621.3

Збірник включено до Переліку наукових фахових видань України, категорія "Б", технічні та фізико-математичні науки (затверджено наказами МОНУ від 17.03.2020 № 409; від 02.07.2020 № 886; від 24.09.2020 № 1188) за спеціальностями: 171 – Електроніка; 172 – Телекомунікації та радіотехніка; 173 – Авіоніка; 125 – Кібербезпека; 151 – Автоматизація та комп'ютерно-інтегровані технології; 152 – Метрологія та інформаційно-вимірювальна техніка; 153 – Мікро- та наносистемна техніка; 163 – Біомедична інженерія; 105 – Прикладна фізика та наноматеріали.

Сборник включен в Перечень научных профессиональных изданий Украины, категория «Б», технические и физико-математические науки (утверждено приказами МОНУ от 17.03.2020 № 409, от 02.07.2020 № 886, от 24.09.2020 № 1188) по специальностям: 171 – Электроника; 172 – Телекоммуникации и радиотехника; 173 – Авионика; 125 – Кибербезопасность; 151 – Автоматизация и компьютерно-интегрированные технологии; 152 – Метрология и информационно-измерительная техника; 153 – Микро- и наносистемная техника; 163 – Биомедицинская инженерия; 105 – Прикладная физика и наноматериалы.

The collection is included in the List of scientific professional publications of Ukraine, category «Б», technical and physical-mathematical sciences (approved by orders of the Ministry of Education and Science from 17.03.2020 № 409; from 02.07.2020 № 886; from 24.09.2020 № 1188) by specialties: 171 – Electronics; 172 – Telecommunications and Radio Engineering; 173 – Avionics; 125 – Cybersecurity; 151 – Automation and Computer-Integrated Technologies; 152 – Metrology and Information-Measuring Equipment; 153 – Micro- and Nanosystem Technology; 163 – Biomedical Engineering; 105 – Applied Physics and Nanomaterials.

Сайт: rt.nure.ua

Реєстраційне свідоцтво КВ № 12098-969 ПР від 14. 12. 2006.

За зміст статті відповідальні автори.

Відповідальні випускові: *І.Д. Горбенко, д-р техн. наук, проф., І.В. Свид, канд. техн. наук, доц.*
Технічний секретар *О.С. Полякова.*

Рекомендовано Вченою радою Харківського національного університету радіоелектроніки, протокол №8/6 від 24.09.2021.

Адреса редакційної колегії: Харківський національний університет радіоелектроніки (ХНУРЕ), просп. Науки, 14, Харків, 61166, тел. (0572) 7021-397.

Збірник «Радіотехніка» включено до Каталогу передплатних видань України, передплатний індекс ***08391.***

ЗМІСТ

МОДЕЛІ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ

ІНФОРМАЦІЙНІ МЕТОДИ РАДІОТЕХНІКИ

БІОМЕДИЧНА РАДІОЕЛЕКТРОНІКА

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТЕХНОЛОГІЇ

CONTENT

МОДЕЛІ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

УДК 681.3.06 **DOI:10.30837/rt.2021.3.206.01**

О.В. ПОТІЙ, д-р техн. наук, Ю.І. ГОРБЕНКО, канд. техн. наук,
О.А. ЗАМУЛА, д-р техн. наук, К.В. ІСІРОВА

АНАЛІЗ МЕТОДІВ ОЦІНКИ І УПРАВЛІННЯ РИЗИКАМИ КІБЕР- І ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вступ

Ефективність роботи установи, підприємства, компанії, організації безпосередньо залежить від якості і оперативності управління виробництвом (бізнес-процесами). У сферу управління включаються різні ресурси – інформація, персонал, технологічні процеси, техніка. Загальновизнаним стратегічним чинником зростання конкурентоспроможності компанії є ефективне застосування інформаційних технологій (ІТ). При цьому застосування ІТ немислимо без підвищеної уваги до питань кібер- і інформаційної безпеки. Руйнування інформаційного ресурсу, його тимчасова недоступність або несанкціоноване використання можуть завдати організації значних матеріальних збитків. Для організацій, комп'ютерні мережі яких налічують не один десяток комп'ютерів з різними апаратними платформами, програмним забезпеченням, операційними системами, додатками тощо, на перше місце виступає завдання управління безліччю різноманітних захисних механізмів в таких гетерогенних корпоративних мережах. Складність мережевої інфраструктури, різноманіття даних і додатків призводять до того, що при реалізації системи інформаційної безпеки за межами уваги адміністраторів безпеки можуть виявитися багато загроз. Тому необхідне здійснення надійного і ефективного управління комп'ютерними мережами і засобами мережевої безпеки.

На перший план при вирішенні задач забезпечення інформаційної і кібербезпеки, а також приватності виходить створення системи управління інформаційною безпекою (СУІБ), яка охоплює всю інфраструктуру компанії.

СУІБ дозволяє (надає можливості) [1]:

- централізовано і оперативно надавати керуючі впливи на всю інформаційну інфраструктуру;
- проводити регулярний аудит і всеохоплюючий моніторинг, що дає об'єктивну інформацію про стан кібер- і інформаційної безпеки для прийняття оперативних рішень;
- накопичувати статичні дані про роботу інформаційної інфраструктури для прогнозування її розвитку;
- оцінювати ризики інформаційної безпеки.

Управління ризиками безпеки та приватності вимагає участі всієї організації – від старших керівників, які визначають стратегічне бачення, цілі та задачі для організації найвищого рівня, до керівників середнього рівня, які здійснюють планування, виконання та управління проєктами, та осіб, які розробляють, впроваджують, використовують і підтримують системи і процеси.

1. Загальні положення щодо оцінки і управління ризиками кібер- і інформаційної безпеки

Активна діяльність міжнародних організацій зі стандартизації підтверджує важливість питань забезпечення кібер- і інформаційної безпеки в системах інформаційних технологій та постійного удосконалення моделей, методів та механізмів безпеки інформаційних технологій. Основний підхід до забезпечення інформаційної безпеки в ІС – стратегія захисту на основі ризику (Risk-Based Protection Strategy). Успішні програми управління ризиками перед-

бачають побудову системи забезпечення інформаційної безпеки, яка інтегрована в організаційну і технічну інфраструктуру. Це вимагає здійснення координованого комплексу заходів, спрямованих на реалізацію вимог безпеки. Ці заходи захисту мають реалізуватися як елементи загального управління, що здійснюється організацією.

Роль управління ризиками стосовно кібер- і інформаційної безпеки під час функціонування та використання інформаційної системи є критичною для досягнення організацією своїх стратегічних цілей та задач.

Виходячи з цих позицій NIST США розробив та впроваджує як методологічну основу забезпечення інформаційної та кібербезпеки концепцію Risk Management Framework (RMF). Концепція RMF впроваджує структурований гнучкий підхід до управління ризиками, що пов'язаний із впровадженням інформаційних систем у бізнес-процеси організації. Концепція RMF викладена у NIST SP 800-37 (Rev 2) та є еволюційним розвитком концепції життєвого циклу системи безпеки (System Security Lifecycle), що використовується NIST з початку 2000-х років. Ця концепція об'єднує серію документів NIST SP 800-XX.

У 2018 р. у зв'язку з актуалізацією питання захисту персональних даних, прийняттям основних положень забезпечення кібербезпеки, впровадженням моделі довірчих систем NIST розпочав перегляд багатьох документів серії NIST SP 800-XX та видав нову версію NIST SP 800-37 – Risk Management Framework in Information Systems and Organizations [1]. У цьому документі впроваджуються принципи управління ризиками та життєвого циклу систем для забезпечення безпеки та приватності.

У нинішній редакції RMF акцентує увагу на управлінні ризиками, створенні умов для забезпечення безпеки та приватності в інформаційних системах на всіх етапах життєвого циклу проєктування системи (SDLC), підтримки інформування про безпеку та приватність на постійний основі за допомогою безперервних процесів моніторингу безпеки, наданні інформації вищому керівництву та керівникам відповідних підрозділів для прийняття рішень стосовно ризиків щодо процесів, ресурсів, персоналу організації, які виникають під час експлуатації та використання систем.

Основні цілі впровадження RMF:

- забезпечення повторюваного процесу забезпечення інформаційної безпеки у відповідності до чинних ризиків;
- впровадження цілісного загальносистемного підходу до управління ризиками безпеки та приватності;
- впровадження єдиної методики класифікації (категоризації) інформаційних систем та загальних заходів безпеки;
- забезпечення управління ризиками в режимі реального часу через впровадження надійних безперервних процесів моніторингу безпеки;
- впровадження засобів автоматизації для забезпечення керівництва необхідною інформацією для прийняття ефективних, економічно доцільних рішень на основі ризиків для ІС, що підтримують місію та бізнес функції організації;
- забезпечення інтеграції вимог безпеки та приватності, заходів захисту в архітектуру підприємства, SDLC, процеси закупівель та постачання, процеси системного інжинірингу;
- об'єднання процесів управління ризиками на рівні організації та бізнес-процесів з процесами управління ризиками на рівні інформаційних систем;
- встановлення відповідальності та спостереження за впровадженням та реалізацією заходів безпеки в ІС.

Під час планування системи управління інформаційною безпекою організація повинна, у відповідності до [2], визначити сукупність методів захисту інформації і організацію проведення аудиту системи управління інформаційної безпеки, визначити ризики та можливості, які потрібно мати на увазі, щоб:

а) гарантувати, що система управління інформаційною безпекою може досягти запланованого результату(-ів);

б) запобігти або зменшити небажані ефекти;

в) досягти постійного вдосконалення.

Організація повинна планувати:

г) дії, які стосуються цих ризиків та можливостей;

д) як саме:

- інтегрувати й упровадити ці дії до процесів її системи управління інформаційною безпекою;

- та оцінювати ефективність цих дій.

Організація повинна визначити та застосовувати процес оцінювання ризиків інформаційної безпеки, який:

а) встановлює та підтримує критерії ризиків інформаційної безпеки, які містять:

– критерії прийняття ризиків; і

– критерії для виконання оцінки ризиків інформаційної безпеки;

б) гарантує, що повторні оцінки ризиків інформаційної безпеки призводять до послідовних, дійових та порівняльних результатів;

в) ідентифікує ризики інформаційної безпеки:

- застосовує процес оцінювання ризиків інформаційної безпеки для ідентифікації ризиків, пов'язаних із втратою конфіденційності, цілісності й доступності в межах сфери застосування системи управління інформаційною безпекою;

- ідентифікує власників ризиків;

г) виконує аналіз ризиків інформаційної безпеки:

- оцінює потенційні наслідки, які будуть результатом реалізації ідентифікованих ризиків;

- оцінює практичну імовірність появи ідентифікованих ризиків;

– визначає рівні ризиків;

д) оцінює ризики інформаційної безпеки:

- порівнює результати аналізу ризиків з визначеними критеріями ризиків; та

- визначає пріоритети проаналізованих ризиків для оброблення ризиків.

Склад і наповнення зазначених процесів залежить від використовуваної методики оцінки та управління ризиками:

Організація повинна визначити та застосовувати процес оброблення ризиків інформаційної безпеки задля:

а) вибору доречних опцій оброблення ризиків інформаційної безпеки з урахуванням результатів оцінки ризиків;

б) визначення всіх заходів безпеки, які необхідно впровадити для вибраної(-их) опції(-ій) оброблення ризиків;

в) порівняння визначення заходів безпеки з наведеними в додатку А [2], і підтвердження, що не було опущено потрібних заходів безпеки;

г) підготовки Положення щодо застосовності, яке містить:

- необхідні заходи безпеки;

- обґрунтування для їх застосування;

- впровадження необхідні заходи безпеки чи ні;

- обґрунтування для виключень заходів безпеки, наданих у додатку А [2] «Цілі заходів безпеки та заходи безпеки» стандарту;

д) розробку плану оброблення ризиків інформаційної безпеки;

е) отримання від власників ризиків підтвердження плану обробки ризиків інформаційної безпеки та згоди на залишкові ризики інформаційної безпеки.

Організація повинна ідентифікувати і оцінити можливості по обробці ризиків. Можливі дії включають в себе наступне [2]:

- застосування відповідних заходів захисту;
- усвідомлене і об'єктивне прийняття ризиків, за умови, що вони строго відповідають

політиці організації та критеріям прийняття ризиків;

- уникнення ризиків;
- перенесення об'єднаних бізнес-ризиків на інші сторони, наприклад страховиків, постачальників.

Методологія визначення оцінки ризиків може бути якісною або кількісною, або деякою комбінацією. Якісна оцінка дуже часто використовується для отримання загального рівня ризику і виокремлення головних ризиків. При якісному підході не використовуються кількісні або грошові вираження для об'єкта оцінки. Замість цього об'єкту оцінки присвоюється показник, що проранжовано за трибальною (низький, середній, високий), п'ятибальною або десятибальною шкалою (0...10). Для збору даних при якісній оцінці ризиків застосовуються опитування цільових груп, інтерв'ювання, анкетування, особисті зустрічі.

При кількісному підході всім елементам оцінки ризиків привласнюють конкретні і реальні кількісні значення. Об'єктом оцінки може бути цінність активу в грошовому вираженні, ймовірність реалізації загрози, збитки від реалізації загрози, вартість захисних заходів та ін.

Кількісний підхід до оцінки ризиків може включати такі етапи:

1. Визначити цінність інформаційних активів в грошовому вираженні.

2. Оцінити в кількісному вираженні потенційний збиток від реалізації кожної загрози щодо кожного інформаційного активу.

3. Визначити ймовірність реалізації кожної із загроз ІБ.

Для цього можна використовувати статистичні дані, опитування співробітників і зацікавлених осіб. У процесі визначення ймовірності розрахувати частоту виникнення інцидентів, пов'язаних з реалізацією даної загрози ІБ за контрольний період (наприклад, за один рік).

4. Визначити загальний потенційний збиток від кожної загрози щодо кожного активу за контрольний період. Значення розраховується шляхом множення разового шкоди від реалізації загрози на частоту реалізації загрози.

5. Провести аналіз отриманих даних по збитку для кожної загрози.

Ідентифікація критеріїв ризику визначає прийняття рішень щодо характеру можливих наслідків та способу їх вимірювання. При визначенні критеріїв необхідно визначити, за якими критеріями прийматимуться рішення щодо необхідності оброблення ризику та критерії, за якими будуть прийматися рішення щодо допустимості чи прийняття ризику. Наявні на сьогодні методи оцінки ризиків в переважній кількості засновані на статистичних підходах. У більшості країн подібна статистика не ведеться, як на державному рівні, так і на рівні підприємств. Саме це обмежує можливості засобів оцінки, наприклад відсутність інформації для використання вхідних даних для оцінки ризику. Загальне оцінювання ризику дає змогу впроваджувати необхідні міри на рівні підрозділів, проєктів, конкретних ризиків або на рівні організації в цілому. Після завершення загального оцінювання ризику провадять обробляння ризику, що передбачає прийняття заходів, які дають можливість зменшити ймовірність виникнення ризиків та їх вплив на систему.

Ризики інформаційної безпеки характеризуються двома параметрами: потенційним збитком для організації та ймовірністю реалізації. Використання для аналізу ризиків сукупності цих двох характеристик дозволяє порівнювати ризики з різними рівнями шкоди і ймовірності, приводячи їх до вигляду зрозумілому для осіб, котрі приймають рішення щодо мінімізації ризиків в організації.

2. Критерії вибору методів оцінки і управління ризиками інформаційної і кібербезпеки

При створенні системи управління ІР постає питання вибору заходів захисту, що забезпечують зниження виявлених в процесі аналізу ризиків інформаційної безпеки без надмірних витрат на впровадження і підтримку цих коштів. Аналіз ризиків інформаційної безпеки дозволяє визначити необхідну і достатню сукупність заходів, спрямованих на зниження ризиків

інформаційної безпеки, і розробити архітектуру СУІБ організації, максимально ефективну для її специфіки діяльності і спрямовану на зниження саме її ризиків інформаційної безпеки.

Проведені дослідження дозволяють сформулювати критерії вибору методів оцінки і управління ризиками інформаційної і кібербезпеки:

– наявність науково-методичного обґрунтування методу для оцінки і управління ризиками;

– відповідність вимогам сучасних стандартів і нормативних документів у сфері створення систем управління інформаційною безпекою;

– простота проведення заходів з оцінки ризиків (ОР) із можливістю залучення на окремих етапах ОР вузькоспеціалізованих фахівців;

– можливість застосування принципів системності та використання засобів структурного аналізу і автоматизованих методів прийняття рішень;

– можливість адаптації методу ОР до вимог організації залежно від її типу та розміру;

– можливість отримання результатів щодо ОР у якісному та кількісному представленні;

– можливість збору інформації, що буде вихідним матеріалом формування (редагування) концепції та розробки політики інформаційної і кібербезпеки Організації, робіт з ОР,

– наявність програмного забезпечення для обробки результатів у повному обсязі із зрозумілим та дружнім інтерфейсом;

– структурованість та модульність складових методу;

– наявність модулю економічного підрахунку вартості проведення ОР та впровадження системи управління інформаційною безпекою;

– наявність модулю економічного обґрунтування доцільності впровадження заходів захисту;

– придатність до застосування як в існуючих інформаційних системах (ІС), так і для ІС, що розробляються;

– наявність шаблонів для звітних документів;

– наочність результатів проведення ОР для Замовника;

– наявність каталогів: загроз, типів інформації, порушників, заходів захисту із встановленими на множинах відносинах причино-наслідкового зв’язку та інші.

3. Порівняльний аналіз методів управління ризиками інформаційної і кібербезпеки

Розглянемо загальну характеристику та проведемо порівняльний аналіз широко застосовуваних методик і методів управління і оцінки ризиками інформаційної і кібербезпеки у відповідності до наведених у розд. 2 та інших критеріїв.

1. Фреймворк "NIST Risk Management Framework" – на базі американських урядових стандартів NIST (National Institute of Standards and Technology), включає в себе набір взаємозв'язаних стандартів:

– Стандарт NIST SP 800-30 "Guide for Conducting Risk Assessments" ("Керівництво з проведення оцінки ризиків") сфокусований на ІТ, інформаційній безпеці (ІБ) і операційних ризиках, описує підхід до процесів підготовки і проведення оцінки ризиків, комунікування результатів оцінки, а також подальшої підтримки процесу оцінки;

– Стандарт NIST SP 800-39 "Managing Information Security Risk" пропонує трирівневий підхід до управління ризиками: організація, бізнес-процеси, інформаційні системи. Даний стандарт описує методологію процесу управління ризиками: визначення, оцінка ризиків інформаційної безпеки, реагування та моніторинг ризиків;

– Стандарт NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations" пропонує для забезпечення безпеки і конфіденційності використовувати підхід управління життєвим циклом систем;

– Стандарт NIST SP 800-137 "Information Security Continuous Monitoring" описує підхід до процесу моніторингу інформаційних систем і IT-середовищ з метою контролю застосованих заходів обробки ризиків ІБ і необхідність їх перегляду.

2. Стандарти управління ризиками інформаційної безпеки Міжнародної організації зі стандартизації ISO (International Organization for Standardization):

– Стандарт ISO / IEC 27005: 2018 "Information technology – Security techniques – Information security risk management" («Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризиків інформаційної безпеки») входить в серію стандартів ISO 27000 та є логічно взаємопов'язаним з іншими стандартами по ІБ з цієї серії. Даний стандарт відрізняється фокусом на ІБ при розгляді процесів управління ризиками;

– Стандарт ISO / IEC 27102: 2019 "Information security management – Guidelines for cyber-insurance" пропонує підходи до оцінки необхідності придбання кіберстраховки як заходу обробки ризиків безпеки інформаційних систем, а також до оцінки і взаємодії зі страховиком;

– Серія стандартів ISO / IEC 31000: 2018 описує підхід до ризик-менеджменту без прив'язки до IT / ІБ. У цій серії варто відзначити стандарт ISO / IEC 31010: 2019 "Risk management – Risk assessment techniques".

3. Методологія FRAP (Facilitated Risk Analysis Process) є відносно спрощеним способом оцінки основних ризиків інформаційної безпеки, з фокусом тільки на найкритичніших активах. Якісний аналіз проводиться за допомогою експертної оцінки.

4. Методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) сфокусована на самостійній роботі членів бізнес-підрозділів. Вона використовується для масштабної оцінки всіх інформаційних систем і всіх бізнес-процесах компанії.

5. Стандарт AS / NZS 4360 є австралійським і новозеландським стандартом з фокусом не тільки на IT-системах, але і на бізнес-здоров'я компанії, тобто пропонує більш глобальний підхід до управління ризиками інформаційної безпеки (наприклад, в банку). Відзначимо, що даний стандарт зараз замінений на стандарт AS / NZS ISO 31000-2009.

6. Методологія FMEA (Failure Modes and Effect Analysis) пропонує проведення оцінки системи з точки зору її слабких місць для пошуку ненадійних елементів.

7. Методологія CRAMM (Central Computing and Telecommunications Agency Risk Analysis and Management Method) пропонує використання автоматизованих засобів для управління ризиками інформаційної безпеки.

8. Методологія FAIR (Factor Analysis of Information Risk) – Фреймворк для проведення кількісного аналізу ризиків, що пропонує модель побудови системи управління ризиками на основі економічно ефективного підходу, прийняття поінформованих рішень, порівняння заходів управління ризиками, фінансових показників і точних ризик-моделей.

9. Концепція COSO ERM (Enterprise Risk Management) описує шляхи інтеграції ризик-менеджменту зі стратегією і фінансової ефективністю діяльності компанії і акцентує увагу на важливість їх взаємозв'язки.

Проведемо порівняльний аналіз окремих перерахованих методів у відповідності до критеріїв, наведених у розділі 2.

4. Методика NIST 800-30

Однією з найпопулярніших та широковживаних методик управління ризиками є методика оцінки ризиків National Institute of Standards and Technology (NIST), яка визначена в Керівництві з управління ризиками в інформаційних технологіях NIST 800-30 (NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems). Ця методика передбачає попереднє оцінювання двох параметрів: потенційного збитку та ймовірності реалізації загрози [3]. Призначення системи управління ризиками безпосередньо пов’язане з можливістю компанії виконувати свої основні функції за умов постійного розширення сфери використання інформаційних технологій. Методика оцінки ризиків, яка наведена в спеціаль-

них рекомендаціях 800-30, охоплює широке коло завдань, що пов'язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками. Проте запропонований процес оцінювання ризику ІБ, який представлений у вигляді таблиці, що відображає залежність ризику від двох вхідних змінних: потенційного збитку і ймовірності можливого інциденту. При цьому значення кожної змінної, зокрема ризику, оцінюється за трирівневою шкалою. Такий "жорсткий" механізм отримання оцінок ризику суттєво обмежує точність результатів, забезпечуючи їх оперативність та відтворюваність.

Використання такої методики передбачає такі етапи:

– опис характеристик системи;
– ідентифікація загроз;
– ідентифікація вразливостей;
– аналіз наявних засобів/заходів захисту;
– визначення значення ймовірності;
– аналіз впливу;
– визначення значення ризику;
– вибір засобів/заходів захисту;
– документування отриманих результатів.

Алгоритм цієї методики зображено на рис 1.

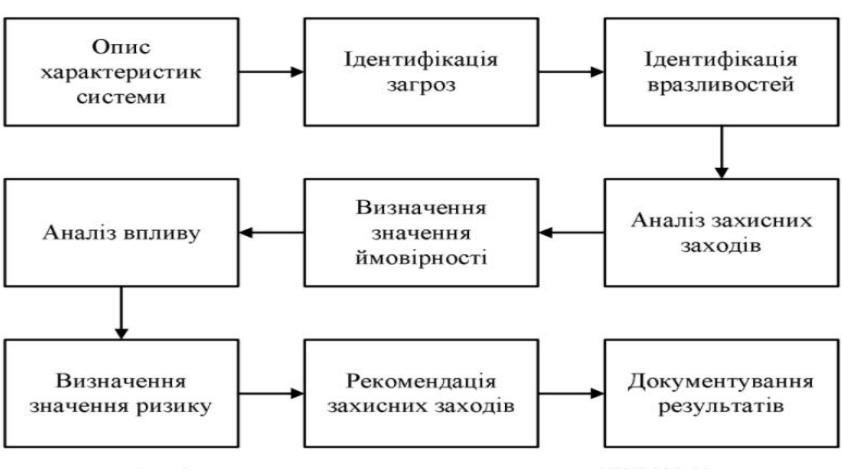


Рис. 1. Алгоритм методики управління ризиками NIST 800-30

Переваги методу NIST 800-30:

– відносна простота проведення заходів з оцінки ризиків (ОР);
– можливість адаптації методу ОР до вимог організації залежно від її типу та розміру;
– детально описує всі можливі ризики для інформаційних активів;
– припускає використання як способів обробки ризиків всіх можливих варіантів (зниження, прийняття, перенесення, уникнення ризику);
– наявність програмного забезпечення для обробки результатів, що реалізовує принципи методики;

Метод NIST 800-30 має деякі обмеження для застосування, а саме:

– довготривалий процес аналізу і оцінки ризиків;
– оцінювання ризиків проводиться лише за трирівневою шкалою, що істотно обмежує можливості методики загалом.

5. Методика CRAMM

Методика CRAMM (CCTA Risk Analysis and Management Method), розроблена Службою безпеки Великобританії, базується на стандартах управління інформаційної безпеки серії BS7799 (в даний час перероблені в ISO 27000) і описує підхід до якісної оцінки ризиків [4].

При цьому перехід до шкали значень якісних показників відбувається за допомогою спеціальних таблиць, що визначають відповідність між якісними та кількісними показниками. Оцінка ризику проводиться на основі аналізу цінності ІТ-активу для бізнесу, вразливостей, загроз і ймовірності їх реалізації.

В основу методики CRAMM покладено комплексний підхід до оцінки ризиків, що поєднує кількісні та якісні методи аналізу. Методика є універсальною і придатна як для великих, так і для малих організацій, як державного, так і комерційного сектору. Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються своїми базами знань (profiles). Для комерційних організацій є комерційний профіль (Commercial Profile), для державних організацій – державний профіль (Government profile). Державний варіант профілю також дає змогу проводити аудит на відповідність вимогам американського стандарту ITSEC.

Правильне використання методики CRAMM дає змогу економічно обґрунтувати витрати організації на забезпечення інформаційної безпеки та неперервності функціонування. Економічно обґрунтована стратегія управління ризиками ІБ дає змогу, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат.

Методика CRAMM припускає поділ всієї процедури ОР на три послідовні етапи. Завданням першого етапу є відповідь на запитання: “Чи достатньо для захисту системи застосування засобів базового рівня, що реалізують традиційні функції ІБ, чи необхідне проведення детальнішого аналізу?” На другому етапі здійснюється ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується завдання про вибір адекватних контрзаходів. Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення інтерв’ю, списки перевірки і набір звітних документів.

Алгоритм методики CRAMM надано на рис. 2

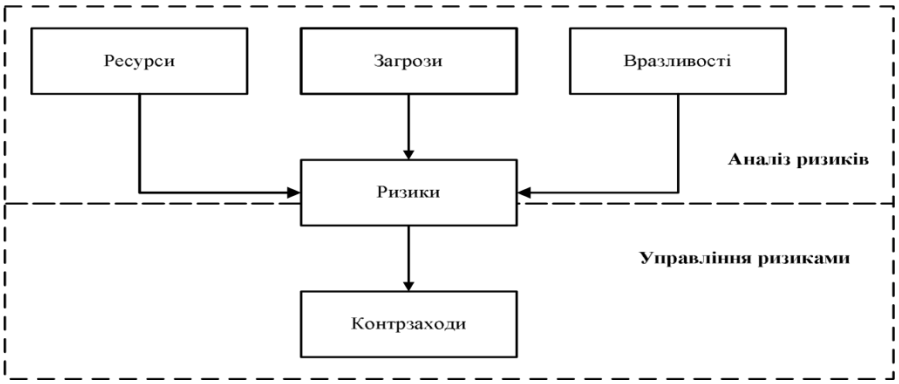


Рис. 2. Алгоритм методики управління ризиками CRAMM

Процес управління ризиками за методикою CRAMM складається з наступних етапів:

1. Ініціювання (Initiation). На цьому етапі проводиться серія інтерв'ю з зацікавленими в процесі аналізу ризиків інформаційної безпеки особами, в тому числі з відповідальними за експлуатацію, адміністрування, забезпечення безпеки і використання ІТ-активів, для яких проводиться аналіз ризиків. В результаті дається формалізований опис області для подальшого дослідження, її кордонів і визначається склад залучених в аналіз ризиків осіб.

2. Ідентифікація та оцінка ІТ-активів (Identification and Valuation of Assets). Визначається перелік ІТ-активів, які використовуються організацією в певній галузі дослідження. Відповідно до методології CRAMM ІТ-активи можуть бути одного з наступних типів:

– дані;
– програмне забезпечення;
– фізичні активи.

Для кожного активу визначається його критичність для діяльності організації і спільно з представниками підрозділів, що використовують ІТ-актив для вирішення прикладних

завдань, оцінюються наслідки для діяльності організації від порушення його конфіденційності, цілісності та доступності.

3. Оцінка загроз і вразливостей (Threat and Vulnerability Assessment). На додаток до оцінки критичності ІТ-активів важливою частиною методології CRAMM є оцінка ймовірності загроз і вразливостей ІТ-активів. Методологія CRAMM містить таблиці, що описують відповідність між уразливими ІТ-активів і погрозами, які можуть впливати на ІТ-активи через ці уразливості. Також є таблиці, що описують збиток для ІТ-активів в разі реалізації цих загроз. Даний етап виконується тільки для найбільш критичних ІТ-активів, для яких недостатньо впровадження базового набору заходів забезпечення інформаційної безпеки. Визначення актуальних вразливостей і загроз проводиться шляхом інтерв'ювання осіб, відповідальних за адміністрування та експлуатацію ІТ-активів. Для інших ІТ-активів методологія CRAMM містить набір необхідних базових заходів забезпечення інформаційної безпеки.

4. Обчислення ризику (Risk Calculation). Обчислення ризику здійснюється за формулою

$$\text{Ризик} = \text{Р (реалізації)} * \text{Збиток}.$$

При цьому ймовірність реалізації ризику обчислюється за формулою

$$\text{Р (реалізації)} = \text{Р (загрози)} * \text{Р (уразливості)}.$$

На етапі обчислення ризиків для кожного ІТ-активу визначаються вимоги до набору заходів щодо забезпечення його інформаційної безпеки за шкалою від «1» до «7», де значенням «1» відповідає мінімальний необхідний набір заходів щодо забезпечення інформаційної безпеки, а значенням «7» – максимальний.

5. Управління ризиком (Risk Management). На основі результатів обчислення ризику методологія CRAMM визначає необхідний набір заходів щодо забезпечення інформаційної безпеки. Для цього використовується спеціальний каталог, що включає близько чотирьох тисяч заходів. Рекомендований методологією CRAMM набір заходів порівнюється з заходами, які вже прийняті організацією. В результаті ідентифікуються області, які потребують додаткової уваги в частині застосування заходів захисту, і області з надлишковими заходами захисту. Дана інформація використовується для формування плану дій зі зміни складу застосовуваних в організації заходів захисту – для приведення рівня ризиків до необхідного рівня.

Методологія CRAMM у значній мірі відповідає критеріям, що наведено у розд. 2, це, насамперед:

– є універсальною і підходить для організацій як державного, так та комерційного сектору;

– використовує кількісні і якісні способи оцінки ризиків;

– розроблені комерційні програмні продукти, що реалізовують положення CRAMM;

– наявність зрозумілого формалізованого опису методології зводить до мінімуму можливість виникнення помилок при реалізації процесів аналізу, оцінки та управління ризиками;

– наявність засобів автоматизації аналізу ризиків дозволяє мінімізувати трудовитрати і час виконання заходів з аналізу та управління ризиками;

– наявність каталогів загроз, порушників, вразливостей, наслідків, заходів забезпечення інформаційної безпеки, що спрощує вимоги до спеціальних знань і компетентності безпосередніх виконавців заходів з аналізу, оцінки та управління ризиками.

Зазначена методологія має і суттєві обмеження для застосування, які обумовлені такими чинниками:

– висока складність і трудомісткість збору вихідних даних, що вимагає залучення значних ресурсів усередині організації або ззовні;

– великі витрати ресурсів і часу на реалізацію процесів аналізу та управління ризиками інформаційної безпеки;

– залучення великої кількості зацікавлених осіб вимагає значних витрат на організацію спільної роботи, комунікацій усередині проєктної команди і узгодження результатів;

– неможливість оцінити ризики в грошах ускладнює використання результатів оцінки ризиків ІБ при техніко-економічному обґрунтуванні інвестицій, необхідних для впровадження засобів і методів захисту інформації.

CRAMM широко застосовується як в урядових, так і в комерційних організаціях по всьому світу, будучи фактично стандартом управління ризиками інформаційної безпеки в Великобританії. Методика може бути успішно застосована у великих організаціях, орієнтованих на міжнародну взаємодію і відповідність міжнародним стандартам управління, які здійснюють початкове впровадження процесів управління ризиками інформаційної безпеки для покриття ними всієї організації відразу. При цьому організації повинні мати можливість виділення значних ресурсів і часу для застосування CRAMM.

6. Метод OCTAVE

Метод OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблений в Університеті Карнегі-Мелон (США) і передбачає оцінювання критичності загроз, активів і вразливостей.

Цю методику широко використовують у всьому світі, виконуючи роботи з оцінки ризиків ІБ та впровадження процесів управління ризиками в компанії загалом.

Зміст методики OCTAVE [5] полягає в тому, що для оцінки ризиків використовується послідовність відповідно організованих внутрішніх семінарів (workshops). Оцінка ризиків здійснюється в три етапи, яким передує набір підготовчих заходів: узгодження графіка семінарів, призначення ролей, планування, координація дій учасників проєктної групи.

На першому етапі, в межах практичних семінарів, здійснюється розроблення профілів загроз, що містять інвентаризацію та оцінку цінності активів, ідентифікацію застосовних вимог законодавства та нормативної бази, ідентифікацію загроз та оцінку їх ймовірності, а також визначення системи організаційних заходів з підтримки режиму інформаційної безпеки.

На другому етапі проводиться технічний аналіз вразливостей систем організації щодо загроз, чиї профілі розроблено на попередньому етапі, який містить ідентифікацію наявних вразливостей компанії та оцінювання їх величини.

На третьому етапі виконується оцінка та оброблення ризиків інформаційної безпеки, що містить визначення величини та ймовірності завданої шкоди внаслідок реалізації загроз ІБ з використанням вразливостей, які ідентифіковано на попередніх етапах, визначення стратегії ІБ, а також вибір варіантів і прийняття рішень з оброблення ризиків. Величина ризику визначається як середнє значення річних втрат компанії в результаті реалізації загроз інформаційної безпеки (ІБ).

Алгоритм цієї методики зображено на рис. 3.

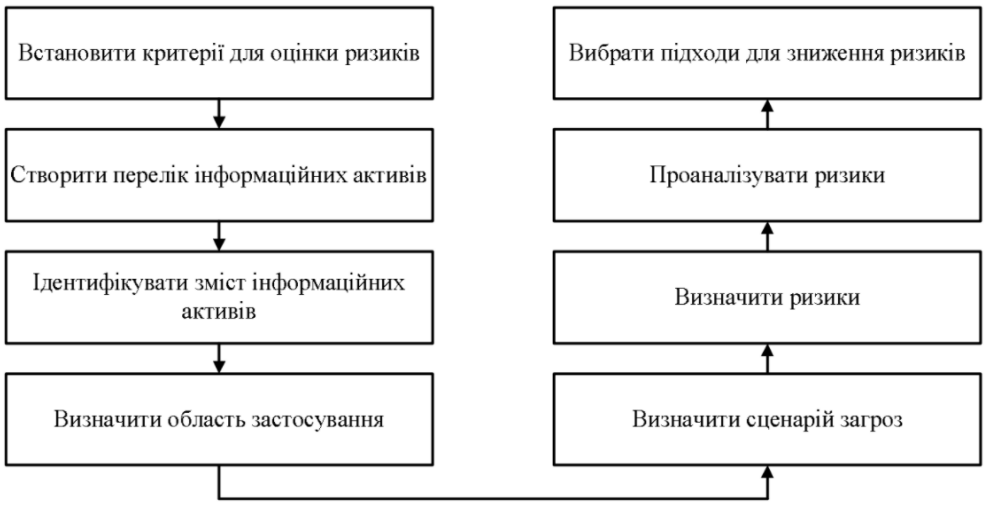


Рис. 3. Алгоритм методики управління ризиками OCTAVE

До показників методики OCTAVE, що відповідають критеріям обрання методів оцінки ризиків, можна віднести:

– можливість адаптації методу ОР до вимог організації залежно від її типу та розміру;
– можливість отримання результатів щодо ОР у якісному та кількісному представленні;
– є комерційні програмні продукти, що реалізовують положення методики;
– високий рівень гнучкості при застосуванні.

Тим не менш даній методиці притаманні низка недоліків, а саме:
– не дає можливості реалізовувати кількісну оцінки ризиків;
– припускає можливість як способів обробки ризиків лише його зниження і прийняття.

7. Методологія COBIT

Методологія COBIT for Risk [6] розроблена асоціацією ISACA (Information Systems Audit and Control Association) в 2013 р. і базується на кращих практиках управління ризиками (COSO ERM, ISO 31000, ISO\IEC 27xxx і ін.). Методологія розглядає ризики інформаційної безпеки стосовно ризиків основної діяльності організації, описує підходи до реалізації функції управління ризиками інформаційної безпеки в організації та до процесів якісного аналізу ризиків інформаційної безпеки і управління ними.

При реалізації функції і процесу управління ризиками в організації методологія виділяє наступні компоненти, що впливають як на ризики інформаційної безпеки, так і на процес управління ними:
– принципи, політики, процедури організації;
– процеси;
– організаційна структура;
– корпоративна культура, етика і правила поведінки;
– інформація;
– IT-сервіси, IT-інфраструктура і додатки;
– люди, їх досвід і компетенції.

Основним елементом аналізу та управління ризиками інформаційної безпеки відповідно до методології є ризикові сценарії. Кожен сценарій являє собою «опис події, яка в разі виникнення, може привести до невизначеного (позитивного або негативного) впливу на досягнення цілей організації».

Методологія містить більше 100 ризикових сценаріїв, що охоплюють такі категорії впливу:
– створення та обслуговування портфелів IT-проєктів;
– управління життєвим циклом програми/проєкту;
– інвестиції в IT;
– експертиза і навички персоналу IT;
– операції з персоналом;
– інформація;
– архітектура;
– IT-інфраструктура;
– програмне забезпечення;
– неефективне використання IT;
– вибір і управління постачальниками IT;
– відповідність нормативним вимогам;
– геополітика;
– крадіжка елементів інфраструктури;
– шкідливе програмне забезпечення;
– логічні атаки;
– техногенне вплив;
– довкілля;
– природні явища;
– інновації.

Для кожного ризикового сценарію в методології визначено ступінь його приналежності до кожного типу ризиків:

– стратегічні ризики – ризики, пов'язані з втраченими можливостями використання ІТ для розвитку та підвищення ефективності основної діяльності організації;

– проєктні ризики – ризики, пов'язані з впливом ІТ на створення або розвиток існуючих процесів організації;

– ризики управління ІТ та надання ІТ-сервісів – ризики, пов'язані із забезпеченням доступності, стабільності і надання користувачам ІТ-сервісів з необхідним рівнем якості, проблеми з якими можуть привести до збитку для основної діяльності організації.

Кожен ризиковий сценарій містить наступну інформацію:

– тип джерела загрози – внутрішній/зовнішній;

– тип загрози – зловмисні дії, природне явище, помилка і ін. ;

– опис події – доступ до інформації, знищення, внесення змін, розкриття інформації, крадіжка та ін. ;

– типи активів (компонентів) організації, на які впливає подія – люди, процеси, ІТ-інфраструктура та ін. ;

– час події.

У разі реалізації ризикового сценарію діяльності організації завдається шкода. Таким чином, при аналізі ризиків інформаційної безпеки відповідно до методології COBIT for Risk проводиться виявлення актуальних для організації ризикових сценаріїв і заходів зниження ризиків, спрямованих на зменшення ймовірності реалізації цих сценаріїв.

Для кожного з виявлених ризиків проводиться прийняття одного з рішень щодо обробки ризику:

– уникнення ризику;

– прийняття ризику;

– передача ризику;

– зниження ризику.

Подальше управління ризиками здійснюється шляхом аналізу залишкового рівня ризиків і прийняття рішення про необхідність реалізації додаткових заходів зниження ризиків. Методологія містить рекомендації щодо впровадження заходів зниження ризиків стосовно кожного з типів компонентів організації.

З точки зору практичного застосування, можна виділити такі переваги методології COBIT for Risk:

– відповідність вимогам сучасних стандартів у сфері створення систем управління інформаційною безпекою (СУІБ);

– зв'язок із загальною бібліотекою COBIT і можливість використовувати підходи та «ІТ-контролі» (заходів щодо зниження ризиків) з суміжних областей, що дозволяють розглядати ризики інформаційної безпеки та заходи щодо їх зниження стосовно впливу ризиків на бізнес-процеси організації;

– багаторазово апробований метод, за яким накопичені значний досвід і професійні компетенції і результати якого визнаються міжнародними інститутами;

– наявність зрозумілого формалізованого опису методології дозволяє звести до мінімуму помилки при реалізації процесів аналізу та управління ризиками;

– є універсальною і підходить для організацій як державного, так комерційного сектору;

– високий рівень гнучкості.

– каталоги ризикових сценаріїв і «ІТ-контролів» дозволяють спростити вимоги до спеціальних знань і компетентності безпосередніх виконавців заходів з аналізу та управління ризиками;

– можливість використання методології при проведенні аудитів дозволяє знизити трудовитрати і необхідний час для інтерпретації результатів зовнішніх і внутрішніх аудитів.

При цьому методології COBIT for Risk притаманні такі недоліки і обмеження:

– висока складність і трудомісткість збору вихідних даних вимагає залучення значних ресурсів або всередині організації, або ззовні;

– допускає лише якісну (суб'єктивну) оцінку співвідношення втрат від загроз безпеки;

– значна трудомісткість реалізації методу.

Даний метод застосовується як в урядових, так і в комерційних структурах. Метод є найбільш ефективним для великих технологічних організацій або організацій з високим ступенем залежності основної діяльності від інформаційних технологій, для таких, що вже використовують (або планують використовувати) стандарти і методики COBIT для управління інформаційними технологіями та мають необхідні для цього ресурси та компетенції. В цьому випадку можлива ефективна інтеграція процесів управління ризиками інформаційної безпеки та процесів загального управління IT та досягнення синергетичного ефекту, який дозволить оптимізувати витрати на реалізацію процесів аналізу та управління ризиками інформаційної безпеки.

8. Методи оцінки ризиків безпеки інформації MAGERIT та MEHARI

Інструментарій MEHARI [7, 8] складається з чотирьох модулів (рис. 4), комплексне використання яких дозволяє адаптувати цей метод до використання у будь-якій організації. Розробники MEHARI пропонують такий порядок проведення ОР: оцінка загрози і її потенціалу, визначення ресурсів, які від неї постраждають, визначення заходів захисту (ЗЗ), що дозволяють забезпечити попередження, захист або відновлення бізнес-процесів організації після реалізації загрози. Для кожного етапу надані прикладні засоби MEHARI надають: практичні рекомендації, таблиці, розрахункові формули та шкали оцінок. Супутня документація містить: інструкції та поради щодо ефективного використання бази знань (подана у форматі Excel), а також теоретичні відомості щодо управління ризиками ІБ. Метод MEHARI використовує трьохфакторну модель ризиків ІБ, елементами якої є: імовірність реалізації загрози, рівень вразливості активу до цієї загрози та цінність втраченого активу.

Для побудови дерева загроз, що є актуальними для ресурсів організації, у методі MEHARI запропоновано використовувати метод сценаріїв. Іншою перевагою MEHARI є наявність шкал оцінювання та способу детермінованого визначення залишкових ризиків ІБ.

Крім цього, у MEHARI визначено підхід до класифікації активів різних типів та запропоновано таблицю відповідності кращих практик з MEHARI до заходів, що визначені у стандарті ISO/IEC 27002 (наявність такої можливості є безумовно важливою, враховуючи широке застосування ISO/IEC 27002 у сучасній практиці з організації захисту інформації). У MEHARI запропоновані опитувальні листи, що дозволяють оцінити рівень досконалості ЗЗ, з урахуванням вагових коефіцієнтів відносної значущістю окремих кращих практик, що свідчать про ефективність/досконаліть ЗЗ. Коефіцієнти за замовчуванням можуть бути змінені в ході проведення ОР ІБ.

Дотримання принципів системного підходу у ході оцінювання ризиків ІБ.

Забезпечення керованості процесу оцінювання ризиків (ОР), а також повторюваності та порівнюваності результатів можливе за рахунок застосування таких принципів системного підходу:

1. Ієрархічність – цілі, що досягаються у результаті виконання процесів ОР мають знаходитись в ієрархічній залежності, тобто кожен рівень цілей має враховувати цілі та чинники, що є актуальними для нього.

2. Декомпозиція – кожен процес ОР має бути представлений у вигляді сукупності підпроцесів. Кожен із підпроцесів повинен мати власні цілі та критерії (метричні показники) своєї ефективності та результативності.

3. Достатність та логічна незалежність – логіка організації процесів ОР не повинна залежати від набору кращих практик захисту, ЗЗ, множини загроз безпеки та множини активів.

4. Модульність та функціональна автономність – має бути виділено окремі модулі (оцінювання активів, оцінювання ЗЗ тощо), що функціонують незалежно для отримання оцінки ризику ІБ.

5. Адаптивність – метод ОР має забезпечувати необхідний рівень ефективності незалежно від умов зовнішнього середовища, в якому проводиться оцінювання ризиків ІБ.

6. Формалізованість – ОР має забезпечувати отримання зрозумілих (для замовника) кількісних/якісних показників ризику ІБ та показників ефективності впровадження МЗ. Опис заходів, що проводяться у ході ОР, повинен виключати неоднозначність тлумачення, тим самим має забезпечуватися повторюваність і порівнюваність результатів оцінки ризиків ІБ.

7. Структурованість – дані, що збираються у процесі ОР, мають бути структуровані і подані у вигляді, придатному для подальшого використання іншими модулями ОР.

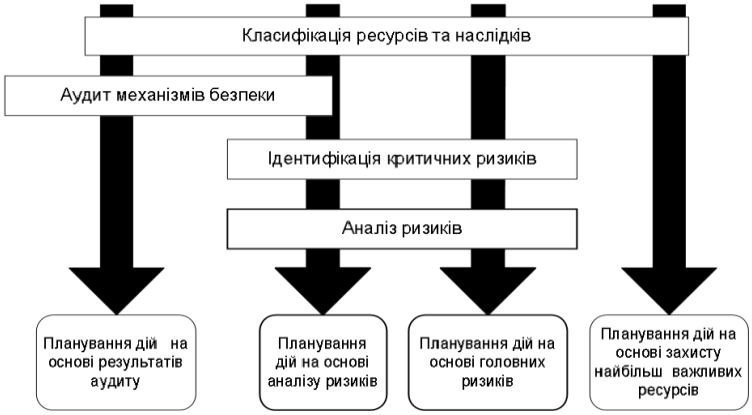


Рис. 4. Модулі MEHARI та підходи до проведення оцінювання ризиків БІ

Застосування методів та засобів системного аналізу у ході оцінювання ризиків ІБ.

Зважаючи на складність проведення ОР та обсяг даних, що мають бути зібрані, актуальною є задача вибору методу опису та представлення як самого процесу ОР, так і компонентів інформаційної системи (ІС), що розглядаються як активи організації.

Для розв’язання цієї задачі доцільно використовувати структурні методи – стандартні моделі та методи системного аналізу (СА), що забезпечують подолання складності великих систем шляхом декомпозиції їх на підсистеми [9].

Традиційно прикладні методи структурного аналізу (СА) поділяють на три групи:

- діаграми, що ілюструють функції, які система повинна виконувати, і зв'язки між цими функціями (DFD, SADT (IDEF0));
- діаграми, що моделюють дані і їх взаємозв'язки (ERD);
- діаграми, що моделюють поведінку системи (STD).

Мабуть найважливіший клас задач, що вирішується у ході ОР, є клас задач прийняття рішень. Рішення можуть стосуватися: визначення границь оцінювання, визначення рівня критичності інформаційних ресурсів, вибору пар загроза/інформаційний ресурс, визначення ефективності ЗЗ тощо. Для підвищення ефективності таких рішень, а також забезпечення порівнюваності та повторюваності результатів оцінки пропонується застосовувати методи підтримки та прийняття рішень. Наприклад, для генерування множини альтернативних рішень, що задовольняють заданим умовам, у СА широко використовуються такі методи: метод колективної генерації ідей, метод сценаріїв, метод Дельфі, морфологічні методи тощо. Однією з ознак, що можуть використовуватися для класифікації методів оцінювання і вибору альтернатив є кількість критеріїв, що вони дозволяють враховувати. Найкраща альтернатива може обиратися за значенням цільової функції, вид та правила побудови якої визначаються використовуваним математичним апаратом.

Для проведення ОР у методах Magerit [10, 11] та MEHARI використовуються такі методи та прийоми СА: композиція, декомпозиція, прикладні методи функціонального структурного аналізу IDEF-0 та DFD, експертні методи, метод Дельфі, метод сценаріїв, табличне завдання відповідностей, критеріальний метод вибору за результатами бінарного оцінюванням.

IDEF-0 – стандарт, що визначає технологію опису системи у виді множини взаємозалежних дій або функцій. Особливість IDEF-0 – функціональна спрямованість, це дозволяє чітко відокремити аспекти призначення системи від аспектів її фізичної реалізації. Опис системи організований у вигляді ієрархічно впорядкованих та взаємопов'язаних діаграм. Вершину структури займає загальний опис призначення та взаємозв'язок системи з оточуючим середовищем, коріння – найбільш деталізовані описи підлеглих функцій, що виконує система.

Слід відмітити, що ступінь деталізації опису процесів ОР у методі Magerit надає достатні дані для побудування родини діаграм процесів ОР у нотації IDEF-0. Даними для цього слугують визначені у методі Magerit: структура процесу; продукти кожного етапу; вхідні та вихідні дані; технологія отримання; керівна інформація; функції та обов'язки учасників; перелік виконавців тощо.

На рис. 5 наведено контекстну діаграму мета процесу ОР, на рис. 6 – результат моделювання під процесу ОР проміжного рівня деталізації [12].

DFD – стандарт для створення моделі потоків інформації, що циркулює в ІТС. Модель системи визначається як ієрархія діаграм потоків даних, що описують асинхронний процес перетворення інформації від введення у систему до отримання користувачем. DFD визначає, яким чином кожний процес перетворює вхідні дані у вихідні та дозволяє виявити співвідношення між процесами.

Розробниками Magerit було запропоновано використовувати DFD на етапі збору інформації, що використовується для визначення цінності активів.

Метод Дельфі – складається з кількох етапів, що циклічно повторюються до моменту прийняття компромісного рішення: проведення індивідуальних анкетних опитувань, обробка результатів, ознайомлення експертів із результатами, повторне анкетне опитування.

У Magerit пропонується використовувати метод Дельфі для ідентифікації елементів, що враховуються при оцінці ризиків БІ – активів, загроз, механізмів захисту тощо.

Метод сценаріїв передбачає підготовку та узгодження уявлень щодо проблеми або об'єкту, що аналізується, у письмовому вигляді. Зазвичай, текст містить логічну послідовність подій або можливі варіанти вирішення проблеми, впорядковані за хронологією. Сценарій передбачує змістовні міркування, що забезпечують деталізований розгляд проблеми, та результати кількісного техніко-економічного або статистичного аналізу з попередніми висновками, що можна отримати на їх основі. У методі MEHARI запропоновано розвинутий перелік ризик-сценаріїв, що дозволяють провести кількісне оцінювання рівнів ризиків БІ.

Критеріальний метод – кожна окрема альтернатива оцінюється одним або кількома показниками. Таким чином, порівняння альтернатив зводиться до обчислення узагальненого показника та порівняння альтернатив за його значенням на основі уведених критеріїв.

Метод попарного порівняння – альтернативи (А та В) порівнюються із використанням бінарних оцінок: (А та В) порівнюються із використанням бінарних оцінок: $A \leq B$, або $A > B$, або $A = B$.

Рис. 5. Контекстна діаграма процесу ОР у нотації IDEF-0

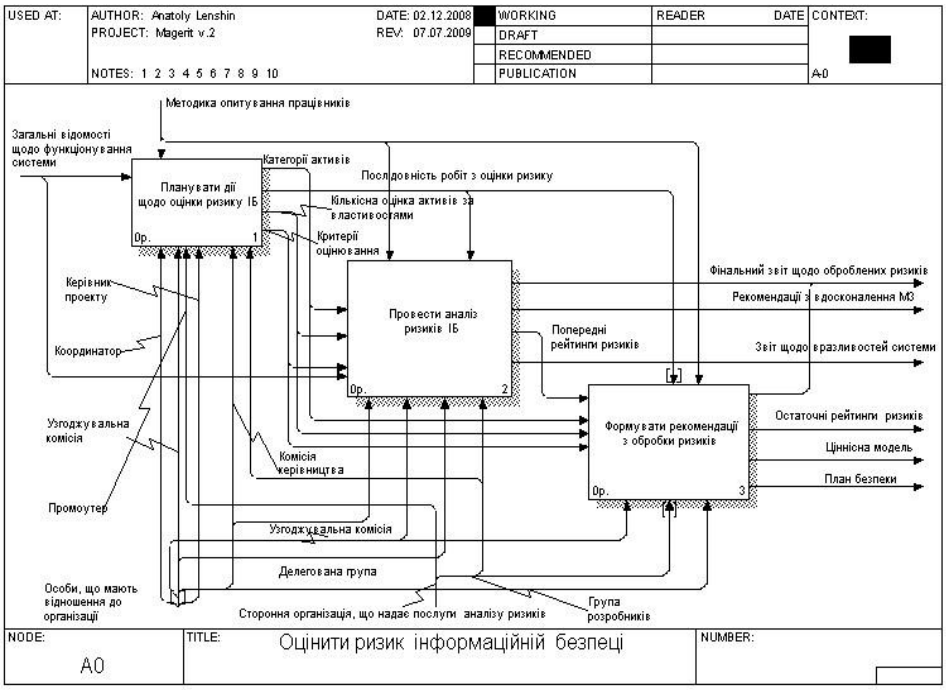


Рис. 6. Декомпозиція мета процесу ОР у нотації IDEF-0

За результатами дослідження зазначених методів (Magerit та MEHARI) можна стверджувати, що кожному із методів притаманні певні позитивні риси, які свідчать про системність підходу до проведення ОР. Проведемо порівняння цих методів за такими критеріями: ступінь відповідності стандартам (К1), організація процесів згідно з моделлю PDCA (К2), модель ризиків, що використовується (К3), вимоги до звітної документації (К4), підтримка методів аналізу вартості проведення ОР (К5), ступінь формалізації алгоритму (К6), суворість вимог до складу аналітичної групи (К7), наявність засобів проведення ОР (К8), види ЗЗ, що розглядаються (К9), використовувані методи збору даних (К10), наявні критерії оцінки (К11), підхід до обчислення ризику (К12), використовувані методи СА (К13), допоміжне ПЗ (К14). Результати порівняння методів ОР Magerit та MEHARI зведено до табл. 1.

Таблиця 1

Номер	Magerit	MEHARI
К1	Розроблений з урахуванням стандартів BSI. Сумісний з профілями захисту ISO/IEC 15408. Сумісний з ISO/IEC 13335 та ISO/IEC 27001	Повністю відповідає ISO/IEC 27002. Формально відповідає ISO/IEC 13335 та ISO/IEC 27001
К2	Підтримується	Підтримується
К3	Двофакторна: імовірність загрози та рівень наслідків	Трьохфакторна: імовірність загрози, рівень вразливості, рівень наслідків
К4	По закінченні кожного етапу обов'язково складається документ за визначеною формою	Обов'язковим є розробка політики безпеки. Припускаються записи у довільній формі
К5	Присутні бази для проведення розрахунків	Не підтримуються
К6	Високий, кожний етап має фіксований вхід, вихід та дію	Середній, збираються дані лише для необхідних структур (таблиць)
К7	Чітко визначені	Присутні у загальному вигляді
К8	Діаграми процесів даних, діаграма цінності активів, типи активів, база МЗ, перелік загроз	Карта природного ризику, карта МЗ, база ризик-сценаріїв, опитувальні листи
К9	Два види: зменшуючи частоту загрози, зменшуючи наслідки	5 видів: попереджуючі, запобіжні, захисні, пом'якшуючі, відновлюючи
К10	Співбесіди з робітниками, опитувальні листи	Опитувальні листи
К11	Критерії для оцінки активів, цінності активів	Критерії для оцінки ризику, статус-ризик
К12	Передбачено розрахунок відхиленого ризику як різниці між базовим та залишковим. Опис алгоритму відсутній	Обчислення з урахуванням множини факторів, передбачає обчислення коефіцієнту вагомості ризику. Наведено опис алгоритму
К13	Експертні методи, метод Дельфі, опис процесів, достатній для побудови IDEF-0 діаграм, DFD	Бальна шкала оцінювання, використання вагових коефіцієнтів, метод сценаріїв
К14	Фрагменти коду для подання даних як XML.	База знань MEHARI

Метод Magerit містить формалізовану, ієрархічно структуровану концепцію проведення ОР, визначені обов'язки і ролі учасників ОР. До переваг методу MEHARI слід віднести формалізований модуль оцінки та розгалужену базу ризик-сценаріїв, спосіб класифікації активів, наявність баз даних у вільному доступі.

З урахуванням зазначеного можуть бути висунуті вимоги щодо розробки вдосконаленого методу ОР, що матиме переваги Magerit та MEHARI.

1. При формуванні групи учасників ОР слід використовувати рекомендації Magerit. У ході класифікації активів доцільно застосовувати бази знань MEHARI, взявши за основу критерії цінності та оцінки вартості, що запропоновані у методі Magerit.

2. Визначення загроз доцільно проводити за базами Magerit, при цьому обчислювати показники природного ризику слід згідно з підходом, визначеним у MEHARI.

3. З огляду на детальність опису МЗ у методі MEHARI та наявність таблиць відповідностей з кращими практиками, що визначені у ISO/IEC 27002 (табл. 2), для ідентифікації впроваджених ЗЗ рекомендується використовувати опитувальні листи MEHARI (табл. 3).

Таблиця 2

Розділ ISO/IEC 27002	Позначення МЗ з MEHARI
5.1 Політика інформаційної безпеки	
5.1.1 Задокументована політика ІБ	01A02-01
5.1.2 Перегляд політики ІБ	01A02-02
6. Організація інформаційної безпеки	
6.1 Внутрішня організація	
6.1.1 Затвердження концепції ІБ керівництвом	01A02-09
6.1.2 Координація ІБ	01A02-03:05
6.1.3 Розподіл обов'язків з ІБ	01A02-06:07

Таблиця 3

01E	Управління безперервністю робочих процесів	Так/ Ні	w_j^i	UL_j^i	LL_j^i
01E01	Питання управління безперервністю бізнесу				
01E0101	Для визначення засад управління безперервністю бізнесу проведений аналіз критичності застосувань і сервісів. Поглиблений аналіз передбачає існування списку інцидентів і ризик-сценаріїв для визначення наслідків	Ні	4	2	
01E0102	Аналіз визначає мінімальні системні вимоги для сервісів та застосувань. Системні вимоги узгоджені з власниками/розпорядниками IP	Так	4	2	3
01E0103	Для розвитку та оновлення планів безперебійної роботи впроваджені та підтримуються процеси OP для кожного IP	Так	2		

В табл. 4 наведено ще один підхід [13] до вибору методів оцінки ризиків інформаційної безпеки, які можуть бути застосовані у інформаційних системах. Такий підхід враховує низку специфічних вимог, які можуть бути висунуті для обґрунтування вимог до вибору методу оцінки ризиків (вартість, необхідність ліцензування, розмір і складність організації, можливості щодо реалізації процедур обробки ризиків тощо).

Таблиця 4

Характеристики / Методи	Ідентифікація ризику (Risk iden	Аналіз ризиків (Risk analysis)	Оцінка ризику (risk evaluation)	Ідентифікація ризику (Risk asses ment)	Обробка ризику (Risk treatment)	Прийняття ризику (Risk accepta	Повідомлення про ризик (Risk c munication)	Мови (Languages)	Ціна	Розмір організації (Size of organ tion)	Необхідні навички (skills neede	Ліцензування (Licensing)	Сертифікування (Certification)	Спеціальні засоби підтримки (D cated support tools)
Austrian IT Security Handbook	• •	•	•	• • •	• • •	• • •	• • •	DE	Free	All	**	N	N	Prototype of charge)
CRAMM	• • •	• • •	• • •					EN, NL	Not fre	Gov, Lar	***	N	N	CRAMM pert, CRA express
Dutch A&K analysi	• • •	• • •	• • •					NL	Free	All	*	N	N	
Ebios	• • •	• • •	• • •	• • •	• • •	• • •	• • •	EN, FR ES	Free	All	**	Y	N	EBIOS ve 2 (open so
ISF methods	• • •	• • •	• • •	• • •	• • •	• • •	• • •	EN	For IS memb	All excep SME	* to *	N	N	Various IS tools(for m bers)
ISO/IEC IS 13335-2 (ISO/IEC IS 27005)	• •	• •	• •	• •	• • •	• • •	• • •	EN	Ca. €1	All	**	N	N	
ISO/IEC IS 17799	•				•			EN	Ca. €1	All	**	N	Y	Many
ISO/IEC IS 27001					•	•		EN, FR	Ca. €8	Gov, Lar	**	Y	Y	Many
IT-Grundschultz	• • •	• • •	• • •	• • •	• • •	• • •	• • •	EN, DE	Free	All	**	Y	Y	Many
Marion (replaced by Mehari)	• • •	• • •	• • •					EN, FR	Not fre	Large	*	N	N	
Mehari	• • •	• • •	• • •					EN, FR	€100-5	All	**	N	N	RISICARI
Octave	• •	• •	• •	• •	• •	• •	• •	EN	Free	SME	**	N	N	
SP800-30 (NIST)	• • •	• • •	• • •	• • •	• • •	• • •		EN	Free	All	**	N	N	

Висновки

NIST США розробив як методологічну основу забезпечення інформаційної та кібербезпеки концепцію Risk Management Framework (RMF). Концепція RMF впроваджує структурований гнучкий підхід до управління ризиками, що пов'язаний із впровадженням інформаційних систем у бізнес-процеси організації.

Система управління інформаційною безпекою (СУІБ) забезпечує збереження конфіденційності, цілісності й доступності інформації за допомогою запровадження процесу управління ризиками та надає впевненості зацікавленим сторонам, що ризиками належним чином управляють. При створенні системи управління ІР постає питання вибору заходів захисту, що забезпечують зниження виявлених в процесі аналізу ризиків інформаційної безпеки без надмірних витрат на впровадження і підтримку цих коштів. Аналіз ризиків інформаційної безпеки дозволяє визначити необхідну і достатню сукупність засобів захисту інформації, а також організаційних заходів спрямованих на зниження ризиків інформаційної безпеки, і розробити архітектуру СУІБ організації, максимально ефективну для її специфіки діяльності і спрямовану на зниження саме її ризиків інформаційної безпеки.

На основі наведеного аналізу можна стверджувати, що оптимальним варіантом для вибору методу управління ризиками ІБ в контексті забезпечення неперервності функціонування СУІБ є, зокрема, адаптація та удосконалення відомих методів шляхом їх логічного поєднання з урахуванням переваг та мінімізації недоліків цих методів. Крім того, при виборі того чи іншого методу оцінки ризиків ІБ необхідно враховувати низку чинників (критеріїв), які визначені у розд. 2 і 3 цієї роботи: наявність науково-методичного обґрунтування методу для проведення оцінки і управління ризиками; відповідність вимогам сучасних стандартам і нормативних документів у сфері створення систем управління інформаційною безпекою; простота проведення заходів з оцінки ризиків із можливістю залучення на окремих етапах оцінки ризиків (ОР) вузькоспеціалізованих фахівців; можливість застосування принципів системності та використання засобів структурного аналізу і автоматизованих методів прийняття рішень; можливість адаптації методу ОР до вимог організації залежно від її типу та розміру; можливість отримання результатів щодо ОР у якісному та кількісному представленні; вартість продукту, організаційно-штатна структура та форма власності організації, ступінь критичності інформації, що обробляється, та інші.

Список літератури:

1. NIST Special Publication 800-37, Revision 2. Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy, 2018.
2. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). ДСТУ ISO/IEC 27001:2015.
3. NIST Special Publication 800-30. Risk Management Guide for Information Technology Systems.
4. CRAMM user guide, Risk Analysis and Management Method, United Kingdom Central Computer and Telecommunication Agency (CCTA), UK, 2001.
5. Методология OCTAVE для оценки информационных рисков [Електроный ресурс]. Режим доступу: http://www.risk24.ru/octave.htm.
6. COBIT 5: A Business Framework for the Governance and Management of Enterprise ISACA, 2012.
7. MEHARI 2007: Concepts and Mechanisms, Club de la Sécurité de l'Information Français.
8. MEHARI 2007: Knowledge Bases, Club de la Sécurité de l'Information Français.
9. Спицнадель В.Н. Основы системного анализа: учеб. пос. / В.Н. Спицнадель. СПб.: Изд. дом «Бизнеспресса», 2000. 326 с.
10. Magerit v2 2006: Book I: The method, Ministerio de Administraciones Publicas, Spain.
11. Magerit v2 2006: Book III: Techniques, Ministerio de Administraciones Publicas, Spain.
12. Потій О.В., Лєншин А.В. Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу // Зб. наук. праць Харків. ун-ту Повітряних Сил. 2010. Вип. 2(24). С. 85-91.
13. Аналіз методів оцінки ризиків інформаційної безпеки [Електроний ресурс]. Режим доступу: https://www.securitylab.ru/blog/personal/secinsight/19205.php.

Надійшла до редколегії 04.08.2021

Відомості про авторів:

Потій Олександр Володимирович – д-р техн. наук, професор, заступник Голови Державної служби спеціального зв'язку та захисту інформації; Україна; e-mail: potav@ua.fm; ORCID: https://orcid.org/0000-0002-2366-0541

Горбенко Юрій Іванович – канд. техн. наук, АТ «інститут інформаційних технологій», перший заступник головного конструктора; Україна; e-mail: gorbenkou@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-0073-9107

Замула Олександр Андрійович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; email: zamylaaa@gmail.com; ORCID: http://orcid.org/0000-0002-8973-6190

Ісірова Катерина Володимировна – АТ «інститут інформаційних технологій», аналітик з систем захисту інформації; Україна; e-mail: katerinaisirova@gmail.com; ORCID: https://orcid.org/0000-0002-0250-7636

UDC 621.391 **DOI:10.30837/rt.2021.3.206.02**

I.D. GORBENKO, Dr. Sc. (Technology), O.A. ZAMULA, Dr. Sc. (Technology)

THEORETICAL APPROACHES TO THE SYNTHESIS OF DISCRETE SIGNALS WITH NECESSARY PROPERTIES

Introduction

Global trends of increasing threats to information and cybersecurity, increasing the level of vulnerability of information and communication systems (ICSs) necessitate the development and implementation of new models, methods and technologies for managing telecommunications networks, information security, services and service quality, development of information exchange methods, methods for synthesizing new classes of complex discrete signals-data carriers with the necessary ensemble, correlation and structural properties. Among the main areas of improvement of information security, noise protection and secrecy of ICSs one can identify the areas associated with the use of channels with high frequency redundancy, significant spatial, structural, energy and temporal secrecy. To ensure frequency redundancy at the physical level, discrete signals have been widely used, in which the manipulated parameters (amplitude, phase, frequency) are changed at strictly fixed time intervals. Efforts of researchers are aimed at finding ensembles of complex signals, the characteristics of which with increasing duration approach the limit of "dense packing" [1-3], i.e., the ensemble, all members of which have zero constant component, ideal periodic function of autocorrelation (PFAC) and periodic function of cross-correlation (PFCC), and have the largest possible volume.

Theoretical basis of synthesis of discrete derivative signals

A common criterion for such an approximation is the minimax criterion, focused on the synthesis of the ensemble by minimizing the maximum values of the side peaks on the set of all undesirable correlations. The limits for the root mean square and maximum (peak) values of auto- and cross-correlation functions are given in [2, 3].

In particular, the fundamentally achievable values of the maximum side peaks of the periodic autocorrelation function (the limits of "dense packing") for a given period of the sequence N are determined from the ratio [4]:

$$R_{\max}^{a} \geq \begin{cases} 0, \textit{якщо } N \equiv 0 \pmod 4; \\ 1, \textit{якщо } N \equiv 1 \pmod 4; \\ 2, \textit{якщо } N \equiv 2 \pmod 4; \\ -1, \textit{якщо } N \equiv 3 \pmod 4, \end{cases} \quad (1)$$

These limits specify the criteria for the synthesis of a set of DSs (signatures). The ensembles with values corresponding to the boundary (1) are optimal ones and called the minimax ensembles. For an ideal hypothetical ensemble $R_{\max}$ is zero, and for any real ensemble the minimum value of the correlation function can serve as an adequate measure of its proximity to the ideal.

The publication presents the results of research on methods of synthesis and analysis of the properties of different classes of signals, which can be attributed (in accordance with the above limits) to the minimax (optimal) signals. The possibilities are discussed to use the offered signals in modern ICSs as physical data carriers in order to improve, first of all, such performance indicators as information security, noise immunity and secrecy of these systems [4 – 6].

The section proposes a method for synthesis of discrete derivative signals based on the use of nonlinear discrete complex cryptographic signals as the signals generating orthogonal discrete signals (ODS) as initial ones. It is known [7, 8] that ODSs have unsatisfactory ensemble, structural and correlation properties, therefore, the use of the ODS in the ICS, which have increased requirements

for noise immunity, signal secrecy, information security is limited. Preservation of the advantages of the ODS, with simultaneous improvement of correlation, spectral, ensemble and structural properties, can be achieved based on formation of derivative signal systems. Derivative signal systems $^{W(i)}$, for the case of phase-manipulated (PM) signals, are formed by a symbol-wise multiplication of the so-called output signal by a signal that produces $^{H(k)}$:

$$W(i) = H(k) \cdot G(i) \tag{2}$$

In this case, the signal system is used as a source signal, which, on the one hand, does not fully meet the requirements for correlation properties, on the other hand, it has some advantages, for example, the simplicity of technical implementation of construction algorithms. Hadamard systems can be used as such signal systems. It is shown in [2, 3] that generating signals must have good autocorrelation properties (small values of lateral peaks of autocorrelation function) to ensure that derived signal systems meet the increased requirements for information security, noise immunity and secrecy of the ICS operation. Considering the above-said, it is advisable to use characteristic signals and cryptographic signals as generating signals [8, 9].

For the phase shift keyed (PM) signals (including derivatives) of the same duration, integral ratios are known [2]

$$U_{kl}(\tau) = (T/2\pi) \cdot \int_{-\infty}^{\infty} R_{kl}(\tau - \Omega) \cdot R_{\mu\nu}(\tau, \Omega) d\Omega; \tag{3}$$

$$U(\tau) = (T/2\pi) \cdot \int_{-\infty}^{\infty} R_Z(\tau - \Omega) \cdot R_Y(\tau, \Omega) d\Omega, \tag{4}$$

where: $U_{kl}(\tau)$ – cross-correlation function (FCC); $R_{kl}(\tau, \Omega)$ – reciprocal uncertainty function; $R_{\mu\nu}(\tau)$ – reciprocal correlation function; $U(\tau)$ – autocorrelation function of derivative signals; $R_Z(\tau, \Omega)$ – uncertainty function of output signals; $R_Y(\tau, \Omega)$ – uncertainty function of the producing signal.

Analysis of expressions (3) – (4) shows that the correlation properties of the derivative signals depend on the properties of the output signals and the signals producing on the frequency-time plane. Expressions (3) – (4) make it possible to find the following assessment:

$$U_{kl}(\tau) \le (T/2\pi) \cdot \sqrt{\int_{\varphi} \left| R_{kl}(\tau, -\Omega) \right|^2 d\Omega} \cdot \int_{\varphi} \left| R_{\mu\nu}(\tau, \Omega) \right|^2 d\Omega \tag{5}$$

$$U(\tau) \le (T/2\pi) \cdot \sqrt{\int_{\varphi} \left| R_Z(\tau, -\Omega) \right|^2 d\Omega} \cdot \int_{\varphi} \left| R_Y(\tau, \Omega) \right|^2 d\Omega \tag{6}$$

Estimates (5) – (6) depend to a large extent on the value of the width of the integration interval φ, that is, on the ratio of the width of the FCC output signals and the producing signals.

Let us assume that the output signals and the producing signals have the same duration T, and the width of the spectrum of the producing signal F_a is greater than the width of the spectrum of the output signal F_V. It is known that if the mutual uncertainty function (MUF) of the output signals and the producing signals are evenly distributed over the frequency-time plane, then the root mean square value

$$\sigma_{ukl} = 1/2 \cdot \sqrt{F_a \cdot T}, \quad \sigma_{u\mu\nu} = 1/2 \cdot \sqrt{F_v \cdot T}. \tag{7}$$

Since $F_a > F_V$, the width of the MUF of the output signals according to the axis Ω is less than the width of the MUF of the producing signals, therefore $\varphi = 1/2 \cdot \sqrt{F_a / F_y}$. After completing replacement of $R_{kl}(\tau, \Omega))$ and $R_{uv}(\tau, \Omega)$ by their root mean square value, we get

$$U_{kl}(\tau) \le 0{,}5 \cdot \sqrt{F_a / F_v}. \tag{8}$$

From the last inequality, it follows that the values of the FCC of the derivative signals are less than or equal to $0,5 \cdot \sqrt{F_a / F_v}$, which in turn means that the maximum lobes of the CCF will be less than this value. Thus, to reduce the maximum side petals of the CCF, it is necessary to increase the width of the producing signal. It also follows from (8) that the method of derivative signals formation, that is, the signal multiplication process, leads to a decrease in the side lobes of the FCC derivative signals, if the base of the signals producing $F_a \cdot T$ is larger than the bases of the output signals so that $\sqrt{F_v} \cdot T > F_a \cdot T$.

It is quite clear that to obtain $U_{kl} < 1$ (in accordance with (17), there is an inequality

$$F_v > F_a , \tag{9}$$

and the frequency band with the width of $\varphi = 4 \cdot \pi \;\; F_a$ will be narrow compared to the width of the uncertainty function of the producing signal along the frequency axis. Since in the band φ the side lobes are close to the side lobes along the time axis τ at $\Omega = 0$, then as a producing signal should be chosen this one, whose side lobes of the autocorrelation function have small values.

As for the producing signals, they must have good autocorrelation properties, secondly, as many characters (elements) as the output signal, that is, the number of $N = 2^n$ characters, where n – is an integer.

Let us illustrate the possibility of constructing derivatives of discrete signals, for which the rows of the Hadamard matrix of $\mathrm{N} = 256$ order are used as output signals, and cryptographic signals (CS) are used as generating signals $\mathrm{H(k)}$. Tables 1 – 3 give examples of: sequences of symbols: rows of the Hadamard matrix of $\mathrm{N} = 256$ order synthesized by the CS, which in the properties of the periodic autocorrelation function (PFAC) are close to the limit of "dense packing" (1); derivative signals generated in accordance with (2), using the sequences shown in tables 1–2.

It was shown in [2] that the correlation and statistical characteristics of the functions of cross correlation (FCC) of signals used by the ICS subscribers have a significant impact on ensuring the required level of noise immunity of signals reception in multiuser ICSs. One of the statistical characteristics of the FCC is the excess coefficient, which affects the probability of error in signals reception. It was shown in [2, 10] that it is necessary to choose a signal system with the lowest value of the excess coefficient to ensure a lower probability of error.

Based on multiple calculations for signal lengths 64, 256, 1024, 2048, statistical and correlation character istics of the CS and characteristic discrete signals (CDS) [8], as well as derived signals, formed on the basis of these signals, were calculated, and the Hadamard matrix rows of appropriate order were used as source.

Table 1

Matrix row №	The row of the Hadamard matrix ($\mathrm{N} = 256$)
1	[1, -1, 1, -1]
2	[1, 1, -1, -1, 1, 1, -1, -1]

Table 2

Signal №	Cryptographic signal (N = 256)
1	[-1, 1, -1, 1, 1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, 1, -1, -1, -1, 1, -1, -1, 1, 1, -1, 1, -1, 1, -1, -1, -1, 1, 1, 1, 1, 1, 1, -1, 1, -1, 1, 1, -1, -1, -1, -1, 1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, -1, -1, -1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, 1, 1, 1, -1, 1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, 1, 1, 1, 1, 1, -1, 1, 1, -1, -1, -1, -1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, -1, -1, -1, -1, 1, 1, -1, 1, 1, -1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, -1, 1, -1, -1, -1, 1, -1, 1, -1, -1, -1, 1, -1, 1, -1, -1, -1, 1, 1, -1, 1, -1, 1, -1, -1, -1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, -1, -1, -1, 1, -1, -1, -1, -1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, 1, 1]
2	[1, 1, 1, -1, 1, -1, -1, 1, 1, 1, 1, -1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1, 1, -1, 1, 1, 1, 1, 1, -1, 1, -1, -1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, -1, 1, -1, 1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, 1, -1, -1, -1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, -1, -1, 1, -1, -1, 1, 1, 1, 1, -1, 1, -1, 1, 1, -1, 1, -1, -1, -1, -1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1, -1, -1, -1, -1, -1, -1, 1, 1, 1, 1, -1, 1, -1, -1, -1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, -1]

Table 3

Signal №	Derived cryptographic signal (N = 256)
1	[-1, -1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1, 1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, -1, -1, 1, 1, -1, -1, -1, -1, -1, -1, 1, -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, 1, 1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, 1, -1, -1, -1, -1, 1, 1, -1, 1, -1, -1, -1, 1, -1, 1, 1, -1, 1, 1, 1, 1, 1, -1, 1, 1, -1, 1, 1, 1, 1, 1, 1, -1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1, -1, -1, 1, 1, -1, -1, -1, 1, 1, -1, -1, -1, 1, -1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, -1]
2	[-1, 1, 1, -1, 1, 1, -1, -1, 1, -1, -1, 1, 1, 1, -1, -1, 1, 1, 1, -1, -1, -1, 1, -1, -1, -1, -1, -1, -1, 1, 1, -1, -1, -1, 1, -1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, -1, 1, 1, -1, 1, 1, -1, 1, 1, 1, 1, -1, -1, 1, -1, -1, -1, -1, -1, 1, 1, -1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, 1, 1, 1, 1, 1, -1, -1, 1, 1, 1, 1, 1, 1, -1, -1, -1, 1, -1, -1, -1, -1, -1, -1, 1, -1, -1, -1, -1, -1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1, -1, -1, -1, 1, 1, -1, 1, -1, 1, -1, 1, -1, -1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1, -1, -1, -1, 1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, -1, 1, 1, 1, -1, -1, -1, -1, 1, 1, 1, -1, 1, 1, -1, -1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1, -1, -1, 1, -1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, -1, -1]

Based on multiple calculations for signal lengths 64, 256, 1024, 2048, statistical and correlation character(istics of the CS and characteristic discrete signals (CDS) [8], as well as derived signals, formed on the basis of these signals, were calculated, and the Hadamard matrix rows of appropriate order were used as source.

Table 4 shows the data on the results of calculations of the statistical characteristics of the FCC of the signal systems under study (all values are normalized relative to the number of elements of the discrete sequence of symbols). The following is used as the PFCC statistical characteristics: $\frac{R_{\delta\max}}{\sqrt{N}}$ is the maximum value of the PFCC side peaks; $\frac{m_{|R|}}{\sqrt{N}}$ is the mathematical expectation of the module of the FCC side peaks; $\frac{D_{|R|}}{\sqrt{N}}$ is variance of the modulus of the FCC side peaks; $\frac{\mathrm{D}_{|\mathrm{R}|}^{1/2}}{\sqrt{\mathrm{N}}}$ is standard deviation of the modulus of the PFCC side peaks; $\frac{D_R^{1/2}}{\sqrt{N}}$ is standard deviation of the PFCC side peaks; $\frac{\gamma}{\sqrt{N}}$ is the excess coefficient. Tables 5, 6 provide data on the statistical characteristics of the PFCC signal systems and values of the excess coefficient γ for different classes of signals, respectively.

Analysis of the data in Tables 4 – 6 shows that the statistical characteristics of the derived signals formed based on the CS are close to the corresponding characteristics of other signals indicated in the table. In this case, the values of the maximum side outliers of the cross-correlation function of

the derivatives of orthogonal signals formed on the basis of cryptographic signals are less than the values of the maximum lateral outliers of linear M – sequences.

Table 4

Signal	N	$\frac{R_{б\max}}{\sqrt{N}}$	$\frac{m_{\|R\|}}{\sqrt{N}}$	$\frac{D_{\|R\|}}{\sqrt{N}}$	$\frac{D_{\|R\|}^{1/2}}{\sqrt{N}}$	$\frac{D_{R}^{1/2}}{\sqrt{N}}$	$\frac{\gamma}{\sqrt{N}}$
Hadamard	64	2.877606	0.839302	7.505229	0.895450	0.578163	0.080803
CS		2.579922	0.800799	2.940059	0.602640	0.995338	0.045952
Derived		2.557872	0.789343	2.968220	0.605073	0.995257	0.063202
Hadamard	256	5.949502	0.971715	31.327805	1.296748	1.163056	0.226740
CS		3.143866	0.802731	6.078791	0.615274	1.013034	0.052455
CDS		2.919304	0.795529	6.012184	0.611412	1.004272	0.063475
Derived		3.060695	0.792919	5.963091	0.609151	0.992591	0.047281
Derived (CDS) and Hadamard		2.838905	0.786446	6.123228	0.61677	1.000319	0.032270
Hadamard	512	8.535875	1.077900	60.183554	1.514880	1.646411	0.279178
CS		3.302501	0.788752	8.310726	0.605370	1.007827	0.042325
Derived		3.292689	0.790902	8.206162	0.601609	1.004050	0.038807
Hadamard	1024	11.996921	1.182539	110.418690	1.724686	2.096328	0.308414
CS		3.573256	0.801196	11.976469	0.611492	0.991789	0.025411
Derived		3.467752	0.800130	11.831620	0.607747	1.000108	0.026396
Hadamard	2048	17.027296	1.304369	207.508662	1.988573	2.383674	0.314253
CS		3.614201	0.805799	16.805120	0.609234	0.994485	0.020321
Derived		3.575909	0.799557	16.474635	0.603198	0.998075	0.018530

Data analysis of Table 6 shows that derivative signaling systems have lower γ value compared to the generating signals. In addition, it was shown in [4] that for the ODS (rows of the Hadamard matrix of N = 64 order) the excess coefficient is equal to 20, while for derivative signals generated using the ODS and CS it is equal to 0.063202, which significantly (by an order of magnitude) reduces the probability of error when receiving signals.

Table 5

Type of signals	$\frac{R_{\max}}{\sqrt{N}}$	$\frac{m_{\|R\|}}{\sqrt{N}}$	$\frac{D_{\|R\|}^{\frac{1}{2}}}{\sqrt{N}}$	$\frac{D_{(R)}^{\frac{1}{2}}}{\sqrt{N}}$
Signals formed on the basis of m-sequences	1,9 – 6,0	0,8	0,62	1,0
Cryptographic signals (CS)	1,64 – 3,4	0,8	0,6	1,0
Characteristic discrete signals	1,48 – 3,35	0,8	0,7 – 0,78	1,0
Derived signals	1,63 – 3,35	0,79	0,6	0,994
Sequences with 3-level PFCC	1,5	0,76	0,62	1,0

Table 6

Signal class	N	$\frac{\gamma}{\sqrt{N}}$
Cryptographic signals (CS)	64	0.045952
Derived signals (CS and ODS)	64	0.063202
Cryptographic signals (CS)	256	0.052455
Characteristic discrete signals (CDS)	256	0.063475
Derived signals (CS and ODS)	256	0.047281
Derived signals (CS and ODS)	256	0.032270
Cryptographic signals (CS)	512	0.042325
Derived signals (CS and ODS)	512	0.038807
Cryptographic signals (CS)	1024	0.025411
Derived signals (CS and ODS)	1024	0.026396
Cryptographic signals (CS)	2048	0.020321
Derived signals (CS and ODS)	2048	0.018530

Using NIST SP 800-22 [11] (frequency bitwise test (monobit test)), frequency block test (frequency within block test), test for a sequence of identical bits (runs test), test for the longest sequence of units in the block (the longest run test), spectral test (spectral test), series subsequence test (serial test), tests of implementations of derivative cryptographic sequences of symbols (DCSS) were performed. In addition, the DCSS was tested using the FIPS-140 standard (frequency bitwise test (monobit test)), poker test, runs test, the longest sequence of ones/zeros (the longest run test)). Tables 7, 8 show the results of tests carried out on these tests.

Table **7**

The name of the test	X	Condition for successful passing the test	X satisfies the condition
Monobit test	10104	$9654 < X < 10346$	Yes
Poker test	16.806400000000394	$1.03 < X < 57.4$	Yes
Test for the maximum length of the series	12	$X < 34$	Yes

Table 8

Symbol	Series length						Test passed
	1	2	3	4	5	6+	
«1»	2504	1245	605	298	159	187	Yes
«0»	2540	1248	605	303	141	162	Yes

Numerous studies of the statistical properties of derivatives of nonlinear cryptographic sequences of symbols using NIST SP 800-22, FIPS-140 have shown that these sequences, formed using the proposed method [8], meet the requirements for random sequences.

Principles of construction and general characteristics of software and hardware complex for synthesis, research of properties, generation and processing of signals

The presence of its own hardware and software complex for implementing the functions of synthesis, analysis, formation, processing, study of the signal systems properties is an important component in creating and applying the theoretical foundations of signal systems for data in modern ICSs.

The components of the software and hardware complex for the synthesis, study of properties, generation and processing of signals (hereinafter – the Complex) are as follows.

Component 1: software for generating/synthesizing signals with given parameters according to the available models (available models of signal construction are laid down at the programming stage, only the configuration parameters are variable). The result of the work of this tool is the generated files with discrete sequences, which can then be used for analysis or for implementation in the ICS (communication system), as a basis for signals – physical data carriers formation.

Component 2: complex software tool for research of statistical, correlation, ensemble and structural (cryptographic) properties of the sequences being synthesized. Particular attention has been given to the analysis of cryptographic properties of the DS, for which the appropriate tests are used. As a result, the complex generates source files that can be further used to display graphically the results in the form of 2D and 3D graphs.

Component 3: software tool for graphical display of research results, which may include third-party software, such as MathCad, MatLab (if necessary, input data processing), or Grafana. Both the source files of Component 1 and the source files of Component 2 can be used as source data. As a result, the user receives the constructed images of various types of correlation functions, the tables containing results of calculations (researches) of properties of signals.

It is possible to note such features of the created Complex.

1. A separate module for data access control (the database and system disk) has been introduced into the structure of the Complex. The functioning of the authentication and authorization system has been provided, which allows users to work simultaneously without interference and to get access their results. After performing the appropriate functions, the results can be sent to the user's e-mail.

2. Combination of these components of the Complex into a single web service. The main idea of creating the Complex consists in developing an accessible user interface that allows even a user who does not have certain qualifications in the field of construction and analysis of signals, to implement the functions of the complex. The decision to duplicate the results is due primarily to the desire to minimize the risk of data loss. The presence of a single web service opens the possibility of simultaneous use of the Complex's capabilities by many users. The presence of the user interface made it possible to expand the capabilities of the Complex without the need to make changes to the program code, as well as to increase the performance of the complex several times.

3. Modularity and openness of the Complex, in the sense of expanding the possibilities for the synthesis, formation, processing and analysis of various classes of signals. Considerable attention has been given to variability and expansion of possibilities for the synthesis of cryptographic signals (CS): generation of a cryptographic key; selection of the necessary library and algorithm of cryptographic algorithm, key data, etc., and all this without interfering with the program code.

4. An adaptive algorithm for configuring the number of simultaneous flows on the CPU has been used to increase the speed of the processes of signals formation, processing, analysis of their properties. This approach makes it possible to increase the overall performance of the software solution, depending on what hardware it is running.

5. All results are generated with the preservation of the original data and system parameters, which allows you to reproduce the obtained result at any time.

Hardware characteristics of the working machine currently used for signal synthesis and analysis (only parameters that have a direct impact on the performance of the complex and the preservation of the obtained results are indicated):

- CPU (central processor unit): Intel iCore i7, 7th Gen (2.9 – 3.4 GHz);
- RAM (random access memory): 16 Gb;
- media type: SSD Kingston (up to 550 Mb/s for recording and up to 520 Mb/s for reading)
- Software features of the constructed complex (programming languages, details of construction of the interface):
- programming language of the back-end part: Java 8 (using the latest features for parallel processing);
- additional libraries and dependencies (back-end): Spring Boot, Spring Security, BouncyCastle security lib;
- programming language of front-end (UI) parts: JavaScript, TypeScript, HTML, SCSS;
- additional libraries and dependencies (front-end): Angular 8;
- components for construction of graphic elements (graphs, diagrams): elements constructed with the use of Angular Framework, Grafana tools and modules;
- storage of results: file system (for source files) + duplication in MySQL database.

Conclusions

The method has been proposed for the synthesis of discrete derivative signals based on nonlinear discrete complex of CSs as producing signals and orthogonal signals formed on the basis of the Hadamard matrix rows as source ones. The choice of the CS is due to the fact that this class of signals has improved autocorrelation, ensemble, structural properties, as well as statistical properties of cross-correlation functions (primarily, the values of maximum side peaks, peak dispersion and excess coefficient). Based on computer simulation and calculations, it is shown that derived signals formed based on cryptographic sequences and rows of the Hadamard matrix have improved, com-

pared to orthogonal and linear signal classes, ensemble, correlation and structural properties. The complex of hardware and software has been developed making it possible to realize synthesis, formation, processing, study of nonlinear CS, nonlinear signals in the Galois finite fields, derivatives of the signal system, M sequences, etc. This complex is almost ready for possible use as part of prototypes and elements of digital communication tools of modern ICS. The architecture of the obtained software and hardware complex, with the use of additional mathematical apparatus, makes it possible to carry out synthesis and analysis of many classes of signals, including those given in this publication. The use of nonlinear complex signals with the necessary properties, the theoretical foundations of which are proposed in this publication, will increase the noise immunity of signals (probability of correct signal reception) and information security and secrecy of modern information and communication systems under conditions of cyber attacks, natural and organized, including structural, relayed and other interference.

References

1. Ipatov, Valery P. Spread Spectrum and CDMA. Principles and Applications / Valery P. Ipatov. University of Turku, Finland and St. Petersburg Electro technical University 'LETI', Russia / John Wiley & Sons Ltd, The Atrium, Southern Gate, Chi Chester, West Sussex PO19 8SQ, England. 2/
2. Varakin L. Ye. Sistemy svyazi s shumopodobnymi signalami [Communication systems with noise-like signals].1985.384 p.
3. Sarvate, D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Parsley // IEEE Trans. Commun. 1980. Vol. Com 68. P. 59–90.
4. Sverdlik M.B. Optimal discrete signals. M. : Sov radio, 1975. 200 p.
5. Sung-Moon, Michael Yang. (2019). Modern Digital Radio Communication Signals and Systems. Springer, 679. doi: https://10.1007/978-3-319-71568-1.
6. I.D. Gorbenko, A.A. Zamula, V.L. Morozov Information security and noise immunity of telecommunication systems under conditions of various internal and external impacts // Telecommunications and Radio Engineering. 2017. Vol. 76, Issue 19. P. 1705-1717.
7. Gorbenko I.D., Zamula A.A., Semenko E.A., Morozov V.L. Method for complex improvement of characteristics of orthogonal ensembles based on multiplicative combining of signals of different classes // Telecommunications and Radio Engineering. 2017. Vol. 76, Issue 18. P. 1581 1594. DOI: 10.1615/TelecomRadEng.v76.i18.10.
8. Ivan Gorbenko, Alexandr Zamula. Devising methods to synthesize discrete complex signals with required properties for application in modern information and communication systems. 2021 // Eastern-European Journal of Enterprise Technologies 2021-06-30. P. 16 – 26. DOI: 10.15587/1729-4061.2021.234674.
9. Ivan Gorbenko and Alexandr Zamula. Theoretical Basis of Synthesis of Complex Signal Quasiortogonal Systems. In.: ISCI'2020: Information Security in Critical Infrastructures : Collective monograph. Edited by Ivan D. Gorbenko, Victor A. Krasnobayev and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2020, pp. 11-28 – ISBN: 978-1-7362833-0-1 (Hardback), ISBN: 978-1-7362833-1-8 (Ebook).
10. Gorbenko I., Zamula A., Morozov V. Information and communication systems based on signal systems with improved properties building concept. CEUR Workshop Proceedings, 2019, 2353. P. 974-991.
11. NIST 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2000.

Надійшла до редколегії 03.09.2021

Відомості про авторів:

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; АТ «Інститут інформаційних технологій», головний конструктор; Україна; e-mail: GorbenkoI@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-4616-3449

Замула Олександр Андрійович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; email: zamylaaa@gmail.com; ORCID: http://orcid.org/0000-0002-8973-6190

UDC 621.317.76.089.68+681.3.07 (3.06) **DOI:10.30837/rt.2021.3.206.03**

O.P. NARIEZHNII, Cand. Sc. (Technology), T.O. GRINENKO, Cand. Sc. (Technology), I.D. GORBENKO, Dr. Sc. (Technology)

STATEMENT OF THE PROBLEM OF ASSESSING INSTABILITY OF PASSIVE QUANTUM FREQUENCY STANDARDS IN THE PRESENCE OF AN ERROR FROM THE INTERACTION

Introduction

Problem statement. Creation of quantum generators (masers and lasers) is deservedly considered one of the greatest achievements of physics in the second half of the 20th century [1]. This discovery led to the emergence of a new branch of technical physics, namely, quantum electronics. In this area of outwardly traditional research, the issues of the theory of interaction of a radio-frequency field with matter and the elements of the theory of quantum amplifiers and generators have been sufficiently well studied. However, over the past two decades, revolutionary changes have taken place that have significantly transformed the scientific and technological appearance of quantum electronics. These changes are associated, first of all, with the emergence of many new fundamental and applied problems of coordinate-time support [2 – 4]. As a result of such a radical expansion of the range of problems, the issues of the influence of the error from the interaction on the estimation of the frequency instability of passive quantum standards of frequency (QSF) are still poorly understood. This is due to the laboriousness of this measuring task associated with the involvement of complex and expensive equipment. This equipment makes it possible to use the atomic time scales (TS), formed by global navigation satellite systems (GNSS) such as GPS\GLONASS, and atomic weighted average scales of spatially separated group standards of frequency and time.

Analysis of the literature. Of the whole variety of studied atomic and molecular transitions caused by hyperfine interactions in atoms or the result of perturbations of the electronic structure in molecules, to create frequency references, atoms or molecules are mainly used, the transition frequencies of which lie in the range of 1...30 GHz [5 – 7]. At the same time, the following types of the QSF have been studied quite well: quantum generators based on beams of ammonia molecules, beams of hydrogen atoms and rubidium vapor with optical pumping; passive QSF on beams of cesium atoms and rubidium vapor with optical pumping and optical indication, etc. [5, 8].

The functioning of these QSF is based on the methods of radio spectroscopy. For example, the most common cesium and rubidium QSF are based on the method of passive atomic beams, based on the interaction of a radio-frequency field with a beam of atoms or molecules. Because of interaction, transitions occur between atomic states. The most precise hydrogen QSF, as well as optically pumped rubidium standards, are based on the method of constructing a standard on a maser, where an atom or molecule is injected into a resonator tuned to the transition frequency.

The accuracy of the passive QSF, based on the measurement of the position of the resonance absorption line, depends on the width of the spectral line. The narrower the line, the higher the accuracy. It is known, that the effect of external fluctuating fields of different physical nature (temperature, electromagnetic, gravitational, etc.) on the QSF leads to the appearance of additional frequency fluctuations in their output signal, due to these influences. A large number of specialists in the theory of quantum amplifiers and oscillators are engaged in compensation for these destabilizing factors affecting the spectral line width.

In general, the issues of the QSF interaction when combining their group have not been sufficiently studied to date. The issues of electromagnetic compatibility of frequency measures in a group are especially poorly studied. In this case, the standard frequency separation requirement does not apply, since all frequency measures used have practically the same frequency of oscillation.

The main part

Determination of spatial coordinates and velocity components is based in navigation systems on rangefinder and Doppler measurements. At the same time, the need for high stability of the systematic TS increases as the requirements for the accuracy of navigation determinations increase, especially when using the passive GNSS rangefinder method such as GPS\GLONASS. Therefore, the radio navigation field in the GNSS data, along with the main function (global autonomous operational navigation of ground mobile objects), allows mutual synchronization of the QSF at remote ground objects. The most precise comparisons of the TS using GNSS are carried out in the differential navigation mode. The differential navigation method is based on the relative constancy of a significant part of the GNSS errors in time and space [3].

In navigation systems, the formation of the systemic TS and its maintenance (storage) during the entire life of the system is carried out by atomic clocks. For modern atomic clocks, the relative frequency instability is $(1\ldots5)\cdot10^{-14}$ and below [7]. Of course, to maintain such a high stability, it is necessary to create a complex hardware complex. The task of this complex is to ensure the functioning of the core of the atomic clock, namely, an atomic (quantum) frequency standard under conditions of constant temperature, minimal influence of external and internal electromagnetic fields, exclusion of vibrations, etc.

It is known that the equation of the atomic clock motion, based on the fundamental concepts of quantum mechanics, in the general case can be represented in the $j\frac{h}{2\pi}\partial\Psi/\partial t = \mathrm{H}\Psi$ form, where Ψ is the wave function; H is the Hamiltonian; h is Planck's constant, and $j=\sqrt{-1}$. The consequence of this equation of motion of the atomic clock (QSF) is the law $\Delta E = h\nu$, where ΔE the difference in energy is, ν is the frequency of radiation. Thus, the postulate of the high stability of the atomic TS follows from the assumption of the invariability of the frequency corresponding to the energy difference ΔE.

At the same time, despite significant advances in the creation of atomic clocks (QSF), there are areas of their practical application, which, in principle, cannot be satisfied with the achieved level. These areas include metrological support for time and frequency measurements. In some cases, while ensuring high metrological characteristics, extremely high requirements are imposed on the reliability of the device.

These difficulties are often solved in practice by building group time and frequency keepers. Analytical (based on calculations) and instrumental (based on appropriate signal conversion) combining of the QSF (generators) into one group, as stated in [9-16], makes it possible to increase the accuracy and stability of the keeper based on averaging the characteristics of several generators and reliability based on their reservation. Modern group time and frequency keepers include up to ten, and reference means up to several dozen QFS.

Analytical methods of averaging the frequency of group keepers allow calculating corrections to the frequency of individual custodians at any time. The use of these corrections in order to regulate the frequencies of the keepers allows maintaining the frequency at the output of the keeper close to the weighted average. The weight (contribution) of each QSF from the group to the formation of the weighted average frequency is inversely proportional to the estimate of the variance of the frequency deviation of each of them from the weighted average for the entire group [11].

Determination of weighting factors based on the results of intercomparisons of QSF in a group encounters two problems.

First, to obtain unbiased estimates of the weighting coefficients, it is necessary to estimate and eliminate the average value of deviation of the frequency of each QSF from the weighted average value. This value, in turn, is determined from the condition that the unbiased estimates of the weight coefficients are known. That is, a certain contradiction arises, the resolution of which allows inaccuracies in the form of certain assumptions based on subjective factors.

Secondly, since only the frequency differences of the output signals of the used QSF can be determined in the process of intercomparisons, in the estimates of the variance of the results of paired comparisons, in addition to the estimates of the variance of the intrinsic noise of each measure, second mixed central moments are added. In the general case, in the presence of an error from mutual interaction, for a system of N measures, there is a need to determine N^2 unknown estimates of the variance of the intrinsic noise of each quantum measure (QSF) and the second mixed central moments. When implementing a complete graph of comparisons, it is possible to obtain $(N-1)^2$ estimates of the second central moments, which can be used as the right-hand sides of a system of linear equations with respect to the desired quantities. According to the theorems of linear algebra, such a system has no unique solution. This determines the inability to determine reliably the weight coefficients for estimating the weighted average value of the frequency of the group measure (standards) based on the results of intercomparisons of measures in the group. Even under the assumption that there is no cross-correlation between the output signals of measures in the group (which contradicts experimental studies), the solution of this system of equations is impossible. Since in this case the rank of the system will be equal to $(N-1)$ in the presence of N unknowns [17]. The rest of the equations of the system in the implementation of the graph of comparisons with the number of nodes exceeding the number $(N-1)$ will be linear combinations of the first $(N-1)$ equations. Resolution of this contradiction requires some subjective assumptions.

Thus, the problem of forming group TS and reference frequencies in the interpretation of the methods of mathematical physics and computational mathematics belongs to the class of ill-posed problems, the solution of which is possible only with the development of an appropriate regularizing algorithm. One of the promising directions in the search for regularizing algorithms is the construction of identification models based on information about the physical processes occurring in the system under consideration [18].

So in the behavior of real group quantum measures (standards), one pattern can be traced: along with the phase drift (stroke of the TS) caused by the deviation of the actual frequency from its nominal value, there are slow phase oscillations relative to its linear drift [14, 15]. These fluctuations can be classified as a manifestation of the Markov fluctuation process. However, the presence of quasi periodicity of such fluctuations suggests the presence of harmonic components with non-multiple frequencies in the spectrum of the output signal of each measure. Indeed, in the presence of electrical or electromagnetic connections between the QSF (measures) included in the group and located quite close to each other, as well as having electrical connections through the means of mutual comparisons, we can assume the formation of a system of coupled oscillators with close frequencies.

In [14], the presence of regular periodic components in the spectrum of the output signal emitted by the GPS equipment and generated by a group of the QSF on board each satellite is shown. Similar results were obtained in [15, 16].

The approach to a group measure as a system of coupled oscillators can allow one to create a model with such a number of parameters that can be unambiguously determined from the results of intercomparisons. For example, the vector equation of state for a group of frequency measures can be represented as a system of differential equations with a set of parameters that are uniquely determined from the results of intercomparisons. This system can be uniquely solved in the class of periodic functions, and the result of the solution can be used to estimate the predicted state of the frequency and phase of the output signal of each measure based on the results of processing their current and previous states. If such estimates are valid, they can be used in the procedures for correcting the output signal of each measure or leading measure in order to compensate for the frequency deviation from the nominal value or the TS stroke.

At present, there are no known hardware methods for compensating the error from interaction in the spectrum of the output signal, since the relative frequency difference between the QSF

included in the group does not exceed the value $1 \cdot 10^{-11}$. The known methods of numerical processing of results of intercomparisons of the output harmonic signals phases are based on their correlation processing and the subsequent application of the apparatus of the discrete Fourier transform [19]. However, the use of such an approach in the presence of such low frequencies in the spectrum contains two problems.

First, the calculation of the autocorrelation function based on the results of intercomparisons of the QFS included in the group, with a sampling rate equal to one second, requires more than the daily time spent by modern processors.

Second, the autocorrelation function, strictly speaking, is an aperiodic function, and therefore, to determine its spectrum (spectral power density of the phase noise of the QSF), it is necessary to use the integral Fourier transform. In this case, methodically, the apparatus of the discrete Fourier transform is applicable only for strictly periodic functions. Application of this apparatus to aperiodic functions leads to methodological errors in determining the spectral density of the process under study. In addition, the presence of the so-called "frequency masking" effect negates the possibility of accurate and unambiguous determination of the frequency values present in the spectrum of powerful spectral components. Obtaining an estimate of the spectral power density of fluctuations of the phase (frequency) of the QSF output signal is the first step in the mathematical formulation of the problem of constructing the structure of its model. In this case, structural identification is carried out for a qualitative description of the investigated process of fluctuations with the help of various operators.

The basis of the mathematical models describing physical processes in the QSF are most often differential operators. At the same time, a distinction is made between models with lumped parameters, described by ordinary differential equations, and models with distributed parameters, described by partial differential equations. For physical processes taking place in continuous QSF media, the transfer of information about the influencing process occurs through a continuum of material points. In the general case, the variables characterizing the state of the object under consideration (atomic beam, optical cell, etc.) are functions of both time and spatial coordinates. Partial differential equations should be used to describe such a physical process. However, in a number of cases, it is possible to introduce generalizing characteristics or functions into the model, which make it possible to reduce a multidimensional problem to a one-dimensional problem, that is, to go over to a model with lumped parameters.

The second step of the mathematical formulation of the problem is to introduce qualitative information into the QSF model, i.e. to determine (estimate) unknown characteristics (model parameters) included in the structural model. This stage is called parametric identification. Structural and parametric identification of physical processes in the QSF is closely related to the solution of inverse problems for differential equations. When formalizing general formulations and identifying the main classes of inverse problems, it is assumed that the formulations of direct problems are known, each of which can be compared within the framework of an identifiable model with a certain set of inverse problems. In what follows, we will consider physical processes in the QSF from the point of view of "cause – effect" relationships. In accordance with the causal model, causal characteristics include boundary conditions and their parameters, initial conditions, coefficients of differential equations that determine the geometric parameters and material substance of the object under consideration (atomic beam, optical cell, etc.). In addition, the causal characteristics also includes the influence external to the object under consideration, which, as a rule, determines the right side of the differential equations. Then the investigative characteristics will describe the states of the object under study, which are usually understood as fields of physical quantities of one nature or another (temperature field of a quartz resonator, its resonant frequency, phase of the output signal of a measure, etc.).

Causal characteristics do not depend on the investigative manifestations in the sense that the first ones can be specified by rather arbitrary values independently of the second ones.

The selected types of quantities are interconnected by a unidirectional causal relationship, the

establishment of which is the goal of the direct problem. If, according to certain information about physical fields or processes obtained as a result of measurements, it is required to restore some causal characteristics, then an inverse problem is obtained. So the inverse problems include: the synthesis of the equation of the QSF state, the determination of the impulse or transient characteristics of the object (atomic beam, optical cell, etc.).

Violation of the causal relationship, which takes place in the formulation of the inverse problem, can lead to its mathematical incorrectness [20], most often to the instability of the solution. Therefore, inverse problems represent a typical example of ill-posed problems [21].

By a mathematical model of a certain physical process occurring in the QSF, we mean a set of equations and relations that describe this process, including the initial and boundary conditions for differential equations. In cases where the structure of the QSF mathematical model is given, but some characteristics of the model require their quantitative determination, i.e. it is necessary to solve the problem of parametric identification, in most situations such a problem is solved based on the experimental data (identification of a mathematical model from experimental data). However, another form of identification is possible, e.g., according to the reference mathematical model. In the latter case, the role of the original is played by the process model, which is quite complete and quite accurate, but as a rule, complex and time-consuming in practical application, which necessitates the development of a simpler model. Since the causal characteristics of physical processes in the QSF are usually subject to evaluation, parametric identification is associated with the solution of inverse problems. This leads to the need to determine the correctness of the inverse problem formulation [22]. The Hadamard condition [23] is usually used as a correctness criterion, if the operator equation of the QSF state is obtained

$$Au = f,\ u \in U,\ f \in F, \tag{1}$$

where u and f are, respectively, the sought and observed characteristics belonging to metric spaces U, F, and the operator $A: U \to F$, which is assumed to be defined by a continuous linear or nonlinear, integral, differential or algebraic operator, has a domain of definition $D(A) \subseteq U$ and a range of values $R(A) \subseteq F$. $R(A) \subseteq F$.

The problem of solving equation (1) is called correctly posed according to Hadamard if:

1) for any $f \in R(A) = F$ there is a solution $u \in U$ (solvability condition);

2) the solution is unique in U (solvability condition);

3) the solution depends continuously on f (stability condition).

If at least one of the listed requirements is violated, problem (1) is called ill-posed.

The question of the existence of a solution to equation (1) consists in the study of belonging $f \in R(A)$. Therefore, U, F spaces should be chosen consistent with each other. For example, if a solution is sought in a specific class of functions, then the choice f cannot be arbitrary, the set of functions on the right-hand side must ensure that the solution to equation (1) belongs to this class.

It is known [24] that most inverse problems of mathematical physics are reduced to solving equations of the first kind (equations of type (1)) with completely continuous compact operators A. In this case, A^{-1} operator, inverse of a completely continuous one, is unbounded [23]. As a result of this, the solution of problem (1) with different, but close to each other, right-hand sides $f, f + \tilde{f} \in F$:

$$u_1 = A^{-1} f,\ u_2 = A^{-1}\left(f + \tilde{f}\right),$$

can differ from each other as much as desired [25].

Let us consider this situation in somewhat more detail for the case when A operator is given in the form of a linear integral operator generated by a specific type of differential equation in combination with certain initial and boundary conditions:

$$Au(x) = \int_{\Omega} u(x')K(x,x')dx'. \quad (2)$$

Here the integral is understood in the sense of Lebesgue, Ω is a measurable region in the n-dimensional space; $K(x,x')$ is a function measurable in its variables, defined on $\Omega \times \Omega$.

Operator (2) is defined for each measurable function $u(x)$ such that the product $u(x')$ and $K(x,x')$ is a function summable over x' on Ω set. Let the function $u(x)$ be treated as an element of space $L_2[\Omega]$, and the kernel $K(x,x')$ satisfies the condition for the existence of a finite integral

$$\int_{\Omega}\int_{\Omega} K^2(x,x')dxdx' < \infty. \quad (3)$$

It was shown in [25] that such A operator is completely continuous and, therefore, has no bounded converse. Therefore, the values of A operator for arbitrarily large variations in $u(x)$ can differ arbitrarily little from the values of this operator on some $u(x)$ "support" function. As a consequence, the inverse mapping $A^{-1}f$ will not have the property of continuity.

A operator meeting the above requirements is a general case when considering linear formulations of various problems of measuring the QSFparameters. In this case, the kernel $K(x,x')$ usually corresponds to one or another Green's function or the kernel of the corresponding potential of a simple or double layer [26]. These functions, as a rule, satisfy requirement (3), in particular, they are continuous (a stronger constraint than (3)). Bounded and closed areas are usually considered as Ω.

It is important to note that the transition from problem (1) to its extreme formulation, namely, the search for an element u from the condition of minimizing the residual functional:

$$u = \arg\inf_{u \in U} \rho_F(Au, f), \quad (4)$$

does not make the task correct.

Residual $\rho_F(Au, f)$, as the distance between elements Au and f in space F, continuously depends on f. Consequently, small changes in f give rise to small changes in the residuals $\rho_F(Au, f)$, which, in turn, can correspond to arbitrarily large deviations in the solution and, i.e. convergence in the functional does not imply the convergence of the approximate solutions of the inverse problem to the true one. Moreover, the conditionality of the variational problem (4) as a property characterizing the order of influence of the smallness of the error in the task f on the solution u may turn out to be worse than the conditionality of the original formulation (1).

The correctness of the problem statement from the point of view of the stability of the solution depends on the choice of a pair of spaces U and F. This choice cannot be arbitrary. In particular, the right-hand side of equation (1) is usually associated with the results of measurements on some real object and, therefore, is burdened with random errors. These errors occur at any point in the segment $[0, \tau_m]$, i.e. $f_\delta(\tau)$ may even be a discontinuous function, which leads to an unstable solution of the inverse problem.

An important role in the solution of inverse problems of measuring the QSF parameters is played by the concept of conditionally correct problems. In [27], requirements are formulated that turn out to be natural in the formulation of problems that are ill-posed in the sense of Hadamard. The essence of these requirements is that an a priori assumption about the existence of a solution and its belonging to a given compact set is added to the conditions of the problem statement. To establish the conditional correctness, it is necessary to prove the uniqueness theorem.

A wide range of studies on conditionally correct problems was carried out in [28 – 30]. Various aspects of the theory of conditionally well-posed problems of mathematical physics are considered

in [31, 32]. Tikhonov A.N. in [28] introduced the notion of regularization. Its essence is that instead of an unbounded operator giving an exact formula for solving an ill-posed problem, a sequence (regularizing family) of continuous operators is considered such that on each element belonging to the domain of existence of a solution, the corresponding sequence converges to a solution.

One of the interesting approaches to the formulation of problems that are incorrect in the Hadamard sense is the use of concepts and methods of the theory of probability. M.M. Lavrent'ev and V.G. Vasil'ev developed these concepts and methods in the most complete form [32]. In works in this direction, the concept of stability is established, algorithms for solving various classes of problems that are optimal in a certain sense are constructed under certain assumptions about the probabilistic properties of errors in the input data and about the probabilistic properties of the set of sought solutions. In [33], a numerical method was formulated for solving inverse evolutionary equations based on the so-called quasi-inversion. A regularizing operator with a small parameter is added to the evolution equation, which is the product of the original operator and its conjugate one. The small parameter is selected based on the specially developed optimal estimates in the solution. The quasi-inversion method is very simple to implement for solving evolutionary problems of mathematical physics.

The paper [34] presents a method for solving conditionally correct problems of evolutionary type based on the application of the method of minimum residuals for the entire space-time domain of the solution definition. Regularization in this method is performed by choosing the optimal number of steps of the iterative process based on an a priori estimate of the errors in the input data. The trend in the development of methods for solving conditionally correct problems indicates that the methods used are closely related to methods for optimizing the computational process.

Statement of the problem of assessing the instability of passive quantum standards of frequency in the presence of an error from the interaction

The measurement of the metrological characteristics of the QSF (quantum measure) is carried out by comparing it with a standard or an equally accurate quantum measure using a frequency (phase) comparator. Due to the proximity of the reference frequencies of quantum generators, the comparator cannot provide complete electrical (electromagnetic) isolation of the input signals. As a result, it can be argued about the formation of an electrical (electromagnetic) relationship between the quantum generators involved in the comparison process.

From the sections of the theory of oscillations, it is known that systems of quantum generators having common electrical connections are described by a system of second-order differential equations in the form:

$$\ddot{U}_i + \beta_i(U_i)\dot{U}_i + \omega_{0i}^2 U_i = \sum_{\substack{k=1 \\ k\neq i}}^{N} \alpha_{ik}\ddot{U}_k\,, \tag{5}$$

where in $U_i = A_i \cos\left[\omega_{0i}t + \psi_i(t)\right]$ is electric voltage fluctuations on the output of the QSF with slowly varying amplitudes A_i and phases $\psi_i(t)$; $\beta_i(U_i)$ is decrement of the i-th quantum generator, a nonlinear function that depends on the signal level of the generator; ω_{0i} is the natural resonant frequency of the i-th quantum generator; $\omega_0 \approx \frac{1}{N}\sum_{i}^{N}\omega_{0i}$ is the nominal value of the frequency of generation of the QFS; α_{ik} is the coupling coefficient between the i-th and the k-th generators in the group.

System (5) can be reduced using the method of slowly varying amplitudes to a system of truncated first-order differential equations with respect to slowly varying amplitudes and phases of quantum generators included in the system. Under the assumption of the additivity of the noise

vector ξ_i, the state vector of system (5) can be written in the form of the differential Langevin equation [17]

$$\frac{d\vec{\Psi}(t)}{dt} = F\left[\vec{\Psi}(t),t\right] + G\left[\vec{\Psi}(t),t\right]\vec{\Xi}(t),\ \vec{\Psi}(t_0) = \vec{\Psi}_0, \tag{6}$$

where $\vec{\Psi}(t) = \{\psi_i\}$ is the N-dimensional vector of the current values of the frequency of each quantum measure; $\vec{\Xi}(t) = \{\xi_i\}$ is N-dimensional vector of shaping noise (white noise); $F\left[\vec{\Psi}(t),t\right]$ and $G\left[\vec{\Psi}(t),t\right]$ are deterministic continuously differentiable functions of their arguments that satisfy the Lipschitz condition [35]: $|f(x,y) - f(x,\eta)| \le M_b|y-\eta|$, M_b is some positive constant.

If the functions $F\left[\vec{\Psi}(t),t\right]$ and $G\left[\vec{\Psi}(t),t\right]$ are known, then it can be argued that the current state of the system of coupled oscillators as a whole has been determined. Indeed, stochastic integration in the sense of Ito [17] of the right and left sides of Eq. (6) (in the extreme case, by numerical methods) leads to an explicit expression of the current state of the system of coupled oscillators $\vec{\Psi}(t)$.

Thus, to solve the problem of determining the metrological characteristics of quantum measures by group comparisons, it is necessary to find in one way or another the expression of the functions $F\left[\vec{\Psi}(t),t\right]$ and $G\left[\vec{\Psi}(t),t\right]$.

Let us represent the process of measuring phase noise in the form of a mathematical expression, i.e., the observation equation [17]

$$\vec{Z}(t) = h\left[\vec{\Psi}(t),t\right] + \vec{\eta}(t), \tag{7}$$

where $\vec{Z}(t)$ is the vector of current values of the measurement results, the dimension of which corresponds to the number of meters included in the system; $h[*]$ the vector-function mathematically expresses the relationship between vectors $\vec{\Psi}(t)$ and measurement results; $\vec{\eta}(t)$ is the noise vector of the meters (comparators).

Since the frequencies of all quantum generators of the system under consideration are very close ($\omega_0 \approx \omega_{0i} \le 10^{-10}$), the indicated spectral lines will be in the near zone of the natural frequency of each measure. This will naturally lead to a sharp increase in the power spectral density of the phase noise near the carrier. These spectral lines do not have a frequency multiplicity; therefore, the external manifestations of this phenomenon will be equivalent to the behavior in time of noises such as random wanderings.

Since only the phase difference of the oscillations $\Phi_{ik} = \psi_i - \psi_k$ generated by the i-th and k-th measures (QSF) is subject to direct measurement with the help of comparators, in the general case ψ_i is not observational. Accordingly, the expression for the single-sideband (SSB) power spectral density of the phase noise, the phase difference Φ_{ik} in the beat mode will have the form:

$$S_{\Phi_{ik}}(\omega) = U_o^2\delta(\omega) + \frac{1}{2}\sum_{k=1}^{K_{ik}} A_k^2\delta(|\omega| - \Omega_k) + S_{\xi_{ik}}(\omega), \tag{8}$$

where $\delta(\omega)$ is the symbolic impulse function of Dirac; $S_{\xi_{ik}}(\omega)$ is the power spectral density of the difference in the intrinsic phase noise of the i-th and the k-th measure; K_{ik} is the number of significant fluctuations in the phase difference between the i-th and k-th measures, due to beating

with the signals of other quantum measures in the group and among themselves; Ω_k is the frequency of the k-th bright spectral line in the spectrum of the phase of the output signal of the i-th measure.

Indirect measurement methods of $S_{\Phi_{ik}}(\omega)$ are based on measuring a set of estimates of the variance of $D_N(\tau)$ fluctuations of the phase difference of the output signal of a measure, obtained at different time measurements τ and subsequent inversion of the Fredholm integral equation of the first kind

$$2\int_0^\infty S_{\Phi_{ik}}(\omega)K_N(\omega,\tau)d\omega = D_N(\tau), \tag{9}$$

where $K_N(\omega,\tau)$ is the kernel of the integral equation, the form of which is determined by the method of obtaining the estimate $D_N(\tau)$ [18].

The inversion of equation (9) by numerical methods is associated with the discretization of this equation and its transformation to a system of algebraic equations of the form:

$$D_N(\tau_i) = \sum_{j=1}^{M} S_{\Phi_{ik}}(\omega_j)K_N(\omega_j,\tau_i)\Delta\omega, \text{ with } i = 1,2,...n.$$

In the matrix form, this expression takes the form:

$$\vec{D}_N = A\vec{S}_{\Phi_{ik}} + \vec{\eta}, \tag{10}$$

where $\vec{D}_N^T = \{D_N(\tau_1),\ldots,D_N(\tau_N)\}$ is the vector of estimates of the variance of the noise of the quantum measure, obtained at the corresponding measurement times of the current frequency value τ_i; A is a well-known matrix with dimensions $n \times M$, each element of which is multiplied by the quantization step of the original integral equation in the analysis frequency range, and, accordingly, is equal to Δf; $\vec{S}_\varphi^T = \{S_\varphi(f_1),\ldots,S_\varphi(\tau_M)\}$ is the vector of the sought-for values of the spectral power density of the phase noise at the frequencies f_i.

Matrix A elements represent the numerical values of the square of the modulus of the corresponding frequency response obtained for certain values of the parameters $f = f_i$ and $\tau = \tau_i$. The variance of the comparator (meter) noise σ_c^2, similar to the variance of the quantization noise σ_q^2, remains constant for all measurement intervals τ_i. Hence, the following expression for the measurement matrix $\Sigma = (\sigma_c^2 + \sigma_q^2)\cdot \mathrm{I}$ is valid, where I is the identity matrix.

The accuracy and stability of solutions is determined by the conditionality of the matrix $(A^T\Sigma^{-1}A)$ [18]. A quantitative estimate of the conditionality of an arbitrary square matrix is the condition number $q = \mu_{\max}/\mu_{\min}$, where $\mu_{\max}$ and $\mu_{\min}$ are the maximum and minimum eigenvalues of the matrix under study. For, $q > 10^v$ where $v > 1$, and not absolutely precisely defined matrix $(A^T\Sigma^{-1}A)$, solution (10) is unstable and has a large error.

Obtaining a stable solution to equation (10) is possible by regularizing it. The essence of the regularization method as applied to the problem under consideration is the transformation of the Fredholm integral equation of the first kind to the Fredholm equation of the second kind [18]. The statistically regularized estimate is in a sense adequate to the Bayesian procedure and comes down to the following.

Let the a priori (for example, the solution in the form (10)) distribution of the vector $\vec{S}_\varphi$ components be known and the first two moments of the random variable $E\left[\vec{S}_\varphi\right] = \vec{m}_S$ and $E\left[\left(\vec{S}_\varphi - \vec{m}_S\right)\left(\vec{S}_\varphi - \vec{m}_S\right)^T\right] = P_S$ are known. With Gaussian measurement noise η, the optimal Bayesian estimate $\vec{S}_\varphi^*$ corresponds to the minimum of the quadratic form $L(\vec{S}_\varphi) = \left(\vec{D}_N - A\vec{S}_\varphi\right)^T \Sigma^{-1}\left(\vec{D}_N - A\vec{S}_\varphi\right) + \left(\vec{S}_\varphi - \vec{m}_S\right)^T P_S^{-1}\left(\vec{S}_\varphi - \vec{m}_S\right)$, from which, using standard operations, one can obtain a solution to equation (10) in the form:

$$\vec{S}_\varphi^* = \left(A^T\Sigma^{-1}A + P_S\right)^{-1}\left(A^T\Sigma^{-1}\vec{D}_N + P_S^{-1}\vec{m}_S\right). \quad (11)$$

Thus, the solution of equation (11) makes it possible to evaluate the parameters of the model of interaction of the passive QSF in the process of their comparisons or application in a group standard.

Conclusions

Based on the results of the analysis of the influence of various external destabilizing factors (ambient temperature, the impact of other QSF) on the characteristics of the output signals of the QSF and methods for their compensation, the following main tasks of further research can be formulated:

1. To develop a method for identifying stochastic processes caused by the error from the interaction of the QSF in a group on the basis of a stochastic model of coupled oscillators, and to develop a method for measuring quantum noise by methods of group standardization.

2. To conduct a study of the behavior of the resonant frequency of a quantum discriminator in a nonstationary fluctuating temperature field of a thermostat and develop a method for compensating for fluctuations in the frequency of a signal generated by a passive QSF caused by fluctuations in the temperature of a thermostat.

3. To develop a method for identifying hidden quasiperiodic processes in the QSF signal using the Fredholm integral equation of the first kind, which connects the noise variance and the power spectral density of phase fluctuations of the output signal containing quasi-harmonic components with non-multiple frequencies.

4. To develop a method for compensating for regular quasiperiodic frequency deviations formed by a group standard based on an identification model of a system of coupled oscillators.

Fundamental experiments in the field of quantum noise in quantum parallel-type random number generators are impossible without precision measurement of time. Therefore, as a promising direction for further research, it is proposed to use the method of identifying a group of quantum standards by a model of a system of coupled oscillators for measuring quantum noise in quantum parallel-type random number generators.

References:

1. Gorbenko, I.D. and Gorbenko, Yu.I., (2012). Applied cryptology. Theory. Practice. Application, Kharkiv, Ukraine: Fort. 878 p. (in Ukraine).
2. Hofmann-Wellenhof B., Lichtenegger H., & Wasle E. (2008). GNSS-Global Navigation Satellite Systems GPS, GLONASS, Galileo and more. Vienna: Springer-Velag Wien. 546 p.
3. Peter J.G. Teunissen and O. Montenbruck, (Eds.), Springer Handbook of Global Navigation Satellite Systems, Springer International Publishing, Cham, p. 1335, 2017.
4. Oduan K. Measurement of time. Basics of GPS / Oduan K., Gino B.; Transl. from English. Moscow : Tekhnosfera, 2002. 400 p. (In Russian).
5. Riley, F., (2009) Frequency Standards: Principles and Applications. Moscow : Fizmatlit, 511 p. (in Russian).
6. Audoin C., Guinot B. (2000). The Measurement of Time, Time, Frequency and the Atomic Clock. 346 p. Cambridge University Press.

7. Schmittberger, B.L., & Scherer, D.R. (2020). A Review of Contemporary Atomic Frequency Standards. *arXiv: Atomic Physics*. 18 p.

8. Riley W. J. Handbook of frequency stability analysis. NIST Special Publication 1065. NIST, 2008. 136 pp.

9. M. Hirano, K. Hashimoto, F. Nakagawa, T. Ido, Y. Hanado, and S. Adachi. State estimation for multiple clocks under anomalies using l_1-norm optimization // Metrologia, vol. 56, no. 2, pp. 1-9, Mar. 2019.

10. C. Zucca and P. Tavella. A mathematical model for the atomic clock error in case of jumps // Metrologia, vol. 52, no. 4, pp. 514-521, June 2015.

11. Panfilo G., Harmegnies A., Tisserand L. A new weighting procedure for UTC // Metrologia, 2014, 51(3), p. 285-292.

12. C. Zucca, P. Tavella (2015). A mathematical model for the atomic clock error in case of jumps. Metrologia. 52. doi: 10.1088/0026-1394/52/4/514.

13. C. Zucca, P. Tavella and G. Peskir (2016). Detecting atomic clock frequency trends using an optimal stopping method // Metrologia. 53. S89-S95. doi: 10.1088/0026-1394/53/3/S89.

14. Trainotti, Christian, Giorgi, Gabriele. Detection and Identification of Phase and Frequency Drifts in Clock Ensembles // Proceedings of the 51st Annual Precise Time and Time Interval Systems and Applications Meeting, San Diego, California, January 2020, pp. 347-365. https://doi.org/10.33012/2020.17310

15. L. Galleani and P. Tavella. Detection and identification of atomic clock anomalies // Metrologia, vol. 45, no. 6, pp. S127-S133, Dec. 2008.

16. W. J. Riley. Algorithms for frequency jump detection // Metrologia, vol. 45, no. 6, pp. S154-S161, Dec. 2008.

17. O. P. Nariezhnii, V. V. Semenets, T. O. Grinenko Method for measuring quantum phase noise and line width of working transition of radio-optical system of random number generator // Telecommunications and Radio Engineering, Volume 77, 2018, Issue 19, pp. 1697-1717. DOI: 10.1615/TelecomRadEng.v77.i19.30

18. Narezhniy A.P. (2005) Identification of latent periodicity in non-stationary phase fluctuations of precision frequency measures // Applied Electronics, 4(2), pp. 148-152 (in Russian).

19. Marple S. L. Digital spectral analysis and its applications. Moscow : Mir, 1990. 584 p. (In Russian).

20. Ivanov V.K. On linear ill-posed problems // DAN USSR, 1962, v. 145, № 2, p. 270 (In Russian).

21. Ivanov V.K. About incorrectly posed tasks // Matematicheskiy sbornik, 1963, v.61, №2, p.211. (In Russian).

22. Ivanov V.K., Vasin V.V., Tanana V.P. The theory of linear ill-posed problems and its applications. Moscow : Nauka Gl. red. fiz.-mat. lit., 1978. 208 p. (In Russian).

23. Lavrent'ev M.M., Romanov V. G., Shishatsky S. P. Incorrect tasks of mathematical physics and analysis. Moscow : Nauka Gl. red. fiz.-mat. lit., 1980. 288 p. (In Russian).

24. Machenov A. S. Solution of linear integral equations of the first kind by the regularization method. Algorithms and programs // VNTICenter, 1975, № 3, p.42 (In Russian).

25. Verlan A. F. Integral equations: Methods, algorithms, programs. Reference book / A. F. Verlan, V. S. Sizikov. K. : Naukova Dumka, 1986. 544 p. (In Russian).

26. Polianin A. D. Handbook of integral equations / Andrei D. Polyanin and Alexander V. Manzhirov. 2nd ed. 2008, 1143 p.

27. Tikhonov A. N. Methods for solving ill-posed problems / A. N. Tikhonov, V. Ya. Arsenin. Moscow : Nauka, 1974. 224 p. (In Russian).

28. Tikhonov A. N. On the solution of ill-posed problems and the method of regularization. – DAN USSR. – 1963. V. 151. № 3. (In Russian).

29. Lavrentiev M. M. Conditionally well-posed problems for differential equations. Novosibirsk : Izd.-vo NGU, 1973. 224 p. (In Russian).

30. Ivanov V. K., Vasin V. V., Tanana V. P. The theory of linear ill-posed problems and its applications. Moscow : Nauka, 1978. (In Russian).

31. Anikonov Yu. E. Some research methods for multidimensional inverse problems for differential equations. Novosibirsk : Nauka, 1978. (In Russian).

32. Lavrentiev M. M., Vasiliev V. G. On the formulation of some ill-posed problems in mathematical physics // Sib. mat. zh., vol. 7, № 3, 1960. (In Russian).

33. Lyons J., Lattes R. Method of quasi-inversion and its application. Transl. from French. V. O. Sergeeva and V. L. Tsetsokho ; Ed. By M. M. Lavrentiev. Moscow : Mir, 1970. 336 p. (In Russian).

34. Marchuk G. I., Atanbaev S. A. Some questions of global regularization // DAN USSR. 1970. V. 190. № 3. (In Russian).

35. Ljung L. Systems identification. Theory for the user ; Transl. from English. A. S. Mandel et al. ; Ed. By Ya. Z. Tsypkina. Moscow : Nauka Gl. red. fiz.-mat. lit., 1991. 432 p. (In Russian).

Надійшла до редколегії 09.09.2021

Відомості про авторів:

Нарєжній Олексій Павлович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна; e-mail: o.nariezhnii@karazin.ua; ORCID: https://orcid.org/0000-0003-4321-0510

Гриненко Тетяна Олексіївна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Україна; e-mail: tetiana.grinenko@nure.ua

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ «Інститут інформаційних технологій», головний конструктор; Україна; e-mail: GorbenkoI@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-4616-3449

УДК 004.056.5 **DOI:10.30837/rt.2021.3.206.04**

Ю.І. ГОРБЕНКО, д-р техн. наук, О.Г. КАЧКО, канд. техн. наук, С.О. КАНДІЙ

ДОСЛІДЖЕННЯ ДОЦІЛЬНОСТІ ЗАСТОСУВАННЯ AVX512 ДЛЯ РЕАЛІЗАЦІЇ СУЧАСНИХ АЛГОРИТМІВ ЕЛЕКТРОННИХ ПІДПИСІВ

Вступ

Постквантова криптографія є напрямом досліджень, що вивчає криптографічні перетворення, які захищені від атак з використанням квантових комп'ютерів. У 2016 р. NIST США оголосили про початок конкурсу NIST PQC, метою якого є створення нових постквантових криптографічних стандартів. Наразі триває третій фінальний етап цього конкурсу. Згідно з аналізом спеціалістів NIST [8], одним з перспективних напрямів у постквантовій криптографії є криптографія на алгебраїчних решітках. У звіті [7] зазначається , що NIST планує стандартизувати хоча б один електронний підпис (ЕП) на решітках. Серед електронних підписів фіналістами , які є представниками криптографії на решітках, є CRYSTALS-Dilithium [2] та Falcon[3].

Сучасні ЕП на решітках потребують ефективних обчислень у поліноміальних кільцях вигляду $R_q = \mathbf{Z}_q[X]/(f(X))$, де $f(X)$ – деякий незвідний поліном. Під час генерації ключової пари, вироблення та верифікації підпису основними операціями є складання та множення поліномів. Складання поліномів потребує лінійну кількість обчислень і працює достатньо швидко. Множення поліномів «шкільним» методом потребує квадратичну кількість операцій, що робить реалізації неефективними. Тому для ефективної реалізації операції множення часто використовується теоретико-числове перетворення (NTT) [4]. Для підвищення швидкодії на сучасних процесорах можливо використовувати векторизовані (SIMD) набори інструкцій. Серед існуючих реалізацій найчастіше використовуються AVX2 інструкції [2 – 4]. У той же час можливість використання AVX512 інструкцій залишається малодослідженою.

Мета роботи – дослідження доцільності використання AVX512 інструкцій для оптимізації FFT і NTT, що використовуються у сучасних ЕП на алгебраїчних решітках. Зокрема, в роботі наведений метод реалізації теоретико-числового перетворення з використанням AVX512 для ЕП CRYSTALS-Dilithium та Falcon. Показано збільшення швидкодії порівняно з еталонними оптимізованими авторськими реалізаціями.

Особливості реалізації теоретико-числового перетворення

У переважної більшості ЕП на решітках [1 – 3] використовується циклотомічне кільце $R_q = \mathbf{Z}_q[X]/(X^n+1)$. Якщо $q \equiv 1 (\mathrm{mod}\, 2n)$, то $\mathbf{Z}_q$ містить n примітивних $2n$-х коренів з одиниці. У цьому випадку R_q є полем розкладу полінома X^n+1 і, відповідно до китайської теореми про залишки, має місце гомоморфізм:

$$f \mapsto (f(\xi), f(\xi^3), ..., f(\xi^{2n-1})) : \mathbf{Z}_q[X]/(X^n+1) \to \prod_i \mathbf{Z}_q[X]/(X-\xi^i), \quad (1)$$

Для описаного випадку цей гомоморфізм є ізоморфізмом [4]. Теоретико-числове перетворення полягає у обчисленні цього ізоморфізму. Операція множення поліномів замінюється на покомпонентне множення векторів над полем $\mathbf{Z}_q$. Відповідно повна операція множення поліномів матиме наступний вигляд:

$$f * g = NTT^{-1}(NTT(f) * NTT(g)), \quad (2)$$

NTT можливо обчислити за $O(n \log n)$ операцій за допомогою алгоритму швидкого теоретико-числового перетворення [4] (рис. 1).

Вхідні данні:

Поліном $f = c_0 + c_1 X \dots c_{n-1} X^{n-1} \in \mathbb{Z}_q[X]/(X^n + 1)$

Примітивні корені з одиниці: $\zeta_k \quad 0 \le k < n.$

Алгоритм 1. Швидке теоретико-числове перетворення

$k \leftarrow 1$
for $l \leftarrow n/2; l > 0; l \leftarrow l/2$ **do**
  for $s \leftarrow 0; s < n; s \leftarrow j + l$ **do**
    for $j \leftarrow s; j < s + l; j \leftarrow j + 1$ **do**
      $t \leftarrow \zeta_k \cdot c_{j+l}$
      $c_{j+l} \leftarrow c_j - t$
      $c_j \leftarrow c_j + t$
    end for
    $k \leftarrow k + 1$
  end for
end for

Алгоритм 2. Зворотне швидке теоретико-числове перетворення

$k \leftarrow 0$
for $l \leftarrow 1; l < n; l \leftarrow 2l$ **do**
  for $s \leftarrow 0; s < n; s \leftarrow j + l$ **do**
    for $j \leftarrow s; j < s + l; j \leftarrow j + 1$ **do**
      $t \leftarrow c_j$
      $c_j \leftarrow t + c_{j+l}$
      $c_{j+l} \leftarrow t - c_{j+l}$
      $c_{j+l} \leftarrow \zeta_k \cdot c_{j+l}$
    end for
    $k \leftarrow k + 1$
  end for
end for
for $j \leftarrow 0; j < n; j \leftarrow j + 1$ **do**
  $c_j \leftarrow c_j / n$
end for

Рис. 1. Алгоритм швидкого теоретико-числового перетворення

Алгоритми на кожній ітерації обчислюють відображення

$$\begin{aligned} & f \mapsto (f \bmod X^{n/2} - \xi^{n/2},\ f \bmod X^{n/2} + \xi^{n/2}) \\ & \mathbf{Z}_q[X]/(X^n - \xi^n) \to \mathbf{Z}_q[X]/(X^{n/2} - \xi^{n/2}) \times \mathbf{Z}_q[X]/(X^{n/2} + \xi^{n/2}) \end{aligned}, \tag{3}$$

При цьому коефіцієнти відповідних поліномів на кожній ітерації обчислюються як

$$\begin{aligned} c'_i &= c_i + \xi^{n/2} c_{n/2+i} \\ c''_i &= c_i - \xi^{n/2} c_{n/2+i} \end{aligned}, \tag{4}$$

Через N ітерацій відображення (3) буде тотожне (1).

Фіналісти третього етапу NIST PQC використовують модифіковані алгоритми обчислення NTT. Від обраних розробниками модифікацій залежать тестові вектори, тож при реалізації схеми необхідно враховувати ці зміни. Розглянемо детальніше особливості реалізації NTT для ЕП CRYSTALS-Dilithium [2] та Falcon [3].

Особливості NTT для ЕП Dilithium

Через те, що коефіцієнти поліномів лежать у кільці $\mathbf{Z}_q$, під час обчислень в стандартній реалізації відбувається багато приведень за модулем q. Ця операція є дорогою. Щоб зменшити кількість її використань при множенні коефіцієнтів автори використовують редукцію

Монтгомері, яка залежить від фактора r і дозволяє швидко обчислювати вирази виду $a * b * r^{-1} \bmod q$. Автори використовують $r = 2^{32}$. На фазі передобчислень всі примітивні корені з одиниці заносяться до масиву. Кожен корень помножується на фактор $2^{-32} \bmod q$. Відповідно після NTT перетворення коефіцієнти поліному будуть помножені на цей фактор. Під час покомпонентного множення цей фактор зникає.

Іншою оптимізацією є використання лінивої редукції. В стандартній реалізації після кожного складання коефіцієнтів під час перетворення NTT також необхідно приводити за модулем q, як і у випадку множення коефіцієнтів. Редукцію Монтгомері тут застосувати неможливо. Проте лінива редукція дозволяє уникнути важких операцій приведення за модулем. Оскільки під час складань значення зростає доволі повільно, то коефіцієнти можна не приводити за модулем у кожній ітерації, а приводити лише в кінці.

На кожній ітерації фактично масив можливо розглядати як сукупність блоків. Ілюстрація такого представлення наведена на рис. 2.

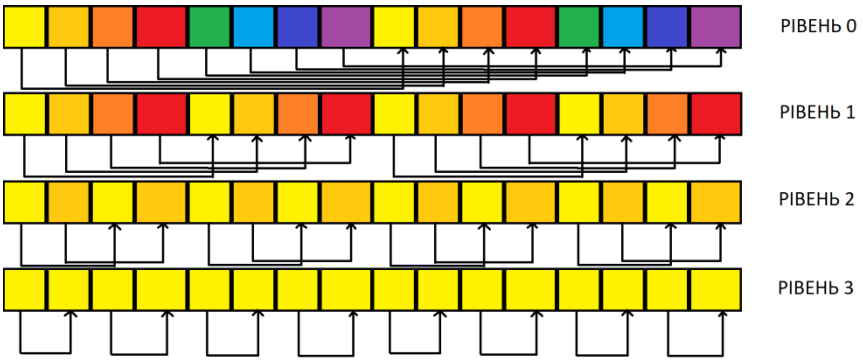


Рис. 2. Представлення взаємодії коефіцієнтів поліномів як взаємодії блоків. Кожен рівень є ітерацією алгоритму швидкого NTT

При обробці кожен блок взаємодіє лише з одним іншим блоком, що знаходиться справа. Відповідно буде 2,4,8,16,32,64,128,256 блоків розміру 128,64,32,16,8,4,2,1 елементів на відповідних ітераціях. З врахуванням всіх покращень перетворення (4) матиме вигляд:

```
t = montgomery_reduce((uint64_t)zeta * c[j + len]);
c[j + len] =( c[j] + 2*Q – t);
c[j] = (c[j] + t);
```

де len – розмір поточного блоку, zeta – примітивний корінь, c – масив з коефіцієнтами поліному.

При використанні AVX512 на перших ітераціях розмір блоків занадто великий, щоб їх повністю розмістити в регістрах zmm. Відповідно, стратегія обчислень буде відрізнятися. Кожен коефіцієнт зберігається в 32-бітній змінній. Проте через використання лінивої редукції з кожною ітерацією значення буде швидко зростати і для зберігання проміжкових даних необхідно 64 біти. Тобто, один регістр zmm може зберігати 8 коефіцієнтів. Припустимо, що у регістрах zmm0=left_block0, zmm1= left_block1, zmm2= left_block2, zmm3=left_block3 зберігаються відповідні значення c[j], а в zmm4=right_block0,zmm5= right_block1,zmm6= right_block2,zmm7= right_block3 відповідні значення c[j + len]. Значення відповідних примітивних коренів відповідно у регістрах zmm8=zeta0,zmm9=zeta1,zmm10=zeta2,zmm11=zeta3 і константа 2Q у регістрі zmm9. Тоді операцію (4) з врахуванням лінивої редукції та редукції Монтгомері можливо реалізувати наступним чином:

- Обчислюємо zeta * c[j + len]);
  right_block0 = _mm512_mul_epu32(right_block0, zeta0);
  right_block1 = _mm512_mul_epu32(right_block1, zeta1);

right_block2 = _mm512_mul_epu32(right_block2, zeta2);
right_block3 = _mm512_mul_epu32(right_block3, zeta3);

- Обчислюємо t = montgomery_reduce((uint64_t)zeta * c[j + len]);

zmm12 = _mm512_mul_epu32(right_block0, q-1);
zmm13 = _mm512_mul_epu32(right_block1, q-1);
zmm14 = _mm512_mul_epu32(right_block2, q-1);
zmm15 = _mm512_mul_epu32(right_block3, q-1);
zmm12 = _mm512_mul_epu32(zmm12, q);
zmm13 = _mm512_mul_epu32(zmm13, q);
zmm14 = _mm512_mul_epu32(zmm14, q);
zmm15 = _mm512_mul_epu32(zmm15, q);
zmm12 = _mm512_add_epi64(zmm12, right_block0);
zmm13 = _mm512_add_epi64(zmm13, right_block1);
zmm14 = _mm512_add_epi64(zmm14, right_block2);
zmm15 = _mm512_add_epi64(zmm15, right_block3);
zmm12 = _mm512_srli_epi64(zmm12, 32);
zmm13 = _mm512_srli_epi64(zmm13, 32);
zmm14 = _mm512_srli_epi64(zmm14, 32);
zmm15 = _mm512_srli_epi64(zmm15, 32);

- Обчислюємо c[j + len] =(c[j] + 2*Q – t);

right_block0= _mm512_add_epi32(left_block0, 2q);
right_block1= _mm512_add_epi32(left_block1, 2q);
right_block2= _mm512_add_epi32(left_block2, 2q);
right_block3= _mm512_add_epi32(left_block3, 2q);
right_block0= _mm512_sub_epi32(right_block0, zmm12);
right_block1= _mm512_sub_epi32(right_block1, zmm13);
right_block2= _mm512_sub_epi32(right_block2, zmm14);
right_block3= _mm512_sub_epi32(right_block3, zmm15);

- Обчислюємо c[j] = (c[j] + t);

left_block0 = _mm512_add_epi32(left_block0, zmm12);
left_block1 = _mm512_add_epi32(left_block1, zmm13);
left_block2 = _mm512_add_epi32(left_block2, zmm14);
left_block3 = _mm512_add_epi32(left_block3, zmm15);

На ітераціях, де розмір блоку є занадто великим для зберігання в регістрах можливо цю операцію викликати декілька разів для покриття повного розміру блоку.

Особливості NTT для ЕП Falcon

У ЕП Falcon реалізація перетворення NTT значно відрізняється від CRYSTALS-Dilithium. Значні зміни відбуваються через новаторський підхід при вирішенні NTRU рівняння. При пошуку рішення на кожному кроці обчислюється проекція поліному за допомогою норми на полі у деяке менше підполе. При цьому коефіцієнти поліному значно зростають, що призводить до необхідності використання довгої арифметики. Автори використовують систему залишкових класів для вирішення цієї проблеми [3]. Реалізація перетворення (4) приймає вигляд

```
uint32_t x, y;

x = *r1;
y = *r2;
*r1 = modp_add(x, y, p);
*r2 = modp_montymul(
        modp_sub(x, y, p), s, p, p0i);
```

де r1,r2 є вказівниками на відповідні елементи в блоках; p – одне з простих чисел, що використовується у системі залишкових класів у якості модуля; p0i – зворотнє до числа p.

При цьому вказівники r1, r1 змінюються з деяким кроком в залежності від підполя, в якому відбуваються перетворення. Це ускладнює використання векторизованих інструкцій так як данні неможливо зчитати одним блоком. Тож, для використання векторизованих інструкцій необхідно спочатку перегрупувати данні в залежності від підполя. Після перегрупування можливо застосувати такий же підхід, як і у випадку CRYSTALS-Dilithium. При цьому операцію складання за модулем можливо реалізувати як

```
static inline __m512i modp_add_avx512(__m512i a,__m512i b,__m512i p){
  __m512i tmp1,tmp2;

  tmp1 = _mm512_add_epi32(a,b);
  tmp1 = _mm512_sub_epi32(tmp1,p);
  tmp2 = _mm512_srli_epi32(tmp1,31);
  tmp2 = _mm512_sub_epi32(_mm256_set1_epi32(0),tmp2);
  tmp2 = _mm512_and_si256(tmp2,p);
  tmp1 = _mm512_add_epi64(tmp1,tmp2);
  return tmp1;
}
```

Операцію віднімання відповідно

```
static inline __m512i modp_sub_avx512(__m512i a,__m512i b,__m512i p){
  __m512i tmp1,tmp2;

  tmp1 = _mm512_sub_epi32(a,b);
  tmp2 = _mm512_srli_epi32(tmp1,31);
  tmp2 = _mm512_sub_epi32(_mm256_set1_epi32(0),tmp2);
   tmp2 = _mm512_and_si256(tmp2,p);
  tmp1 = _mm512_add_epi64(tmp1,tmp2);
  return tmp1;
}
```

І редукцію Монтгомері як

```
static inline __m512i modp_montymul_avx512(__m512i a,__m512i b,
                  __m512i p,__m512i p0i){
  __m512i tmp1,tmp2,tmp3;
  __m512i mask = _mm512_set1_epi64x(0x7FFFFFFF);

  tmp1 =_mm512_mul_epu32(a,b);
  tmp2 =_mm512_mul_epu32(tmp1,p0i);
  tmp2 =_mm512_and_si256(tmp2,mask);
  tmp2 =_mm512_mul_epu32(tmp2,p);

  tmp1 = _mm512_add_epi64(tmp1,tmp2);
  tmp1 = _mm512_srli_epi64(tmp1,31);
  tmp1 = _mm512_sub_epi32(tmp1,p);
  tmp2 = _mm512_srli_epi64(tmp1,31);
  tmp2 = _mm512_sub_epi32(_mm256_set1_epi32(0),tmp2);
  tmp2 = _mm512_and_si512(tmp2,p);
  tmp1 = _mm512_add_epi64(tmp1,tmp2);
  return tmp1;
}
```

В порівнянні з CRYSTLAS-Dilithium, реалізація NTT є складнішою і потребує більшої кількості ресурсів.

Множення в спектральній області з використанням AVX512

Множення в спектральній області, відповідно до формул (2) та (3), відбувається покомпонентно. Розглянемо загальну ситуацію, де потрібно знайти значення виразу

$$a_1 * b_1 + ... + a_l * b_l, \tag{5}$$

де $a_1, ..., a_l, b_1, ..., b_l$ є поліноми у NTT, що представлені (в спектральній області).

Щоб не використовувати дорогу операцію приведення за модулем, скористаємося редукцією Монтгомері: кожен елемент помножимо на фактор 2^{32} і виконаємо операцію редукції у кінці. Тож, для обчислення виразу (5) виконаємо наступні кроки:

- Оскільки вираз (5) є сумою, то необхідні регістри, що слугуватимуть у ролі акумулятора. Відведемо під цю роль регістри zmm2-zmm9.
- Нехай a та b є вказівниками типу _m512i на відповідні представлення поліномів в пам'яті. Зчитаємо з пам'яті поточний блок

```
zmm10 = _mm512_load_si512(a);
    zmm12 = _mm512_load_si512(a + 1);
    zmm14 = _mm512_load_si512(a + 2);
    zmm16 = _mm512_load_si512(a + 3);
    zmm18 = _mm512_load_si512(b);
    zmm20 = _mm512_load_si512(b + 1);
    zmm22 = _mm512_load_si512(b + 2);
zmm24 = _mm512_load_si512(b + 3);
```

- Помножимо на фактор 2^{32} :

```
    zmm11 = _mm512_srli_epi64(zmm10, 32);
    zmm13 = _mm512_srli_epi64(zmm12, 32);
    zmm15 = _mm512_srli_epi64(zmm14, 32);
    zmm17 = _mm512_srli_epi64(zmm16, 32);
    zmm19 = _mm512_srli_epi64(zmm18, 32);
    zmm21 = _mm512_srli_epi64(zmm20, 32);
    zmm23 = _mm512_srli_epi64(zmm22, 32);
zmm25 = _mm512_srli_epi64(zmm24, 32);
```

- Виконаємо по компонентне множення

```
zmm10 = _mm512_mul_epu32(zmm18, zmm10);
    zmm11 = _mm512_mul_epu32(zmm19, zmm11);
    zmm12= _mm512_mul_epu32(zmm20, zmm12);
    zmm13= _mm512_mul_epu32(zmm21, zmm13);
    zmm14 = _mm512_mul_epu32(zmm22, zmm14);
    zmm15 = _mm512_mul_epu32(zmm23, zmm15);
    zmm16 = _mm512_mul_epu32(zmm24, zmm16);
    zmm17 = _mm512_mul_epu32(zmm25, zmm17);
```

- Запишемо результати до обраних акумуляторів

```
    zmm2 = _mm512_add_epi64(zmm2, zmm10);
zmm3 = _mm512_add_epi64(zmm3, zmm11);
zmm4 = _mm512_add_epi64(zmm4, zmm12);
zmm5 = _mm512_add_epi64(zmm5, zmm13);
zmm6 = _mm512_add_epi64(zmm6, zmm14);
zmm7 = _mm512_add_epi64(zmm7, zmm15);
zmm8 = _mm512_add_epi64(zmm8, zmm16);
zmm9 = _mm512_add_epi64(zmm9, zmm17);
```

- На останньому кроці виконаємо редукцію Монтгомері над акумуляторами (в регістрах zmm0,zmm1 містяться відповідні константи для редукції.

```
zmm10 = _mm512_mul_epu32(zmm2, zmm0);
zmm11 = _mm512_mul_epu32(zmm3, zmm0);
zmm12 = _mm512_mul_epu32(zmm4, zmm0);
zmm13 = _mm512_mul_epu32(zmm5, zmm0);
zmm14 = _mm512_mul_epu32(zmm6, zmm0);
zmm15 = _mm512_mul_epu32(zmm7, zmm0);
zmm16 = _mm512_mul_epu32(zmm8, zmm0);
zmm17 = _mm512_mul_epu32(zmm9, zmm0);
zmm10 = _mm512_mul_epu32(zmm10, zmm1);
zmm11 = _mm512_mul_epu32(zmm11, zmm1);
zmm12 = _mm512_mul_epu32(zmm12, zmm1);
zmm13 = _mm512_mul_epu32(zmm13, zmm1);
zmm14 = _mm512_mul_epu32(zmm14, zmm1);
zmm15 = _mm512_mul_epu32(zmm15, zmm1);
zmm16 = _mm512_mul_epu32(zmm16, zmm1);
zmm17 = _mm512_mul_epu32(zmm17, zmm1);
zmm2 = _mm512_add_epi64(zmm10, zmm2);
zmm3 = _mm512_add_epi64(zmm11, zmm3);
zmm4 = _mm512_add_epi64(zmm12, zmm4);
zmm5 = _mm512_add_epi64(zmm13, zmm5);
zmm6 = _mm512_add_epi64(zmm14, zmm6);
zmm7 = _mm512_add_epi64(zmm15, zmm7);
zmm8 = _mm512_add_epi64(zmm16, zmm8);
zmm9 = _mm512_add_epi64(zmm17, zmm9);
zmm2 = _mm512_srli_epi64(zmm2, 32);
zmm4 = _mm512_srli_epi64(zmm4, 32);
zmm6 = _mm512_srli_epi64(zmm6, 32);
zmm8 = _mm512_srli_epi64(zmm8, 32);
```

Швидкодія реалізації NTT з використанням AVX512

Результати реалізації [5] наведено в таблиці для процесору Intel (R) Core (TM) i 9-7960X CPU @ 2.80GHz, 2808 MHz cores, 16 logical processors: 32. Компиляторы: Microsoft Visual Studio Community 2019, Version 16.6.2, VisualStudio.16.Release / 16.6.2 + 30204.135, / o2 optimization flags GCC 9.3, флаги оптимізації: -O3 –march=native,-mtune=native

Таблиця 1

Швидкодія теоретико-числового перетворення

	Linux, Dilithium (lang asm, GCC)	Linux(lang C, GCC)	Windows 10, (lang C, msvc)	Speedup Linux	Speedup Windows
ntt	987	663	727	1.48	1.35
Покомпонентне множення	135	81	87	1.6	1.51
Зворотнє ntt	972	677	741	1.43	1.31

В таблиці наведено результати виміру кількості тактів для кожної функції. Для виміру кількості тактів застосовувалась команда процесора rdtsc або відповідна функція. В другій колонці таблиці наведені результати для авторської реалізації (розробники Dilithium), які отримані з застосуванням ключів компілятора GCC, які застосовували автори (Linux).

В третій колонці наведені результати нашої реалізації для тих же ключів компілятору GCC, які застосовувалися для отримання попередніх результатів (Linux). В четвертій колонці наведено результати нашої реалізації з застосуванням компілятору msvc В наступних колонках наведено прискорення для нашої реалізації по відношенню до авторської реалізації.

Висновки

Розроблено реалізацію теоретико-числового перетворення з використанням AVX512 для постквантових електронних підписів, що є фіналістами конкурсу NIST PQC. Показано, що використання AVX512 дозволяє отримати прискорення у 1,5 рази, порівняно з існуючими реалізаціями. Для схеми Falcon реалізація NTT має складнішу реалізацію, ніж для CRYSTALS-Dilithium.

Список літератури:

1. Gorhan Alagic Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner

2. Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler and Damien Stehlé CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation. – Access mode: https://pq-crystals.org/dilithium/data/dilithium-specification.pdf

3. Thomas Prest et Al. aFlcon: Fast-Fourier Lattice-basedCompact Signatures over NTRU – Access mode: https://falcon-sign.info/falcon.pdf

4. Gregor Seiler Faster AVX2 optimized NTT multiplication for Ring-LWE lattice cryptography – Access mode: https://crypto.ethz.ch/publications/files/Seiler18.pdf

5. AVX512 NTT implementation for Dilithium. Access mode: https://github.com/KandiyIIT/dilithium_ntt_avx512

6. Качко О.Г. Осика О.Ф. Використання SIMD команд для паралельних обчислень. Навчальний посібник з дисципліни Паралельне програмування. Харків : ХНУРЕ, 2020. 274 с.

7. NISTR 8309. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standartization Process. NIST, 2020. 39 p.

8. NIST Post-Quantum Cryptography Standartization Project : веб сайт. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization (дата звернення: 27.11.2020)

Надійшла до редколегії 13.09.2021

Відомості про авторів:

Горбенко Юрій Іванович – канд. техн. наук, АТ «інститут інформаційних технологій», перший заступник головного конструктора; Україна; e-mail: gorbenkou@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-0073-9107

Качко Олена Григорівна – канд. техн. наук, Харківський національний університет радіоелектроніки, професор кафедри програмної інженерії, факультет комп'ютерних наук; АТ «Інститут інформаційних технологій», начальник відділу програмування; Україна; e-mail: iit@iit.kharkov.ua, ORCID: https://orcid.org/0000-0001-9249-0497

Кандій Сергій Олегович – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; АТ «Інститут Інформаційних технологій», технік-конструктор; Україна; e-mail: sergeykandy@gmail.com; ORCID: https://orcid.org/0000-0003-0552-8341

УДК 004.056.5 **DOI:10.30837/rt.2021.3.206.05**

О.О. КУЗНЕЦОВ, д-р техн. наук, М.О ПОЛУЯНЕНКО, канд. техн. наук,
В.О. КАТРИЧ, д-р фіз.-мат. наук, С.О. КАНДІЙ, Ю.О. ЗАЙЧЕНКО

ДОСЛІДЖЕННЯ ЕВРИСТИЧНИХ ФУНКЦІЙ ПОШУКУ НЕЛІНІЙНИХ ПІДСТАНОВОК ДЛЯ СИМЕТРИЧНОЇ КРИПТОГРАФІЇ

Вступ

Для захисту важливої інформації зазвичай застосовуються різні технології, зокрема, механізми криптографічного перетворення [1, 2]. В основі багатьох симетричних криптоалгоритмів лежить застосування т. з. вузлів ускладнення (нелілійних таблиць заміни, S-блоків) [2 – 5]. Саме на криптографічних властивостях S-блоків базується стійкість більшості симетричних шифрів від різних криптоаналітичних атак (диференційного, лінійного, алгебраїчного та інших методів криптоаналізу) [6 – 9]. Отже аналіз нелінійних підстановок, вивчення методів їх генерації (пошуку) та дослідження криптографічних властивостей є актуальною та важливою науковою задачею.

Методи генерації вузлів заміни умовно поділяють на випадкові, алгебраїчні та евристичні [6, 10, 11].

Випадкові S-блоки забезпечують високі показники статистичної безпеки. Крім того, вони, як правило, дають захищеність від алгебраїчних методів криптоаналізу. Дійсно, якщо таблиця заміни сформована випадковим чином, тоді система алгебраїчних рівнянь, що аналітично описує підстановку, ймовірно буде надзвичайно складною. Експерименти показують, що це дійсно так. Але інші криптографічні показники випадкових S-блоків є не дуже високими. Наприклад, нелінійність (що є визначальним показником стійкості до лінійного криптоаналізу) випадкових S-блоків є значно нижчою, ніж у алгебраїчно сформованих таблиць заміни [12 – 14].

Алгебраїчні техніки формування S-блоків дозволяють отримати дуже високі показники нелінійності [9, 13, 15]. Наприклад, таблиця замін шифру AES сформована алгебраїчним способом і за нелінійністю є найвищою серед всіх відомих на сьогодні S-блоків [9]. Тобто шифр AES дійсно захищений від певних криптографічних атак. Але алгебраїчні таблиці мають дуже просту математичну конструкцію, через що шифр описується значно простішою системою алгебраїчних рівнянь [16 – 19]. Існує багато наукових робіт, присвячених цьому питанню. Фактично алгебраїчна простота S-блоку шифру AES призвела до появи нового методу алгебраїчного криптоаналізу [16]. Для забезпечення захищеності від таких атак застосовують показник алгебраїчної імунності і для S-блоку шифру AES цей показник не є високим [20].

Евристичні техніки генерації (пошуку) S-блоків зазвичай використовують випадково сформовані таблиці заміни і шляхом поступового ітераційного оновлення їх станів дозволяють значно покращити окремі криптографічні показники [14, 21 – 24]. Наприклад, за допомогою евристичних алгоритмів інформованого пошуку вдається значно підвищити нелінійність. Отже саме така генерація дозволяє досягти захищеності від більшості відомих атак: випадковість забезпечує високу алгебраїчну імунність, а евристичні техніки дозволяють покращити інші показники безпеки.

В цій роботі розглядаються евристичні техніки генерації вузлів заміни.

Для реалізації інформованого пошуку підходящого рішення в просторі можливих станів зазвичай застосовуються спеціальні евристичні функції (наприклад, у вигляді функції вартості) [25 – 27]. Евристична функція на кожному кроці на підставі додаткової інформації оцінює можливі альтернативи з метою прийняття рішення про те, в якому напрямку слід продовжувати пошук. При порівнянні можливих евристик мають значення ступінь інформованості (що визначається конкретною функцією вартості), а також складність обчислення кожної з евристик [25]. Більш поінформовані евристики дозволяють скоротити кількість вузлів пере-

борного пошуку, хоча платою за це можуть бути значні витрати часу на обчислення функції вартості для кожного вузла.

В роботі розглядається найбільш поширена версія функції вартості, що застосовується в більшості відомих евристичних алгоритмах генерації вузлів заміни. Метою дослідження є визначення конкретних параметрів евристичної функції, які з одного боку не знижують ступінь інформованості стосовно вузлів пошуку, а з іншого боку не вимагають значних обчислювальних витрат. Також надаються конкретні рекомендації з формування параметрів функції евристичного формування S-блоків.

Пов'язані роботи

Методи генерації криптографічних булевих функцій вивчалися в [10, 31, 37]. В роботах [6, 38] розглядаються векторні булеві функції для криптографічних застосувань. Зокрема, у [14, 23, 39 – 42] введено основні криптографічні показники S-блоків, вивчено їх властивості та досліджено різні техніки генерації.

Дослідженню евристичних методів пошуку нелінійних підстановок присвячено роботи [10, 11, 21, 34] та інші. Зокрема, у [28 – 30] досліджено інформований пошук локальних екстремумів, у роботах [14, 29, 31, 32] досліджено техніки градієнтного пошуку, роботи [12, 29, 33] присвячено алгоритмам імітації відпалу, в статтях [28, 34 – 36] розглянуто генетичні алгоритми і т.д.

Функції вартості досліджувалися в роботах [29, 33, 37, 39, 43] та ін. Зокрема, в [39, 43] досліджено алгоритми імітації відпалу, в [37] розглянуто метод «hill-climbing», в роботах [29, 33] досліджено різні функції вартості при їх застосуванні до різних технік евристичного пошуку.

В статті розглядаються та досліджуються найбільш поширені форми функції вартості з [39, 43] та досліджується вплив окремих показників на ефективність пошуку нелінійних вузлів заміни.

Вихідні дані та методика дослідження

В евристичному алгоритмі пошуку з використанням комбінаторної оптимізації користувач намагається вирішити проблему, створюючи або «розвиваючи» сутність певної форми [10, 11]. Спочатку користувач евристично визначає деяку цільову функцію («функцію вартості» або «функцію придатності»), яка приймає об'єкт, що еволюціонує, і видає скалярне значення. В алгоритмах, що використовують функції вартості, якісні рішення задач повинні відповідати низьким значенням цільової функції, а погані рішення – великим.

Метою комбінаторної оптимізації, до якої можна віднести ряд методів формування S-блоків зі заданими властивостями [29, 33, 44], завжди є мінімізація або максимізація певної цільової функції. Традиційно у алгоритмах імітації відпалу цільовою функцією називається функція вартості [39].

У 2000 р. було запропоновано нове сімейство функцій вартості, яке реалізувало суттєві покращення для випадку з одним виходом. Після значних експериментів ця функція вартості показала, що вона здатна створювати S-блоки з винятковими профілями критеріїв безпеки. Замість того, щоб засновувати вартість на екстремальних значеннях (згідно з визначенням нелінійності та автокореляції), вона визначила вартість у всьому спектрі Уолша – Адамара та спектрі автокореляції [39]. Деталі експериментів для окремого випадку випуску та детальна мотивація прийнятої функції вартості визначені у [43]. В цій статті застосовується та досліджується функція вартості у вигляді

$$WHS = \sum_{i=1}^{255} \left| \left| \max\left(WHT\right) \right| - X \right|^{R}, \qquad (1)$$

де X і R – дійсні параметри. У наявній літературі зазначається, що важко передбачити, якими повинні бути такі значення параметрів та з яких міркувань їх вибирати [29, 39, 43]. У цій

роботі досліджується поведінка функції вартості (1) та надаються відповідні рекомендації щодо вибору параметрів X і R.

Символ WHT (англ. Walsh – Hadamard transform) в (1) позначає спектральні коефіцієнти Уолша – Адамара. Типовий розподіл максимальних значень спектру коефіцієнтів Уолша – Адамара для окремої лінійної комбінації наведено на рис. 1 (тут і далі досліджуються бієктивні S-блоки із розміром входу-виходу 8*8).

У наведеному розподілі (рис. 1) максимальне є значення 68, середнє значення складає 49,2, а сума – 12 548. Якщо від всіх значень відняти 36, що буде відповідати параметру $X = 36$ з WHS, то гістограма набуде вигляду, який наведено на рис. 2. При цьому середнє значення буде складати 13,2, а сума – 3 368.

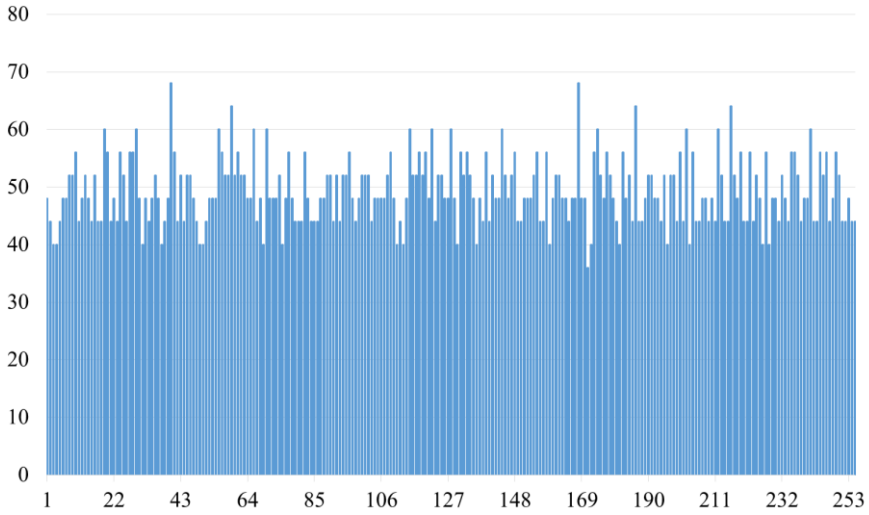


Рис. 1. Типовий розподіл максимальних значень спектру коефіцієнтів Уолша – Адамара для окремої лінійної комбінації

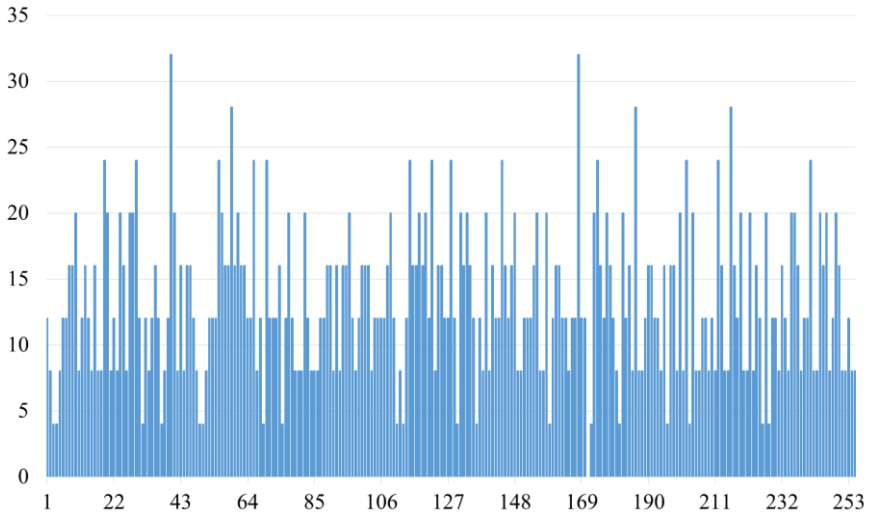


Рис. 2. Типовий розподіл максимальних значень спектру коефіцієнтів Уолша – Адамара для окремої лінійної комбінації з урахуванням параметру $X = 36$ з WHS

Максимальне значення спектру коефіцієнтів Уолша – Адамара ($\max(WHT)$) може приймати значення лише кратні чотирьом (детальніше це твердження розглянуто наприклад у [10, 11, 21]).

З метою експериментального встановлення розподілу, яке приймає WHS, було проведено серію окремих експериментів з різними вхідними параметрами X та R. Кожна серія складалась з 10^7 незалежних формувань випадковим чином S-блоку та встановлення його WHS.

Введемо наступні позначення:

- $f(WHS)$ – функція розподілу ймовірності значень WHS;
- $WHS^{\max}$ – значення функції розподілу ймовірності WHS при якому $f(WHS)$ приймає максимальне значення.

Окремо для кожної серії експериментів будемо підраховувати інтервал, до якого потрапляє 90 % найбільш значущих значень ймовірності $f(WHS)$. Величину значущості визначає $f(WHS)$. Інтервал підраховувався наступним чином:

1) до $f\left(WHS^{\max}\right)$ додавалося значення $f\left(WHS^{\max}+1\right)$ або $f\left(WHS^{\max}-1\right)$ в залежності від того, яке з них є більшим;
2) перевірялася сума;
3) якщо сума перевищувала 0,9, підрахунок вважалося завершеним, якщо ні – інтервал збільшувався на одиницю (в бік значення, яке було обрано в п.1) та процедура повторювалась знову.

Фіксувалась межа цього інтервалу:

- WHS^{-} – найменше значення функція розподілу ймовірності WHS, при якому $f(WHS)$ ще потрапляє до 90 % інтервалу найбільш значущих значень;
- WHS^{+} – найбільше значення функції розподілу ймовірності WHS, при якому $f(WHS)$ ще потрапляє до 90 % інтервалу найбільш значущих значень.

Метою цих досліджень є визначення впливу параметрів X і R на значення WHS та на ефективність евристичного пошуку.

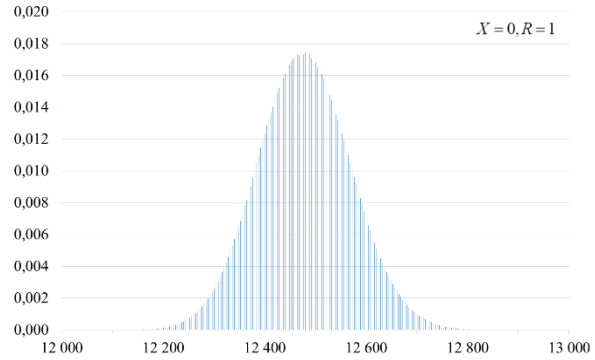
Отримані результати

Функції розподілу ймовірності значень WHS, які були отримані за результатами серії експериментів, наведено на рис. 3 – 7, у табл. 1 наведено основні показники, що характеризують функцію розподілу ймовірності та є вагомими.

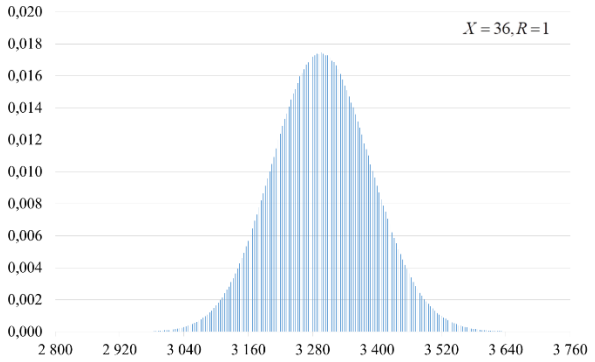
Таблиця 1

Результати дослідження WHS при різних параметрах R та X

R	X	$WHS^{\max}$	WHS^{-}	WHS^{+}	$f(WHS)$
1	0	12 480	12 324	12 632	рис. 3, *а*
1	22	6 862	6 714	7 022	
1	30	4 824	4 672	4 980	
1	35	3 548	3 396	3 704	
1	36	3 296	3 144	3 452	рис. 3, *б*
1	37	3 032	2 888	3 196	
1	38	2 784	2 636	2 944	
1	39	2 528	2 384	2 688	
1	40	2 280	2 132	2 436	
2	0	618 224	603 312	634 416	рис. 4, *а*
2	22	193 408	184 288	202 240	
2	36	50 880	46 144	55 808	рис. 4, *б*
3	0	31 144 000	29 896 000	32 352 000	рис. 5, *а*
3	22	5 664 000	5 216 000	6 112 000	
3	36	900 736	769 664	1 052 800	рис. 5, *б*
4	0	1 587 424 000	1 501 408 000	1 678 048 000	рис. 6, *а*
4	22	173 776 000	156 240 000	194 640 000	
4	36	17 735 680	14 110 720	22 917 120	рис. 6, *б*
5	0	81 184 000 000	75 616 000 000	87 552 000 000	рис. 7, *а*
5	22	5 587 200 000	4 800 000 000	6 547 200 000	
5	36	387 568 000	273 904 000	565 744 000	рис. 7, *б*

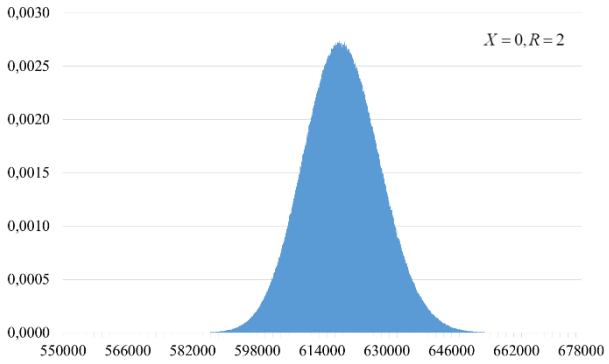


а

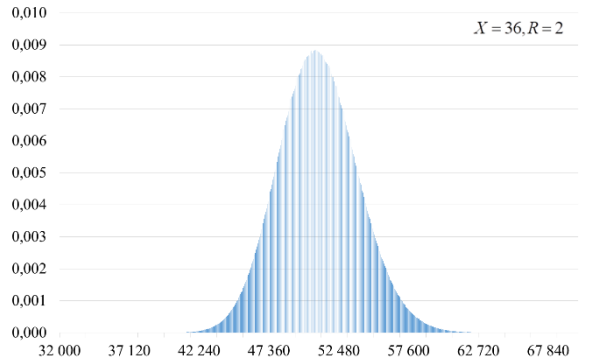


б

Рис. 3. Функція ймовірності розподілу значень цільової функції *WHS* при $R = 1$ та *а* – $X = 0$, *б* - $X = 36$

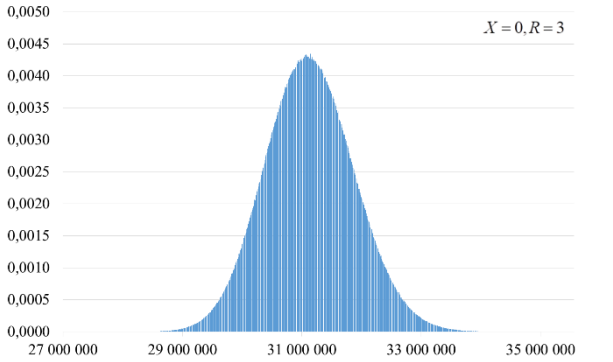


а

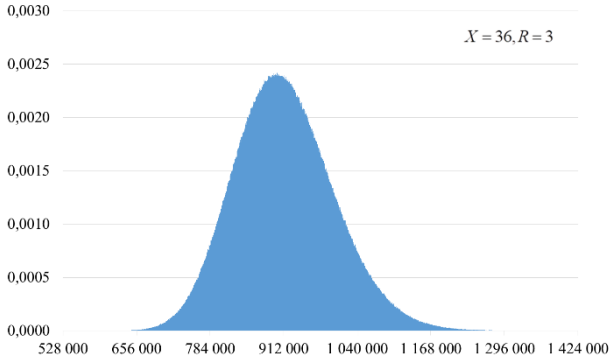


б

Рис. 4. Функція ймовірності розподілу значень цільової функції *WHS* при $R = 2$ та *а* – $X = 0$, *б* – $X = 36$

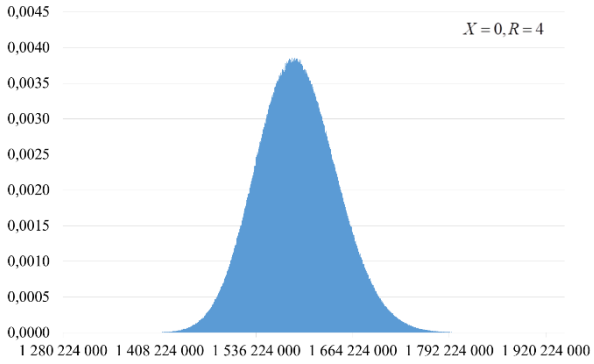


а

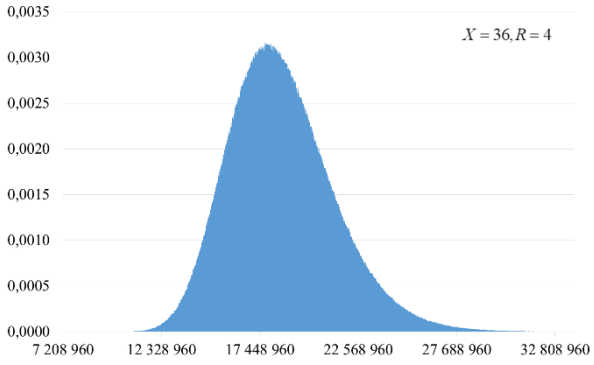


б

Рис. 5. Функція ймовірності розподілу значень цільової функції *WHS* при $R = 3$ та *а* – $X = 0$, *б* – $X = 36$



а



б

Рис. 6. Функція ймовірності розподілу значень цільової функції *WHS* при $R = 4$ та *а* – $X = 0$, *б* - $X = 36$

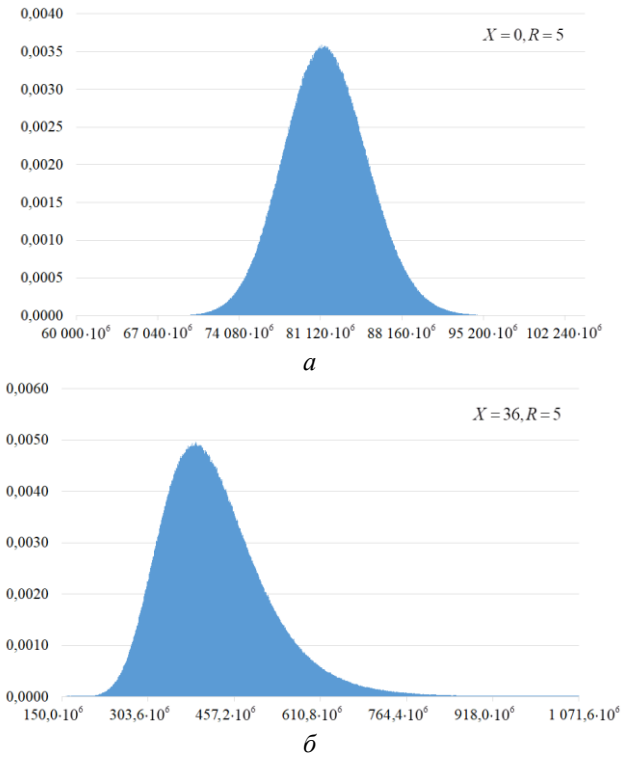


Рис. 7. Функція ймовірності розподілу значень цільової функції *WHS* при $R = 5$ та *а* – $X = 0$, *б* - $X = 36$

З наведених результатів бачимо, що параметри X та R суттєво не впливають на форму функцій ймовірності розподілу самих значень. З ростом параметра R спостерігається невелика асиметрія, що пояснюється зведенням до степеню. Параметри можна вважати коефіцієнтами масштабування функції ймовірності розподілу *WHS*. Параметр R значно впливає на ширину функцій ймовірності розподілу цільової функції.

Змінюючи параметр X, можна переміщувати функцію ймовірності розподілу *WHS* по осі абсцис. Змінюючи значення X на одну одиницю, при $R = 1$, змінюємо значення *WHS* на 255 відповідно.

Збільшення параметру X призводить до наближення значень, які додаються у виразі (1), до нуля. Тому є сенс збільшувати цей параметр, що приведе до зменшення самих значень цільової функції з занадто великих значень до прийнятних.

Однак, якщо взяти параметр X великим, то завдяки модулю у виразі, при менших максимальних значень спектру Уолша – Адамара, вираз (1) буде мати більше значення *WHS*. Отже, при мінімізації значення *WHS* можливо спостерігати результат протилежну очікуваному.

Пояснимо останнє твердження, тобто якщо збільшувати параметр X, то при підсумовуванні максимальних значень спектру Уолша – Адамара за всіма 255 лінійними комбінаціями деякі з них можуть стати меншими за параметр X, що приведе до від'ємних значень. Але, завдяки модулю, сума абсолютних значень буде зростати, а з ним буде зростати значення *WHS*. Таким чином, якщо шукається S-блок з максимальною нелінійністю, а сума максимальних значень спектру Уолша – Адамара за всіма 255 лінійними комбінаціями буде менше за аналогічною сумою деякого попередньо найденого S-блоку (що потенційно може свідчить про більш високу нелінійність), то при великих значеннях параметр X, значення *WHS* буде вищим, а отже це буде вважатися за гірше рішення.

В якості прикладу такої поведінки *WHS* можна навести її функції ймовірності розподілу при різних параметрах X. На рис. 8 наведено результати дослідження розподілу $f(WHS)$ при

$R=1$ та зміни X від 0 до 70. Кожна серія складалась з 10^7 незалежних формувань випадковим чином S-блоку та встановлення його WHS.

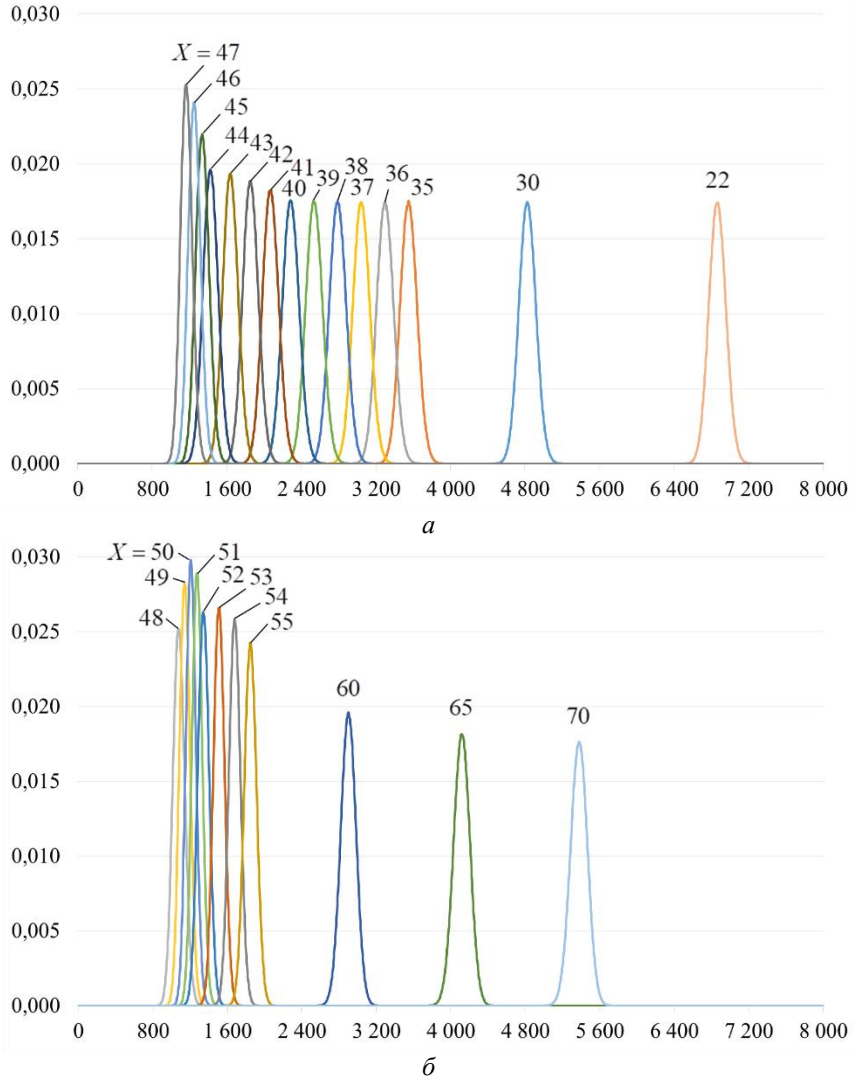


Рис. 8. $f(WHS)$ при $R=1$ та різних значеннях параметра X: *а* – $X=22-47$; *б* – $X=48-70$

Окремо, на рис. 9 наведено залежність $WHS^{\max}$ від параметру X, яку було встановлено при кожній серії. Пунктиром наведено розрахункове значення: $WHS^{\max}_{X=0}-255\cdot X$.

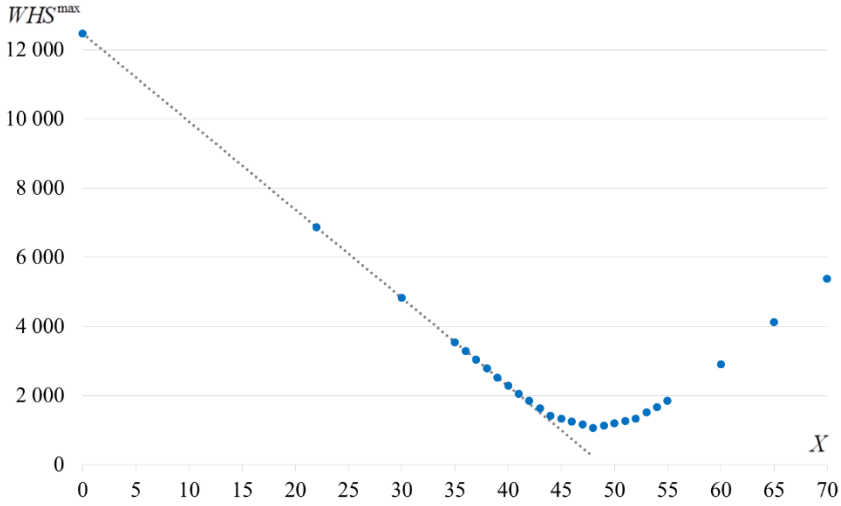


Рис. 9. $WHS^{\max}$ в залежності від параметру X при $R=1$

Значення WHS не знижується нижче деякого порогового значення (приблизно 1 000), яке відповідає сумі девіацій від середнього значення максимальних значень спектру Уолша – Адамара. Значне відхилення від розрахункового значення починається з порогового $X = 41$ (відхилення від розрахункового значення становить близько 2 %), а при $X = 44$ відхилення досягає 11,5 %, що свідчить о невідповідності поведінки WHS реальній картині та вже не може використовуватися в якості цільової функції. При застосуванні WHS на практиці є сенс його зменшення (без втрати адекватності відображення реальним значенням).

Зазначимо, що параметр R не впливає на величину знайденого порогового значення X, це випливає з безпосереднього аналізу виразу (1) для знаходження WHS. Порогове значення X зберігається при любих значеннях R.

При застосуванні на практиці величину $\left(WHS^{+} - WHS^{-}\right)$ є сенс збільшувати, що впливає на «чутливість» алгоритмів, які використовують WHS в якості цільових функції. Однак, при збільшенні параметру R значення WHS дуже швидко зростає та вже при $R = 5$ перевищує 32-бітне значення, що може негативно вплинути на швидкодію алгоритму та привести до небажаних помилок при застосуванні таких алгоритмів.

Висновки

Генерація нелінійних підстановок є важливим та актуальним напрямком пошукових досліджень, оскільки криптографічні параметри S-блоків безпосередньо впливають на стійкість симетричних шифрів до різних методів криптографічного аналізу (диференційного, лінійного, алгебраїчного та ін.). Найбільш перспективними вважаються евристичні техніки інформованого пошуку S-блоків, в яких застосовуються так звані функції вартості. Саме від властивостей цільових функцій та вибору їх окремих параметрів залежить ефективність евристичного пошуку, тобто конкретні обсяги часу та обчислювальних ресурсів, які витрачають для пошуку нелінійної підстановки із потрібними властивостями.

В роботі проаналізовано поведінку цільової функції (1), яка використовується в алгоритмах формуваннях S-блоків із заданими криптографічними властивостями (наприклад, локального пошуку, градієнтного підйому, імітації відпалу, генетичного пошуку, тощо). Також в роботі надано рекомендації з вибору параметрів зазначеної функції.

В якості оптимальних параметрів цільової функції (1) обрано:

- $X = 36$ як максимально допустиме значення, яке зменшує WHS, але не приводить до суттєвого впливу на її адекватний взаємозв'язок з нелінійністю S-блоку;
- $R = 4$ як максимально допустиме значення, яке збільшує діапазон можливих значень WHS, що може покращити «чутливість» алгоритмів формування S-блоків, які її використовують.

Зазначені параметри доцільно використовувати в різних алгоритмах евристичного пошуку. Це дозволить, на нашу думку, значно підвищити ефективність генерації нелінійних підстановок.

References:

1. Menezes A.J., Oorscho, P.C., van Vanstone S.A., Oorschot P.C. van, Vanstone S.A. Handbook of Applied Cryptography. CRC Press (2018). https://doi.org/10.1201/9780429466335.
2. Schneier B. Applied cryptography : protocols, algorithms, and source code in C. New York : Wiley (1996).
3. Technology N.I. of S. and: Advanced Encryption Standard (AES). U.S. Department of Commerce (2001). https://doi.org/10.6028/NIST.FIPS.197.
4. Kuznetsov A., Gorbenko Y., Andrushkevych A., Belozersev I. Analysis of block symmetric algorithms from international standard of lightweight cryptography ISO/IEC 29192-2 // 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). pp. 203–206 (2017). https://doi.org/10.1109/INFOCOMMST.2017.8246380.
5. Kuznetsov O., Potii O., Perepelitsyn A., Ivanenko D., Poluyanenko N. Lightweight Stream Ciphers for Green IT Engineering // Kharchenko V., Kondratenko Y., and Kacprzyk J. (eds.) Green IT Engineering: Social, Business and Industrial Applications. pp. 113–137. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-00253-4_6.

6. Álvarez-Cubero J. Vector Boolean Functions: applications in symmetric cryptography (2015). https://doi.org/10.13140/RG.2.2.12540.23685.

7. AlSalami Y., Martin T., Yeun C. Linear and Differential Properties of Randomly Generated DES-Like Substitution Boxes // Park, J.J. (Jong H., Stojmenovic I., Jeong H.Y., and Yi G. (eds.) Computer Science and its Applications. pp. 517–524. Springer, Berlin, Heidelberg (2015). https://doi.org/10.1007/978-3-662-45402-2_77.

8. Eastlake 3rd D., Schiller J., Crocker S. Randomness Requirements for Security. (2005).

9. Daemen J., Rijmen V. Specification of Rijndael // Daemen, J. and Rijmen, V. (eds.). The Design of Rijndael: The Advanced Encryption Standard (AES). pp. 31–51. Springer, Berlin, Heidelberg (2020). https://doi.org/10.1007/978-3-662-60769-5_3.

10. Burnett L.D. Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography, https://eprints.qut.edu.au/16023/ (2005).

11. Clark A.J. Optimisation heuristics for cryptology, https://eprints.qut.edu.au/15777/, (1998).

12. Clark J.A., Jacob J.L., Stepney S. The design of s-boxes by simulated annealing. In: Proceedings of the 2004 Congress on Evolutionary Computation (IEEE Cat. No.04TH8753). pp. 1533-1537 Vol. 2 (2004). https://doi.org/10.1109/CEC.2004.1331078.

13. Nyberg K. Linear Approximation of Block Ciphers. In: EUROCRYPT (1994). https://doi.org/10.1007/BFb0053460.

14. Millan W. How to improve the nonlinearity of bijective S-boxes. In: Boyd, C. and Dawson, E. (eds.). Information Security and Privacy. pp. 181–192. Springer, Berlin, Heidelberg (1998). https://doi.org/10.1007/BFb0053732.

15. Nover H. Algebraic Cryptanalysis of Aes: An Overview.

16. Bard G.V. Algebraic Cryptanalysis. Springer US, Boston, MA (2009). https://doi.org/10.1007/978-0-387-88757-9.

17. Ferguson N., Schroeppel R., Whiting D. A Simple Algebraic Representation of Rijndael // Vaudenay S. and Youssef A.M. (eds.). Selected Areas in Cryptography. pp. 103–111. Springer, Berlin, Heidelberg (2001). https://doi.org/10.1007/3-540-45537-X_8.

18. Courtois N.T., Pieprzyk J. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations // Zheng, Y. (ed.) Advances in Cryptology – ASIACRYPT 2002. pp. 267–287. Springer, Berlin, Heidelberg (2002). https://doi.org/10.1007/3-540-36178-2_17.

19. Courtois N.T., Bard G.V. Algebraic Cryptanalysis of the Data Encryption Standard // Galbraith, S.D. (ed.). Cryptography and Coding. pp. 152–169. Springer, Berlin, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77272-9_10.

20. Kuznetsov O.O., Gorbenko Y.I., Bilozertsev I.M., Andrushkevych A.V., Narizhnyi O.P.: ALGEBRAIC IMMUNITY OF NON-LINEAR BLOCKS OF SYMMETRIC CIPHERS. TRE. 77, (2018). https://doi.org/10.1615/TelecomRadEng.v77.i4.30.

21. Millan W., Burnett L., Carter G., Clark A., Dawson E. Evolutionary Heuristics for Finding Cryptographically Strong S-Boxes // Varadharajan V. and Mu Y. (eds.) Information and Communication Security. pp. 263–274. Springer, Berlin, Heidelberg (1999). https://doi.org/10.1007/978-3-540-47942-0_22.

22. Nedjah N., Mourelle L. de M., Mourelle L. de M. Multi-objective Evolutionary Design of Robust Substitution Boxes, https://www.taylorfrancis.com/, last accessed 2020/07/25. https://doi.org/10.1201/9781315366845-7.

23. Rodinko M., Oliynykov R., Gorbenko Y. Optimization of the High Nonlinear S-Boxes Generation Method. Tatra Mountains Mathematical Publications. 70, 93–105 (2017). https://doi.org/10.1515/tmmp-2017-0020.

24. Laskari E.C., Meletiou G.C., Vrahatis M.N. Utilizing Evolutionary Computation Methods for the Design of S-Boxes. In: 2006 International Conference on Computational Intelligence and Security. pp. 1299–1302 (2006). https://doi.org/10.1109/ICCIAS.2006.295267.

25. Edelkamp S., Schroedl S. Heuristic Search Theory and Applications. Morgan Kaufmann, Amsterdam ; Boston (2011).

26. Informed Search Algorithms in AI – Javatpoint, https://www.javatpoint.com/ai-informed-search-algorithms, last accessed 2021/05/19.

27. Katz M., Domshlak C. Optimal admissible composition of abstraction heuristics. Artificial Intelligence. 174, 767–798 (2010). https://doi.org/10.1016/j.artint.2010.04.021.

28. Kapuściński T., Nowicki R.K., Napoli C. Application of Genetic Algorithms in the Construction of Invertible Substitution Boxes // Rutkowski L., Korytkowski M., Scherer R., Tadeusiewicz R., Zadeh L.A., and Zurada J.M. (eds.) Artificial Intelligence and Soft Computing. pp. 380–391. Springer International Publishing, Cham (2016). https://doi.org/10.1007/978-3-319-39378-0_33.

29. Picek S., Cupic M., Rotim L. A New Cost Function for Evolution of S-Boxes. Evolutionary Computation. 24, 695–718 (2016). https://doi.org/10.1162/EVCO_a_00191.

30. Cusick T., Stănică P. Cryptographic Boolean Functions and Applications: Second edition. (2017).

31. Izbenko Y., Kovtun V., Kuznetsov A. The Design of Boolean Functions by Modified Hill Climbing Method // 2009 Sixth International Conference on Information Technology: New Generations. pp. 356–361. IEEE, Las Vegas, NV, USA (2009). https://doi.org/10.1109/ITNG.2009.102.

32. Freyre-Echevarría A., Martínez-Díaz I., Pérez C.M.L., Sosa-Gómez G., Rojas O. Evolving Nonlinear S-Boxes With Improved Theoretical Resilience to Power Attacks // IEEE Access. 8, 202728–202737 (2020). https://doi.org/10.1109/ACCESS.2020.3035163.

33. Freyre Echevarría A., Martínez Díaz I. A new cost function to improve nonlinearity of bijective S-boxes. (2020).

34. Ivanov G., Nikolov N., Nikova S. Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties // Cryptogr. Commun. 8, 247–276 (2016). https://doi.org/10.1007/s12095-015-0170-5.

35. Freyre-Echevarría A., Alanezi A., Martínez-Díaz I., Ahmad M., Abd El-Latif A.A., Kolivand H., Razaq A. An External Parameter Independent Novel Cost Function for Evolving Bijective Substitution-Boxes // Symmetry. 12, 1896 (2020). https://doi.org/10.3390/sym12111896.

36. Tesar P. A New Method for Generating High Non-linearity S-Boxes (2010).

37. Kavut S., Yücel M.D. Improved Cost Function in the Design of Boolean Functions Satisfying Multiple Criteria // Johansson, T. and Maitra, S. (eds.) Progress in Cryptology – INDOCRYPT 2003. pp. 121–134. Springer, Berlin, Heidelberg (2003). https://doi.org/10.1007/978-3-540-24582-7_9.

38. Carlet C. Vectorial Boolean functions for cryptography. Boolean Models and Methods in Mathematics, Computer Science, and Engineering (2006).

39. Clark J.A., Jacob J.L., Stepney S. The design of S-boxes by simulated annealing // New Gener Comput. 23, 219–231 (2005). https://doi.org/10.1007/BF03037656.

40. Nyberg K. Perfect nonlinear S-boxes // Davies, D.W. (ed.) Advances in Cryptology — EUROCRYPT ’91. pp. 378–386. Springer, Berlin, Heidelberg (1991). https://doi.org/10.1007/3-540-46416-6_32.

41. Carlet C., Ding C. Nonlinearities of S-boxes. Finite Fields and Their Applications. 13, 121–135 (2007). https://doi.org/10.1016/j.ffa.2005.07.003.

42. Fuller J., Millan W. Linear Redundancy in S-Boxes // Johansson, T. (ed.) Fast Software Encryption. pp. 74–86. Springer Berlin Heidelberg, Berlin, Heidelberg (2003). https://doi.org/10.1007/978-3-540-39887-5_7.

43. Clark J.A., Jacob J.L., Stepney S. Searching for cost functions // Proceedings of the 2004 Congress on Evolutionary Computation (IEEE Cat. No.04TH8753). pp. 1517-1524 Vol.2 (2004). https://doi.org/10.1109/CEC.2004.1331076.

44. Ivanov G., Nikolov N., Nikova S. Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm // Pasalic, E. and Knudsen, L.R. (eds.) Cryptography and Information Security in the Balkans. pp. 31–42. Springer International Publishing, Cham (2016). https://doi.org/10.1007/978-3-319-29172-7_3.

Надійшла до редколегії 12.09.2021

Відомості про авторів:

Кузнецов Олександр Олександрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук; Україна; e-mail: kuznetsov@karazin.ua, ORCID: https://orcid.org/0000-0003-2331-6326

Полуяненко Микола Олександрович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук; Україна; e-mail: nlfsr01@gmail.com, ORCID: https://orcid.org/0000-0001-9386-2547

Катрич Віктор Олександрович – д-р фіз.-мат. наук, професор, заслужений діяч науки і техніки України, Харківський національний університет імені В.Н. Каразіна, проректор з наукової робот; Україна; e-mail: vkatrich@karazin.ua, ORCID: https://orcid.org/0000-0001-5429-6124

Кандій Сергій Олегович – технік-конструктор, АТ «Інститут інформаційних технологій», Україна; e-mail: sergeykandy@gmail.com, ORCID: https://orcid.org/0000-0003-0552-8341

Заїченко Юлія Олександрівна – магістрант, Харківський національний університет імені В.Н. Каразіна, кафедра безпеки інформаційних систем і технологій, факультет комп’ютерних наук; Україна; e-mail: yuliya.zaicenko.00@gmail.com, ORCID: https://orcid.org/0000-0001-6116-2693

УДК 004.056.5 **DOI:10.30837/rt.2021.3.206.06**

О.О. КУЗНЕЦОВ, д-р техн. наук, М.О. ПОЛУЯНЕНКО, канд. техн. наук,
С.Л. БЕРДНИК, канд. техн. наук, С.О. КАНДІЙ, Ю.О. ЗАИЧЕНКО

ОПТИМІЗАЦІЯ ПАРАМЕТРІВ АЛГОРИТМУ ЛОКАЛЬНОГО ПОШУКУ ДЛЯ ГЕНЕРАЦІЇ НЕЛІНІЙНИХ ПІДСТАНОВОК

1. Вступ

Проєктування симетричних шифрів передбачає застосування різних криптопримітивів, зокрема і нелінійних таблиць заміни (званих також S-блоками, нелінійними підстановками, вузлами ускладнення, тощо) [1, 2]. Від криптографічних показників S-блоків залежить ефективність симетричних шифрів, зокрема їх стійкість до різних криптоаналітичних атак [3 – 5]. Отже, генерація нелінійних таблиць заміни з потрібними криптографічними показниками є безумовно актуальною та важливою науковою задачею [6 – 9].

В роботі розглядаються алгоритми локального пошуку та проводяться експериментальні дослідження їх ефективності для генерації S-блоків.

Локальний пошук відноситься до евристичних технік вирішення оптимізаційних задач та об’єднує групу обчислювальних алгоритмів, зокрема, сходження на пагорб, імітації відпалу, генетичні алгоритми та ін. [10 – 12]. Локальний пошук використовують для вирішення різних проблем, для яких можна сформулювати критерій пошуку серед безлічі можливих рішень (наприклад, у вигляді спеціальної функції вартості). По суті, всі алгоритми локального пошуку застосовують локальні зміни початкового стану до тих пір, поки не буде знайдено рішення, яке вважається оптимальним, або поки не закінчиться обмеження за часом (кількістю ітерацій) [13].

Розглядаються алгоритми локального пошуку, які застосовують спеціальну функцію вартості для інформованого пошуку підходящих рішень (S-блоків з необхідними криптографічними показниками) у просторі можливих станів (всіх можливих таблиць заміни) [6, 14, 15]. Тобто на кожному кроці через розрахунок функції вартості алгоритм оцінює можливі альтернативи та приймає рішення стосовно подальшого переборного пошуку. В статті застосовується цільова функція з робіт [16, 17] та досліджується її поведінка та вплив на ефективність алгоритму локального пошуку. Проводяться багаточисельні експерименти та евристично обираються оптимальні параметри алгоритму, наводяться оцінки його результативності. Фактично вдалося оптимізувати алгоритм локального пошуку S-блоків з цільовою нелінійністю 104 і отримати середній час генерації (при багаторазовому запуску алгоритму) 33,2 секунди (на ПК з тактовою частотою процесору 3,49 GHz, AMD Rizen 9 3950 X 16, RAM 128 GB, Windows 10). При однократному запуску алгоритму ймовірність знаходження цільового S-блоку становить 21,5 %. Це, на думку авторів, є одним із найкращих результатів для швидкої генерації нелінійних вузлів симетричних шифрів.

2. Пов’язані роботи

Техніки евристичного пошуку нелінійних підстановок розглядалися в багатьох роботах. Наприклад, в ранніх роботах [18–20] досліджувалися евристичні техніки генерації криптографічних булевих функцій, які згодом було поширено на пошук бієктивних S-блоків [6, 7, 14, 21, 22]. Цей напрямок досліджень виявився дуже продуктивним, оскільки вдавалося поступово підвищувати криптографічні показники згенерованих таблиць заміни. Зокрема, у роботах [7, 17, 22 – 24] ті ін. досліджено алгоритми імітації відпалу. Роботи [6, 21, 23, 25, 26] та ін. присвячено вивченню техніки сходження на пагорб. В [27 – 30] досліджено генетичні алгоритми. Найчастіше ставилася задача генерації бієктивних 8×8 S-блоків з найвищою нелінійністю, і поступово вдавалося підвищувати цей показник. Наприклад, в [14, 19, 21] досліджено ефективність випадкової генерації (досягнуто нелінійність 98) та техніки схо-

дження на пагорб (сформовано S-блоки з нелінійністю 100). В роботах [16, 17] застосовано техніку імітації відпалу та досягнуто нелінійність 102. В [15, 27] розглянуто генетичні алгоритми, які у комбінації із іншими методами оптимізації дозволили формувати підстановки з нелінійністю 104. На сьогодні дослідники акцентують свою увагу на функціях вартості [15, 31, 32]. Дійсно, зміна параметрів або форми функції вартості може значно вплинути на ефективність локального пошуку, і це наочно продемонстровано, наприклад, у роботах [15, 31].

В цій роботі розглянуто найпростіший варіант алгоритму локального пошуку і просту форму функцію вартості з ранніх робіт, наприклад, з [7, 16]. Метою роботи є оптимізація параметрів цього варіанту локального пошуку таким чином, щоб швидко формувати S-блоки з високою нелінійністю, тобто коли навіть для простих і добре відомих алгоритмів і функцій вартості вдається досягти показників, які є порівняні із кращими відомими на сьогодні результатами.

3. Опис алгоритму

Алгоритм локального пошуку (англ. – Local Search Algorithm, або також відомий у літературі як алгоритм Монте – Карло) – це ітераційний алгоритм, який починає свій пошук з можливої точки, випадково обраної в просторі станів. Потім послідовно застосовується механізм генерації для пошуку кращого рішення (з точки зору значення цільової функції), досліджуючи сусідство поточного рішення. Якщо знайдено краще рішення, воно стає поточним рішенням. Алгоритм закінчується, коли не вдається знайти покращення, а поточне рішення розглядається як приблизне рішення задачі оптимізації.

Алгоритм локального пошуку оптимізує цільову функцію, досліджуючи сусідні точки рішення відносно поточної точки в просторі рішень. У наступних визначеннях розглянемо (S, f) приклад комбінаторної задачі оптимізації (де S – набір можливих рішень; f – цільова функція, яку слід мінімізувати).

Нехай N – програма, яка визначає для кожного розв'язку $i \in S$ підмножину $S_i \subset S$ рішень, «близьких» (близькість визначається користувачем) відповідно до задачі i. Вважаємо, що N – структура сусідства, що визначена (S, f).

Механізм, що породжує наступний стан, – це засіб для вибору рішення j у будь-якому сусідстві S_i поточного рішення i. Конкретна методика, яка застосовується для зміни рішення, залежить від задачі, яка вирішується, та подання рішення. Наприклад, якщо рішення представлено у вигляді двійкового рядка фіксованої довжини, тоді підходящим механізмом пропонування можливих нових рішень може бути доповнення одного (або декількох) випадково вибраних значень у бітовому рядку.

Алгоритм локального пошуку (для задачі мінімізації) можна представити узагальнити наступним псевдокодом 1:

Псевдокод 1. Алгоритм пошуку локального мінімуму

1. Вибрати початкове рішення i;
2. Генерувати рішення j із сусідства S_i поточного рішення i;
3. Якщо ($f(j) < f(i)$), то j стає поточним рішенням;
4. Якщо ($f(j) \geq f(i)$) для всіх $j \in S_i$, то закінчити;
5. Перейди до кроку 2.

Розв'язок $i^* \in S$ називається *локальним оптимумом* відносно N для (S, f), якщо $f(i^*) \leq f(j)$ для всіх $j \in S_{i^*}$.

Структура сусідства N *називається точною*, якщо для кожного локального оптимуму щодо N, $i^* \in S$, i^* також є глобальним оптимумом (S, f).

В роботі запрограмований алгоритм локального пошуку, який одночасно виконував пошук в декількох потоках, працюючих паралельно. Кількість потоків вказується у вхідному параметрі thread_count (в нашому випадку thread_count = 30). Алгоритм локального пошуку

починає свою дію з рішення, яке встановлене випадково. Воно ж встановлюється як поточне рішення i. На кожній ітерації циклу утворюється декілька нових рішень j, які генеруються за заданими операторами мутації. Оператор мутації, в свою чергу, обирає випадковим чином k (використовувалось $k=2$) різних позицій у поданому рішенні і надалі переставляє елементи у обраних позиціях.

Всі ітерації алгоритму локального пошуку виконуються у внутрішньому циклі. Ітерації внутрішнього циклу вложено в зовнішній цикл. Зовнішній цикл не є обов'язковим для роботи алгоритму, він був введений для відстеження поточного стану процесу пошуку та оптимізації вибору його параметрів.

Нове рішення порівнюється з поточним. В разі отримання кращого, ніж поточне, рішення воно встановлюється як поточне. В якості цільового S-блоку було обрано S-блок з нелінійністю $N_f = 104$.

4. Трек цільової функції

В якості цільової функції було обрано функцію вартості:

$$WHS = \sum_{i=1}^{255} \left| \left| \max\left(WHT\right) \right| - X \right|^R , \tag{1}$$

де $\max(WHT)$ – максимальне значення спектральних коефіцієнтів Уолша – Адамара S-блоку (WHT – англ. Walsh – Hadamard transform – коефіцієнти Уолша – Адамара);

- X=36, R=4 – обрані параметри для функції вартості.

На рис. 1 наведено приклад роботи алгоритму з формування треку функції вартості (WHS) для перших шести зовнішніх циклів (max_outer_loops=6), десяті внутрішніх циклів (max_inner_loops=10) та чотирьох незалежних (працюючих асинхронно) потоків у кожному циклі (threads_count=4). Для наочності зміни нелінійності S-блоку для кожної функції вартості неведено поточне значення нелінійності S-блоку (N_f). Знаком «+» позначено поточний вибір кращих значень функції вартості.

Першим виконується зовнішній цикл з індексом 0 (відповідні строки з ліво на право позначені «[0] =»). Перше значення, яке обирається за найкраще, є cost=24573952 у четвертому потоці (Tread = 4) при першій ітерації. При цьому нелінійність початкового S-блоку дорівнює $N_f = 88$. Наступне значення обертається також при першій ітерації, але у другому потоці (Tread = 2) та дорівнює: cost=24315904. Першу ітерацію внутрішнього циклу закінчено. При другій ітерації внутрішнього циклу найкраще значення приймає WHS=22753280 у першому потоці, при цьому нелінійність відповідного S-боксу вже становить $N_f = 90$. Наступним краще значення при третій ітерації має третій потік з WHS=21907456 та відповідно нелінійність $N_f = 92$, і так далі. Перший цикл закінчено з кращим значенням WHS=17156352 (Tread = 3) та $N_f = 92$.

При другому зовнішньому циклі (відповідні строки позначені «[1] =») найкраще значення знаходиться у третьому потоці з WHS=16667392 при першій ітерації, а також при другій – WHS=16410112, де значення нелінійності покращується до $N_f = 94$. І так далі.

Наведені ітераційні цикли закінчуються найкращим значенням WHS=7531264 та нелінійністю $N_f = 100$ (Tread = 3, друга внутрішня ітерація). Нагадаємо, що потоки виконуються незалежно, тому попереднє найкраще значення WHS=7968000 було знайдено при четвертій ітерації другого потоку, який фактично (в часовому просторі) виконаний раніше.

```
Thread = 1
[0] = 24657664 Nf = 88   22753280 Nf = 90 + 23070720 Nf = 90   22593280 Nf = 90   22968576 Nf = 92   21449472 Nf = 92   21255936 Nf = 92   19173120 Nf = 92   18697984 Nf = 92   18793216 Nf = 92
[1] = 18027008 Nf = 92   18005504 Nf = 92   16793856 Nf = 92   15598080 Nf = 94 + 15716352 Nf = 94   16421888 Nf = 94   16390912 Nf = 96   14831360 Nf = 96   13995776 Nf = 96   13843968 Nf = 96
[2] = 13491968 Nf = 96   12124416 Nf = 96 + 13575168 Nf = 96   11696128 Nf = 96 + 12137728 Nf = 96   12347648 Nf = 98   11511040 Nf = 98 + 12165120 Nf = 96   11317248 Nf = 96   11478784 Nf = 96
[3] = 11712000 Nf = 96   12338944 Nf = 96   11095296 Nf = 98   10488832 Nf = 98   10444288 Nf = 98   10187008 Nf = 98   10444288 Nf = 98   10750464 Nf = 98   10460416 Nf = 98   10411776 Nf = 98
[4] = 10547712 Nf = 98    9615360 Nf = 98    9725184 Nf = 96    9268736 Nf = 98   10171136 Nf = 98    9630720 Nf = 98    9520896 Nf = 98   10310144 Nf = 98    9314816 Nf = 98    8844288 Nf = 98
[5] =  8568832 Nf = 98    9028352 Nf = 98    8864000 Nf = 98    8786944 Nf = 98    8770816 Nf = 98    8971520 Nf = 98    8061184 Nf = 98    9039616 Nf = 98    9148672 Nf = 98    7842560 Nf = 100
Thread = 2
[0] = 24315904 Nf = 88 + 23898880 Nf = 88   23206400 Nf = 90   22245120 Nf = 90   22760704 Nf = 92   22665728 Nf = 92   20834560 Nf = 92   18776832 Nf = 94   17977856 Nf = 92 + 17735680 Nf = 92 +
[1] = 19432960 Nf = 92   17823744 Nf = 92   16498944 Nf = 94   18161408 Nf = 94   14856448 Nf = 96 + 14267648 Nf = 98 + 13939968 Nf = 96 + 13594624 Nf = 96 + 13083648 Nf = 96 + 12351744 Nf = 96 +
[2] = 12496384 Nf = 96   13166080 Nf = 96   13451264 Nf = 94   11650816 Nf = 98 + 12574720 Nf = 98   11817728 Nf = 96   12244736 Nf = 96   12432896 Nf = 98   11992320 Nf = 96   12736512 Nf = 96
[3] = 10489856 Nf = 98 + 10110720 Nf = 98 + 10356480 Nf = 96   10467840 Nf = 98   10352128 Nf = 98   11083008 Nf = 96    9971200 Nf = 98 +  9626368 Nf = 98 +  9175040 Nf = 98 +  9773824 Nf = 98
[4] =  9661184 Nf = 96    9307136 Nf = 98    9175552 Nf = 98    9824000 Nf = 98    9406208 Nf = 98    9231360 Nf = 98    8359936 Nf = 100 + 9008128 Nf = 98    8836608 Nf = 98    8626944 Nf = 98
[5] =  8660480 Nf = 98    8963328 Nf = 98    8995072 Nf = 98    7968000 Nf = 100 + 8084736 Nf = 100   8303616 Nf = 98    8035840 Nf = 98    7788032 Nf = 98    7102976 Nf = 98 +  8151552 Nf = 98
Thread = 3
[0] = 27599872 Nf = 86   25770240 Nf = 86   21907456 Nf = 92 + 24334336 Nf = 90   20675584 Nf = 92   19764992 Nf = 92 + 18215936 Nf = 92 + 18451456 Nf = 92   19691776 Nf = 90   17156352 Nf = 92 +
[1] = 16667392 Nf = 92 + 16410112 Nf = 94 + 16765952 Nf = 92   15900928 Nf = 94   15229184 Nf = 94   15523584 Nf = 94   14140672 Nf = 96   14247680 Nf = 96   14633984 Nf = 96   13194240 Nf = 96
[2] = 13859840 Nf = 96   12294912 Nf = 96   12169728 Nf = 98   11537408 Nf = 96 + 11919616 Nf = 96   11451392 Nf = 96 + 11375360 Nf = 96   11492352 Nf = 98   11019264 Nf = 98 + 11715840 Nf = 96
[3] = 11386880 Nf = 98   11131136 Nf = 96   10740992 Nf = 98   11609600 Nf = 96   11675904 Nf = 98   10878976 Nf = 96   10360832 Nf = 96   10788608 Nf = 98   10004736 Nf = 98    9824768 Nf = 98
[4] =  9257728 Nf = 98   10234112 Nf = 96    8558080 Nf = 98 +  8600576 Nf = 98    9052672 Nf = 98    8968192 Nf = 98    8140288 Nf = 100 + 8516096 Nf = 98    8473600 Nf = 98    8650752 Nf = 98
[5] =  8844544 Nf = 98    7531264 Nf = 100 + 7816704 Nf = 98    7820544 Nf = 98    8189952 Nf = 98    8210176 Nf = 100   7491840 Nf = 98    7312128 Nf = 98    8351232 Nf = 98    7273728 Nf = 98
Thread = 4
[0] = 24573952 Nf = 88 + 25537280 Nf = 88   24875264 Nf = 88   24933376 Nf = 88   23527168 Nf = 90   20508928 Nf = 92 + 19581184 Nf = 92 + 18914048 Nf = 92   18319616 Nf = 92   18215936 Nf = 92
[1] = 17441792 Nf = 92   17569280 Nf = 92   16595200 Nf = 92   16707584 Nf = 94   17074944 Nf = 94   14479872 Nf = 96   15001088 Nf = 96   13867008 Nf = 96   14000384 Nf = 96   12122624 Nf = 96 +
[2] = 13317376 Nf = 94   12077824 Nf = 98   12715520 Nf = 96   12618752 Nf = 98   11909888 Nf = 96   11212544 Nf = 98 + 12107776 Nf = 96   12372736 Nf = 98   11607296 Nf = 98   10898944 Nf = 98 +
[3] = 11386880 Nf = 98   11131136 Nf = 96   10740992 Nf = 98   11609600 Nf = 96   11675904 Nf = 98   10878976 Nf = 96   10360832 Nf = 96   10788608 Nf = 98   10004736 Nf = 98    9824768 Nf = 98
[4] =  9552896 Nf = 98    9323776 Nf = 98    9490688 Nf = 98    9609472 Nf = 98    9658880 Nf = 98    8787712 Nf = 98    8607232 Nf = 98    9565952 Nf = 98    9072128 Nf = 98    8256256 Nf = 98
[5] =  8723200 Nf = 98    9068544 Nf = 98    8913408 Nf = 98    7851520 Nf = 98    7603200 Nf = 98    8335872 Nf = 98    7756544 Nf = 96    7708416 Nf = 98    7272448 Nf = 98    7477760 Nf = 98
```

Рис. 1. Значення перших чотирьох циклів при формуванні функції вартості.
Знаком «+» позначено поточний вибір кращих значень функції вартості

Таким чином, можна побудувати так званий трек функції вартості, що буде відповідати поточному кращому значенню функції WHS. Наведемо зазначений трек для зовнішнього циклу, тобто найкраще значення WHS, яке буде у кінці кожного зовнішнього циклу: 17156352 ($N_f = 92$); 12122624 ($N_f = 96$); 10898944 ($N_f = 98$); 9175040 ($N_f = 98$); 8140288 ($N_f = 100$); 7531264 ($N_f = 100$).

Розглянемо трек функції вартості наприкінці кожного з внутрішніх циклів (табл. 1). У таблицю заносилися значення, якщо хоча б один раз у потоці було знайдено найкращу поточну функцію вартості (вона може не бути кращою серед інших потоків). Символом «–» відзначено зовнішній цикл, при якому жодного покращення не було знайдено. Пошук завершено на 33 ітерації зовнішнього циклу, коли знайдено S-блок з нелінійністю $N_f = 104$.

Таблиця 1

Приклад зміни значення найкращої функції вартості (cost) та нелінійності (N_f) для зовнішніх циклів та окремих потоків

Зовнішній цикл, номер	Thread = 1		Thread = 2		Thread = 3		Thread = 4	
	WHS	N_f	*WHS*	N_f	*WHS*	N_f	*WHS*	N_f
0.	3869696	100	4185088	102	3728896	100	3553536	100
1.	3536128	100	3527168	102	3413248	102	3496448	100
2.	3039744	102	–		3212032	102	3138304	102
3.	–		–		3015680	102	–	
4.	–		–		2941952	102	2929664	102
5.	–		–		–		2897664	102
6.	–		–		–		–	
7.	–		–		2832384	102	–	
8.	2803968	102	–		–		2814464	102
9.	2769920	102	–		–		2774784	102
10.	–		–		–		2695680	102
11.	2657280	102	–		–		–	
12.	–		–		–		–	
13.	2636800	102	2614784	102	2607104	102	–	
14.	–		–		–		–	
15.	–		2606080	102	–		–	
16.	2577408	102	–		–		2541824	102
17.	–		–		–		–	
18.	–		–		–		–	
19.	–		–		–		–	
20.	2408448	102	2485248	102	–		–	
21.	–		–		–		–	
22.	–		–		–		–	
23.	–		–		–		–	
24.	–		–		–		–	
25.	–		–		–		–	
26.	–		–		–		–	
27.	–		–		–		–	
28.	–		–		–		2395648	102
29.	–		–		2370304	102	–	
30.	–		–		–		–	
31.	–		–		–		–	
32.	–		–		–		–	
33.	2321408	104	2143488	102	2312704	102	–	

Завдяки випадковості зміни двох елементів S-блоку виконуються як зондування сусідніх станів на можливість покращення функції вартості у кожному з потоків. В разі можливості такого покращення воно виконується, і нова ітерація у кожному потоці приймає за поточний стан проведені зміни у S-блоку.

Із збільшенням номеру зовнішнього циклу функція вартості наближується до «дна» поточного локального мінімуму, що зменшує ймовірність покращити значення функції вартості при випадковій мутації. Тому є сенс обмежитися деякою максимальною кількістю поспіль зовнішніх циклів (max_frozen_outer_loops), при яких не виконано жодного покращення функції вартості, а також деякою максимальною кількістю зовнішніх циклів (max_outer_loops). При досягненні значення max_frozen_outer_loops або max_outer_loops вважається, що стан знаходиться у локальному мінімумі функції вартості. Тому пошук припиняється, формується новий стан S-блоку та процедура пошуку цільових параметрів S-блоку починається знову.

Для вибору оптимального значення max_outer_loops та max_frozen_outer_loops розглянемо їх вплив на результати роботи алгоритму пошуку.

5. Оптимізація параметрів локального пошуку

5.1. Оптимізація кількості зовнішніх циклів (max_outer_loops)

Для визначення максимальної кількості зовнішніх циклів (max_outer_loops) було проведено пошук S-блоків з цільовою нелінійністю $N_f = 104$ алгоритмом локального пошуку. Пошук виконувався за наступними параметрами:

- threads_count=30;
- max_outer_loops=50
- max_inner_loops=1000
- X=36;
- R=4.

Загалом було проведено 1500 запусків алгоритму локального пошуку, з яких було знайдено 346 (23 %) S-блоків з цільовою нелінійністю 104. Кількість зовнішніх циклів, протягом яких було знайдено покращення функції вартості, наведена на рис. 2 (гістограми суцільного кольору), для порівняння окремо наведено стовпчики (зі штрихованим заповненням) лише для випадку, коли у результаті роботи алгоритму було досягнуто цільову нелінійність. З 1500 лише в двох випадках було виконано 25 ітерацій зовнішнього циклу. Таким чином, при обраних параметрах, доцільно обмежитися максимальним значенням кількості зовнішніх циклів max_outer_loops=25.

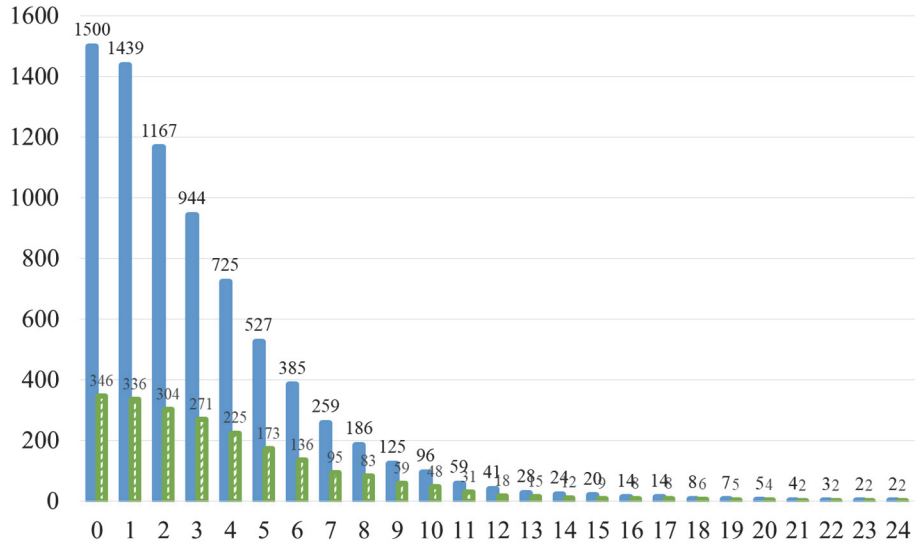


Рис. 2. Кількість зовнішніх циклів, протягом яких було знайдено покращення функції вартості

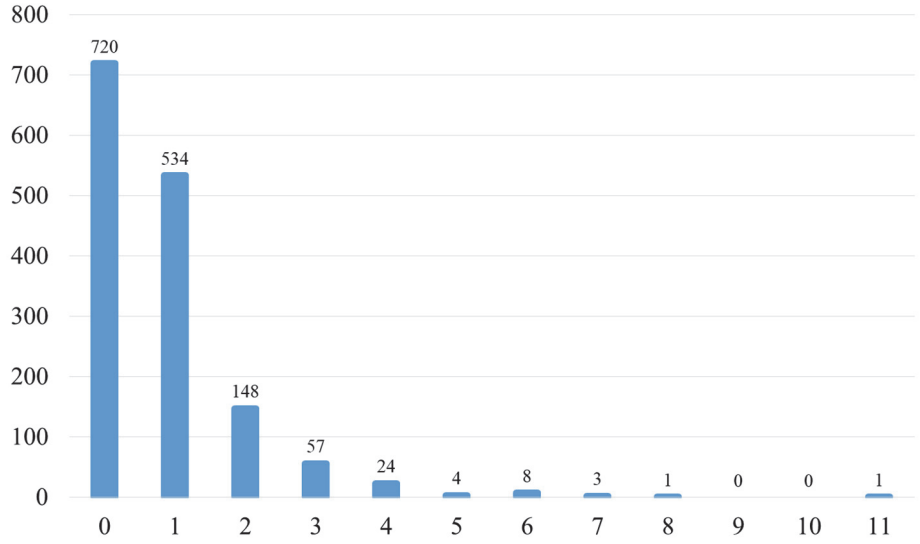


Рис. 3. Розподіл кількості поспіль виконаних зовнішніх циклів,
при яких не знайдено жодного покращення, однак потім покращення мали місце

На рис. 3 наведено гістограму розподілу кількості поспіль зовнішніх циклів, при яких не знайдено жодного покращення, однак потім покращення мали місце (для наочного пояснення цього випадку можна звернутися до комірок позначених символом «–» табл. 1). Бачимо, що після дев'ятої ітерації зовнішнього циклу менш ніж 9 % зовнішніх циклів знаходять покращення функції вартості. Нуль відповідає випадку, якщо у кожному зовнішньому циклі були знайдені рішення, які покращують цільову функцію. Якщо обмежитися пятьма поспіль відсутніми покращеннями, то з 1500 проведених випробувань будуть помилково відкинуті 15 випробувань (4 – випробування з 5 поспіль нерезультативними випробуваннями, 8 – з 6 поспіль нерезультативними випробуваннями, 3 – з 7 та по одному з 9 та 11), що становить 1 %.

Таким чином, при заданих параметрах (threads_count=30, max_inner_loops=1000, X=36, R=4) будимо вважати за кращі:

- max_outer_loops=25;
- max_frozen_outer_loops=5.

Ще раз зазначимо, при інших параметрах (наприклад, зменшення threads_count та / або max_inner_loops) необхідно вибирати інші кращі значення max_outer_loops та max_frozen_outer_loops (в наведеному прикладі необхідно буде їх збільшити, так як буде зменшена кількість сусідніх значень, які тестуються). При max_frozen_outer_loops=5 та max_inner_loops=1 000 маємо загальне обмеження у 5000 тестів, при яких відсутнє жодне покращення значення цільової функції.

Узагальнена картина зміни треку функції вартості з кожним новим кроком ітерації зовнішнього циклу наведена на рис. 4. Суцільною лінією позначено усереднене значення WHS за 1500 випробуваннями. Пунктир – усереднене значення WHS за 346 випробуваннями, за яким знайдено S-блоків з $N_f = 104$. Як бачимо, середнє значення функцій вартості, які приходять до цільових показників нелінійності має характерний для інших трек. Крапкова лінія – середнє відхилення від усередненого значення функції вартості за всіма1500 випробуваннями. Середнє відхилення має невелике значення, що вказує на добру узгодженість різних випробувань з середньо статистичними результатами. Лінія крапка-тире – абсолютне максимальне відхилення від середнього значення. Значення функції вартості, у випадках, де було знайдено S-блок з цільовою нелінійністю, не перевищувало $2,6 \cdot 10^6$. За допомогою алгоритму локального пошуку можна досить швидко знайти S-блок з функцією вартості нижчі ніж $2 \cdot 10^6$, що добре буде поєднуватися з іншими методами пошуку S-блоків з цільовими характеристиками.

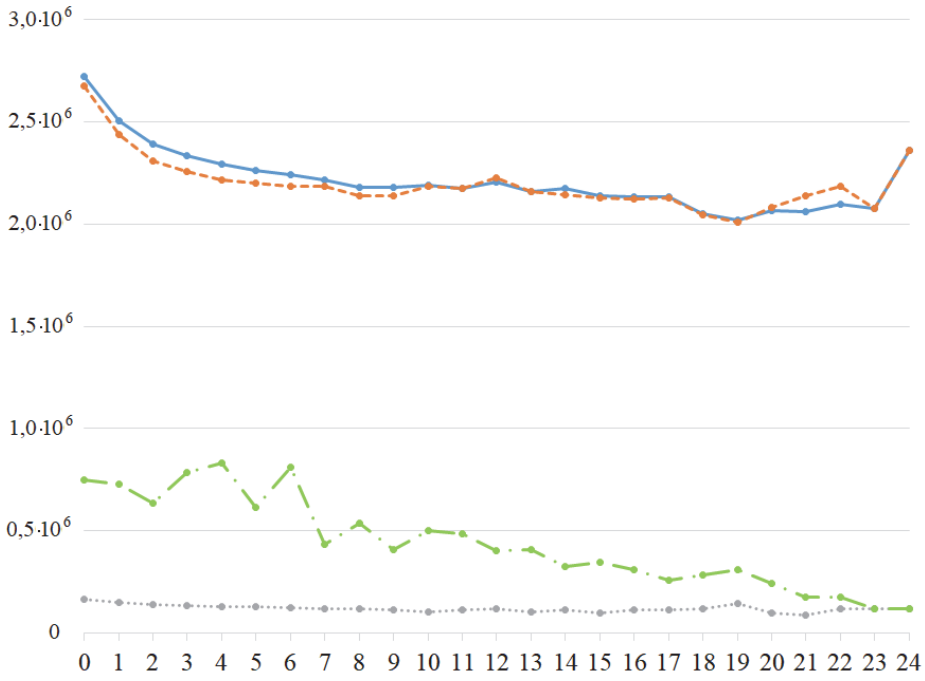


Рис. 4. Трек зміни середнього значення найкращої функції вартості

5.2. Оптимізація кількості внутрішніх циклів (max_inner_loops)

Наступним кроком встановимо вплив кількості внутрішніх циклів (параметр max_inner_loops). Тестування проводилися на двох обчислювальних машинах з багатоядерними процесорами:

- з тактовою частотою процесору 2,59 GHz, Intel Core i9-7980 XE, RAM 64 GB, Window 10 (на ПК № 1);
- з тактовою частотою процесору 3,49 GHz, AMD Rizen 9 3950 X 16, RAM 128 GB, Windows 10 (на ПК № 2).

На кожній машині запускалось по 30 окремих потоків, тобто threads_count = 30, кількість зовнішніх циклів була max_outer_loops=50, параметри цільової функції *WHS* залишалися фіксованими: $X = 36$; $R = 4$. Параметр max_inner_loops змінювався у наступному діапазоні:

- max_inner_loops від 200 до 600 з шагом 10 (на машині № 1);
- max_inner_loops від 610 до 1000 з шагом 10 (на машині № 2).

Тестування проводилось по 11 груп, у кожній групі виконувалось 100 запусків алгоритму пошуку. У кожній групі іспитів всі параметри залишалися незмінними. Таким чином, для кожного параметра проводилось 1 100 запусків. Всього було проведено 89 100 запусків алгоритму за приблизно 367 годин (астрономічного часу) на кожній машині. На рис. 5 наведено кількість знайдених цільових S-блоків в залежності від кількості внутрішніх циклів для кожної з 11 груп. Як бачимо з отриманих результатів при max_inner_loops менш 250 цільові S-блоки майже не знайдено. В інтервалі від 250 до 650 йде майже лінійних ріст кількості знайдених цільових S-блоків, а з 650 та вище значного приросту кількості знайдених цільових S-блоків не спостерігається.

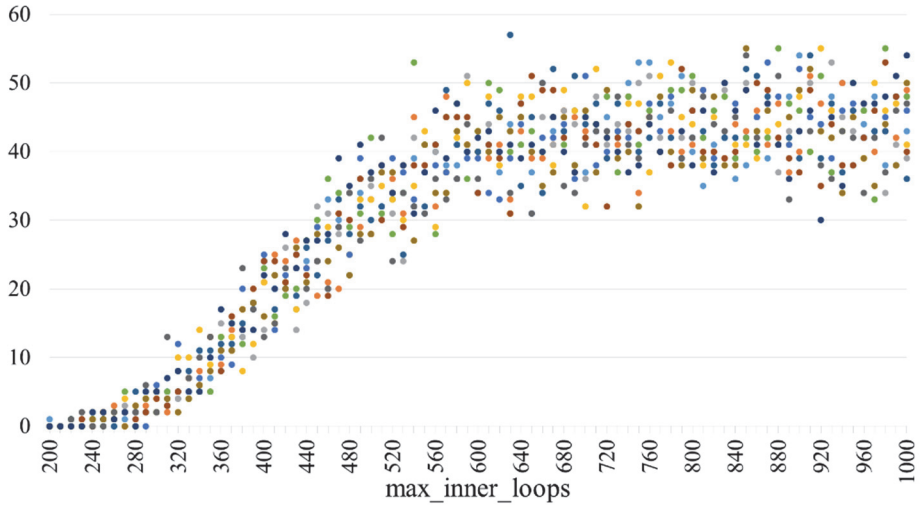


Рис. 5. Кількість знайдених цільових S-блоків в залежності від кількості внутрішніх циклів

Якщо треба знайти максимальну кількість цільових S-блоків, то слід брати велике значення max_inner_loops у кожному тестуванні. Однак, якщо збільшується кількість внутрішніх циклів, то пропорційно зростає час на кожне тестування. На рис. 6 наведено середній (за 100 запусків) час, що було затрачено на кожне виконання алгоритму локального пошуку у кожній групі. Нагадаємо, що тестування проведено на двох різних обчислювальних машинах, тому результати затраченого часу, які наведені на першій половині графіку, кількісно не співпадають із затраченим часом наведеним на другій половині графіку. Це пояснюється різною обчислювальною потужністю цих ПК. Але якісно відповідні залежності є продовженням одна одної.

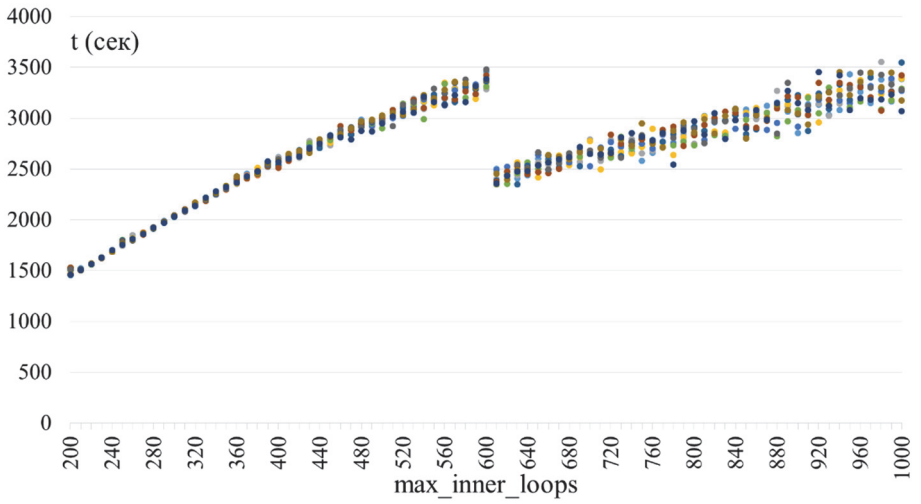


Рис. 6. Час, що було затрачено для тестування у кожній групі

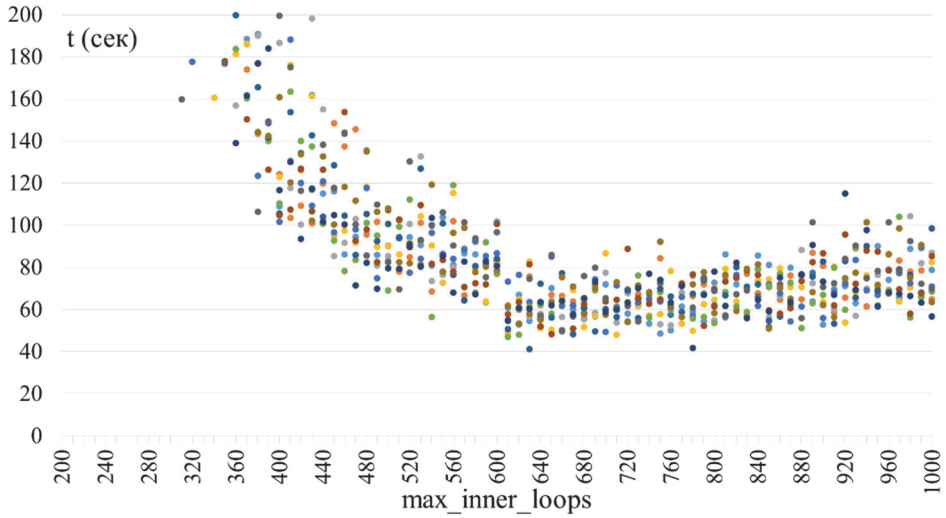


Рис. 7. Середній час пошуку цільового S-блоку у кожній групі

Доцільно розглянути середній час, що було затрачено у кожній групі на пошук цільового S-блоку. Зазначений час будемо обраховувати як відношення часу виконання алгоритму (див. рис. 6) до кількості знайдених цільових S-блоків у циклі (див. рис. 5). Обчислений таким чином середній час пошуку цільового S-блоку наведено на рис. 7. Виходячи з мінімізації значення середнього часу пошуку цільового S-блоку обираємо значення max_inner_loops = 650.

Слід відзначити, що загальна кількість ітерації при пошуку цільового S-блоку алгоритмом пошуку локального мінімуму складає: threads_count * max_outer_loops * max_inner_loops = 30 * 50 * 650 = 975 000. Від вказаного значення треба відштовхуватися під час вибору вхідних параметрах на фізичних пристроях, які підтримують іншу кількість потоків (threads_count).

5.3. Оптимальні параметри алгоритму локального пошуку цільового S-блоку

Узагальнюючи наведений матеріал встановлені наступні оптимальні (с точки зору мінімального часу) параметри для проведення пошуку S-блоку методом локального пошуку з цільовою нелінійністю $N_f = 104$ та кількістю паралельних потоків threads_count = 30:

- максимальна кількість зовнішніх циклів: max_outer_loops=25;
- максимальна кількість внутрішніх циклів: max_inner_loops=650;
- максимальна кількість поспіль зовнішніх циклів, при яких не виконано жодного покращення функції вартості: max_frozen_outer_loops=5;

Параметри наведено за умови використання цільової функції (1) з параметрами:

- $X = 36$;
- $R = 4$;

Наведені параметри справедливі для 30 потоків, для іншої кількості потоків оптимальні параметри можуть бути іншими. Це пов’язано із загальною кількістю випробувань, які проводяться для кожного циклу пошуку цільового S-блоку.

6. Середній час пошуку цільового S-блоку при оптимальних параметрах

При вказаних оптимальних параметрах було проведено 78 869 запусків алгоритму локального пошуку. Часом пошуку вважався загальний час роботи програми до знаходження цільового S-блоку. Тобто, якщо за два запуски по 30 секунд кожний не було знайдено цільового S-блоку, а впродовж третього знайдено за 10 секунд, то часом пошуку вважається 70 секунд.

Кожний запуск закінчувався або при знаходженні цільового S-блоку або виходом з циклу при досягненні граничних значень ітерації у пошуку. Загалом було знайдено 16 980

(21,5 % від загальної кількості циклів тестувань) цільових S-блоків із середнім часом пошуку одного блоку у 33,2 секунди. Гістограма розподілу кількості знайдених цільових S-блоків в залежності від часу, що був затрачений на їх пошук, наведено на рис. 8. На рисунку наведено значення, що не перевищують двох хвилин пошуку. Ще 390 цільових S-блоків (2,3 % від загальної кількості) було знайдено за час, що перевищував дві хвилини.

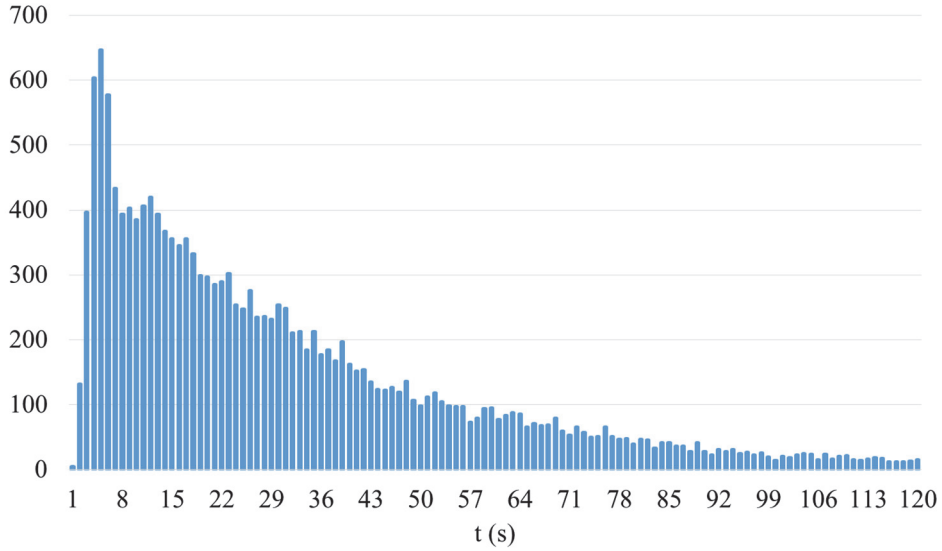


Рис. 8. Розподіл кількості знайдених цільових S-блоку в залежності від часу (t, секунди), що було затрачено на їх пошук

Висновки

Досліджено алгоритм локального пошуку з точки зору застосування у формуванні S-блоків з заданими криптографічними властивостями, серед яких було обрано нелінійність $N_f = 104$. Наведено опис алгоритму. Досліджено основні його параметри та встановлено оптимальні (з точки зору часу формування S-блоку) їх значення:

- максимальна кількість зовнішніх циклів: max_outer_loops=25;
- максимальна кількість внутрішніх циклів: max_inner_loops=650;
- максимальна кількість поспіль зовнішніх циклів, при яких не виконано жодного покращення функції вартості: max_frozen_outer_loops=5;

Вказані значення є оптимальними за умови запуску алгоритму з 30 паралельно працюючими потоками та застосування цільової функції (1) з параметрами: $X = 36$ та $R = 4$.

При вказаних параметрах середній час формування S-блоку з нелінійністю $N_f = 104$ становить 33,2 секунди та ймовірність знаходження S-блоку становить 21,5 %.

References:

1. Schneier B. Applied cryptography: protocols, algorithms, and source code in C. New York : Wiley, 1996.
2. Menezes A.J., Oorschot P.C. van, Vanstone S.A., Oorschot P.C. van, Vanstone S.A. Handbook of Applied Cryptography // CRC Press (2018). https://doi.org/10.1201/9780429466335.
3. Carlet C. Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering (2006).
4. Carlet C., Ding C. Nonlinearities of S-boxes // Finite Fields and Their Applications. 13, 121–135 (2007). https://doi.org/10.1016/j.ffa.2005.07.003.
5. Álvarez-Cubero J. Vector Boolean Functions: applications in symmetric cryptography, (2015). https://doi.org/10.13140/RG.2.2.12540.23685.
6. Burnett L.D. Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography, https://eprints.qut.edu.au/16023/, (2005).
7. Clark A.J. Optimisation heuristics for cryptology, https://eprints.qut.edu.au/15777/ (1998).
8. Fuller J.E. Analysis of affine equivalent boolean functions for cryptography, https://eprints.qut.edu.au/15828/ (2003).

9. McLaughlin J. Applications of search techniques to cryptanalysis and the construction of cipher components, http://etheses.whiterose.ac.uk/3674/ (2012).

10. Battiti R., Brunato M., Mascia F. Reactive Search and Intelligent Optimization : Springer US (2009). https://doi.org/10.1007/978-0-387-09624-7.

11. Hromkovič J. Algorithmics for Hard Problems // Introduction to Combinatorial Optimization, Randomization, Approximation, and Heuristics. Springer-Verlag, Berlin Heidelberg (2004). https://doi.org/10.1007/978-3-662-05269-3.

12. Arya V., Garg N., Khandekar R., Meyerson A., Munagala K., Pandit V. Local search heuristic for k-median and facility location problems // Proceedings of the thirty-third annual ACM symposium on Theory of computing. pp. 21–29. Association for Computing Machinery, New York, NY, USA (2001). https://doi.org/10.1145/380752.380755.

13. Edelkamp S., Schroedl S. Heuristic Search: Theory and Applications. Morgan Kaufmann, Amsterdam; Boston (2011).

14. Millan W., Burnett L., Carter G., Clark A., Dawson E. Evolutionary Heuristics for Finding Cryptographically Strong S-Boxes // Varadharajan, V. and Mu, Y. (eds.) Information and Communication Security. pp. 263–274. Springer, Berlin, Heidelberg (1999). https://doi.org/10.1007/978-3-540-47942-0_22.

15. Freyre-Echevarría A., Alanezi A., Martínez-Díaz I., Ahmad M., Abd El-Latif A.A., Kolivand H., Razaq A. An External Parameter Independent Novel Cost Function for Evolving Bijective Substitution-Boxes // Symmetry. 12, 1896 (2020). https://doi.org/10.3390/sym12111896.

16. Clark J.A., Jacob J.L., Stepney S. The design of S-boxes by simulated annealing // New Gener Comput. 23, 219–231 (2005). https://doi.org/10.1007/BF03037656.

17. Clark J.A., Jacob J.L., Stepney S. Searching for cost functions // Proceedings of the 2004 Congress on Evolutionary Computation (IEEE Cat. No.04TH8753). pp. 1517-1524 Vol.2 (2004). https://doi.org/10.1109/CEC.2004.1331076.

18. Millan W., Clark A. Smart Hill Climbing Finds Better Boolean Functions. (1997).

19. Millan W., Clark A., Dawson E. Heuristic design of cryptographically strong balanced Boolean functions // Nyberg, K. (ed.) Advances in Cryptology – EUROCRYPT'98. pp. 489–499. Springer Berlin Heidelberg, Berlin, Heidelberg (1998).

20. Millan W., Clark A., Dawson E. Boolean Function Design Using Hill Climbing Methods // Pieprzyk, J., Safavi-Naini, R., and Seberry, J. (eds.) Information Security and Privacy. pp. 1–11. Springer, Berlin, Heidelberg (1999). https://doi.org/10.1007/3-540-48970-3_1.

21. Millan W. How to improve the nonlinearity of bijective S-boxes // Boyd C. and Dawson E. (eds.) Information Security and Privacy. pp. 181–192. Springer, Berlin, Heidelberg (1998). https://doi.org/10.1007/BFb0053732.

22. Clark J.A., Jacob J.L., Stepney S. The design of s-boxes by simulated annealing // Proceedings of the 2004 Congress on Evolutionary Computation (IEEE Cat. No.04TH8753). pp. 1533-1537 Vol.2 (2004). https://doi.org/10.1109/CEC.2004.1331078.

23. Kavut S., Yücel M.D. Improved Cost Function in the Design of Boolean Functions Satisfying Multiple Criteria // Johansson T. and Maitra S. (eds.) Progress in Cryptology – INDOCRYPT 2003. pp. 121–134. Springer, Berlin, Heidelberg (2003). https://doi.org/10.1007/978-3-540-24582-7_9.

24. Souravlias D., Parsopoulos K.E., Meletiou G.C. Designing bijective S-boxes using Algorithm Portfolios with limited time budgets // Applied Soft Computing. 59, 475–486 (2017). https://doi.org/10.1016/j.asoc.2017.05.052.

25. Ivanov G., Nikolov N., Nikova S. Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm // Pasalic E. and Knudsen L.R. (eds.) Cryptography and Information Security in the Balkans. pp. 31–42. Springer International Publishing, Cham (2016). https://doi.org/10.1007/978-3-319-29172-7_3.

26. Eastlake 3rd, D., Schiller J., Crocker S. Randomness Requirements for Security (2005).

27. Tesar P. A New Method for Generating High Non-linearity S-Boxes (2010).

28. Laskari E.C., Meletiou G.C., Vrahatis M.N. Utilizing Evolutionary Computation Methods for the Design of S-Boxes // 2006 International Conference on Computational Intelligence and Security. pp. 1299–1302 (2006). https://doi.org/10.1109/ICCIAS.2006.295267.

29. Kapuścińsk T., Nowicki R.K., Napoli C. Application of Genetic Algorithms in the Construction of Invertible Substitution Boxes // Rutkowski L., Korytkowski M., Scherer R., Tadeusiewicz R., Zadeh L.A., and Zurada J.M. (eds.). Artificial Intelligence and Soft Computing. pp. 380–391. Springer International Publishing, Cham. (2016). https://doi.org/10.1007/978-3-319-39378-0_33.

30. Ivanov G., Nikolov N., Nikova S. Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties // Cryptogr. Commun. 8, 247–276 (2016). https://doi.org/10.1007/s12095-015-0170-5.

31. Picek S., Cupic M., Rotim L. A New Cost Function for Evolution of S-Boxes // Evolutionary Computation. 24, 695–718 (2016). https://doi.org/10.1162/EVCO_a_00191.

32. Freyre Echevarría A., Martínez Díaz I. A new cost function to improve nonlinearity of bijective S-boxes. (2020).

Надійшла до редколегії 10.09.2021

Відомості про авторів:

Кузнецов Олександр Олександрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: kuznetsov@karazin.ua, ORCID: https://orcid.org/0000-0003-2331-6326

Полуяненко Микола Олександрович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: nlfsr01@gmail.com, ORCID: https://orcid.org/0000-0001-9386-2547

Бердник Сергій Леонідович – канд. техн. наук, доцент, Харківський національний університет імені В.Н. Каразіна, в.о. завідувача кафедри фізичної і біомедичної електроніки та комплексних інформаційних технологій, факультет радіофізики, біомедичної електроніки та комп`ютерних систем; Україна; e-mail: berdnik@karazin.ua, ORCID: https://orcid.org/0000-0002-0037-6935

Кандій Сергій Олегович – технік-конструктор, АТ «Інститут інформаційних технологій», Україна; e-mail: sergeykandy@gmail.com, ORCID: https://orcid.org/0000-0003-0552-8341

Заїченко Юлія Олександрівна – магістрант, Харківський національний університет імені В.Н. Каразіна, кафедра безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: yuliya.zaicenko.00@gmail.com, ORCID: https://orcid.org/0000-0001-6116-2693

УДК 004.056.5 **DOI:10.30837/rt.2021.3.206.07**

К.Ю. ШЕХАНІН, С.В. ПШЕНИЧНА, О.О. КУЗНЕЦОВ, д-р техн. наук

ДОСЛІДЖЕННЯ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ У КЛАСТЕРНІ СТЕГАНОСИСТЕМИ

Вступ

На сьогодні інформацію розглядають як один з основних ресурсів для розвитку сучасного суспільства, а інформаційні системи та технології – як засоби підвищення ефективності та продуктивності роботи сучасних систем.

Інформаційні технології визначають процеси передачі і розповсюдження, зберігання та обробки інформації, а також її використання у певних цілях. Інколи факт виконання цих процесів має бути прихований від сторонніх осіб. Цим і займається галузь науки стеганографія.

Суспільству здавна відома більшість стеганографічних методів, заснованих на фізичних явищах природи чи фізіологічних особливостей людського організму. Але технології не стоять на місці, із відкриттям нових засобів обробки та зберігання інформації з'являються нові методи приховування інформації, що засновані на технічних особливостях технологічних засобів і методів обробки інформації, дана галузь науки називається технічною стеганографією.

На даний час відомо декілька методів технічної стеганографії. Наприклад, приховування інформації у модель під час 3D-друку [1 – 3]. Дана галузь приховування інформації має певні переваги та недоліки, а саме: відносно більшу вартість при створенні прихованого повідомлення та складності при зчитуванні інформації. Другий напрямок технічної стеганографії пов'язаний із мережевим трафіком [4 – 7]. У даному методі інформація може приховуватись, наприклад, у поля заголовків протоколів, чи, наприклад, приховане повідомлення шляхом передається через посилання певної послідовності пакетів. Також існують методи приховування інформації у структуру файлової системи [8 – 10], але відомі методи, які або здатні приховати малу кількість інформації, або мають належний рівень стійкості до детектування. Таким чином, актуальною задачею є розробка методу приховування інформації, який здатний приховати більшу кількість інформації та має більший рівень стійкості до детектування, із задовільним рівнем обчислювальної складності.

У роботах [11, 12] представлено методи технічної стеганографії, що базуються на структурній особливості файлових систем у носіях інформації. А саме, приховування інформації у файловій системі FAT шляхом перемішування кластерів певних, ключових файлів. Методи приховування інформації у структуру кластерної файлової системи шляхом перемішування кластерів покриваючих файлів потребують значних обчислювальних ресурсів.

У даній роботі досліджено методи підвищення обчислювальної ефективності за кількістю необхідної оперативної пам'яті та за кількістю необхідних операцій для приховування повідомлення.

Обчислювальна складність методів приховування інформації

Необхідно визначити обчислювальну складність методів приховування та вилучення інформації шляхом перестановки кластерів покриваючих файлів структури файлової системи FAT для подальших рекомендацій щодо використання методів та розробки програмної реалізації.

Так як більшість часу на приховування повідомлення у структуру файлової системи займає саме робота із фізичним носієм, то виділимо такі операції:

– обчислювальна складність на переміщення зчитуючої головки фізичного носія (для HDD накопичувачів) чи зміна позиції робочого сектору (для SSD накопичувачів) – $O\left(f\left(n\right)\right)$,

де n – кількість переміщень зчитуючої головки фізичного носія у кількості пройдених секторів;

– обчислювальна складність на зчитування даних із сектору – $O\left(g\left(n\right)\right)$, де n – кількість кластерів що зчитані;

– обчислювальна складність на запис даних у сектор – $O\left(h\left(n\right)\right)$, де n – кількість кластерів що записано;

У деяких випадках обчислювальна складність залежить від кількості стеганоблоків – k. Далі необхідно визначити загальну обчислювальну складність для базового [11] та для модифікованого методів [11 – 13]. Обчислювальну складність f, g, h вважатимемо складністю за часовими ознаками, у той час як необхідну кількість оперативної пам'яті m – вважатимемо складністю за об'ємними параметрами.

Обчислювальною складністю на генерацію перестановки будемо нехтувати, так як час на виконання даної операції, у порівняні на час роботи із фізичним носієм, є мінімальним.

Загальна обчислювальна складність для базового методу складається із суми перелічених вище елементів обчислювальної складності:

$$O\left(B\right)=O\left(f\left(n\right)\right)+O\left(g\left(n\right)\right)+O\left(h\left(n\right)\right) \tag{1}$$

Також необхідно зазначити, що загальна обчислювальна складність залежить від кількості секторів що були перезаписані, та від кількості переміщень зчитуючої головки пристрою, а отже необхідно виявити залежність між розміром повідомлення (кількістю стеганоблоків) та кількістю перезаписаних кластерів. Для цього спиратимемося на роботу [11 – 14] приховування даних у структуру файлової системи.

Приховування інформації стеганографічними методами [11, 12] виконується за рахунок перезапису даних із кластерів. Та для того щоб покриваючи файли були цілісними інформацію, необхідно копіювати повністю, це робиться із використанням оперативної пам'яті. За способом роботи із оперативною пам'яттю можна виділити такі варіації:

– повний запис даних з кластерів до оперативної пам'яті, у такому випадку необхідна кількість оперативної пам'яті залежить від кількості кластерів покриваючих файлів;

– почерговий запис даних з кластерів до оперативної пам'яті, у такому випадку у оперативну пам'ять зчитуються дані з кластеру *Б*, після чого записуються дані з кластеру *А*, далі каретка зчитуючої головки переміщується до кластеру *В* і процес повторюється (зчитуються дані із *В*, записуються дані із *Б* і так далі). Таким чином, при виконанні приховування інформації необхідно мати розмір оперативної пам'яті як подвійний розмір до одного кластеру.

За шляхом генерації перестановок, можна виділити такі варіації виконання методів приховування:

– виконання перестановки із подальшим послідовним перезаписом кластерів у необхідній послідовності. Це означає, що спочатку приховуються кластери, які складають стеганограму, а вже після цього необхідно розмістити усі вільні (ті, які не несуть інформаційного навантаження на приховування повідомлення) кластери покриваючих файлів у впорядкованій послідовності. Спочатку впорядковані кластери першого покриваючого файлу, потім другого і так далі. Така варіація методу приховування дозволяє знизити надлишковий рівень фрагментації покриваючих файлів;

– виконання перестановки із переміщенням лише інформативних кластерів у нормальну послідовність. У такому випадку спочатку переміщуємо інформаційні кластери у відповідну до повідомлення послідовність, після чого переміщуємо кластери, які були витиснені інформаційними кластерами. Витиснені кластери впорядковано розміщуємо лише на позиції, де знаходилися інформаційні кластери. Перевагою такого методу є те, що необхідно буде перемістити лише обмежену розміром повідомлення кількість кластерів;

– виконання перестановки із оптимальним переміщенням лише інформативних кластерів. У такому випадку переміщуємо інформаційні кластери у відповідну до повідомлення послідовність, але із можливістю збереження позиції кластером, якщо він відповідає значенню стеганоблока. Усе інше аналогічно до попереднього методу. Такий метод дозволяє ще значніше зменшити кількість перезаписів кластерів, але можуть виникати випадку, коли покриваючі файли матимуть переплетеність (деякі кластери файлу розміщені у зворотній послідовності, що є аномальною поведінкою файлової системи і може детектувати приховане повідомлення).

Комбінуючи методи оптимізації за оперативною пам'яттю та методи зменшення обчислювальної складності, ми запропонували чотири способи приховування інформації у структуру кластерних файлових систем (чотири для базового методу та чотири – для модифікованого) із прикладами.

ПЗОП

Виконання перестановки із повним завантаженням кластерів до оперативної пам'яті та подальшим послідовним перезаписом кластерів у необхідній послідовності, рис. 1. Далі даний метод називатимемо повним завантаженням до оперативної пам'яті ПЗОП.

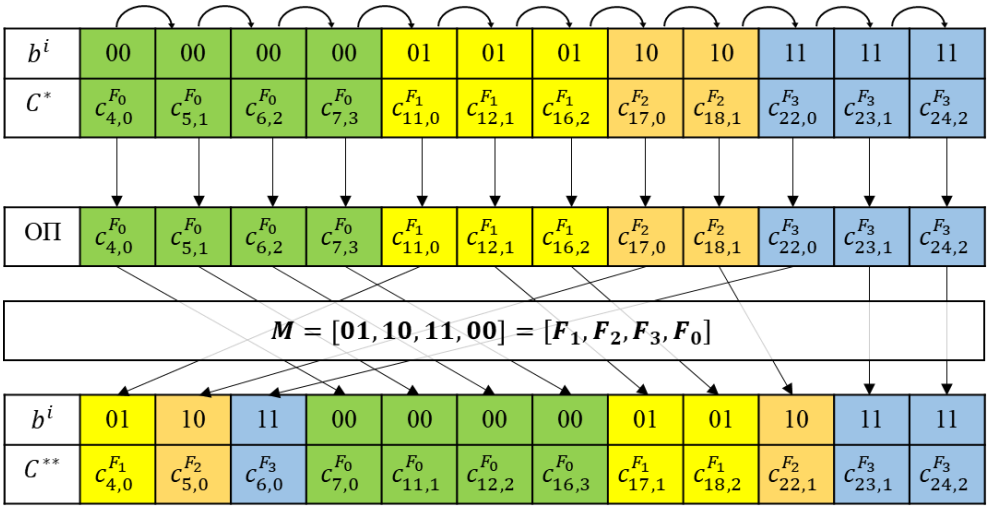


Рис.1. Приклад перестановки кластерів із повним завантаженням даних у операційну пам'ять

Даний метод реалізацій перестановки дозволяє нівелювати обчислювальну складність на переміщення зчитуючої головки фізичного носія, так як спочатку виконується послідовне зчитування кластерів до операційної пам'яті. Потім перестановка виконується у операційній пам'яті як робота із масивом, а далі так само послідовно виконується перезапис кластерів. Необхідно зазначити, що спосіб перемішування кластерів потребує значного розміру оперативної пам'яті, щоб завантажити усі кластери усіх покриваючих файлів до неї. А отже $O\left(m\left(n\right)\right)=n\times Cluster_{size}$, що означає, що може виникнути ситуація, коли операція перестановки не може бути виконана взагалі. Але як висновок необхідно буде перезаписати усі кластери, а отже загальна обчислювальна складність матиме вигляд

$$O\left(B\right)=O\left(f\left(2n\right)\right)+O\left(g\left(n\right)\right)+O\left(h\left(n\right)\right);n=C_{len}, \quad (2)$$

де C_{len} – довжина матриці стану у кластерах, тобто загальний розмір покриваючих файлів у кластерах. Подвійне переміщення зчитуючої головки як раз і пов'язане із тим, що необхідно спочатку зчитати усі кластери, а потім записати усі кластери.

Для даного прикладу матимемо такі показники, що зазначені у табл. 1, де $\varphi(F_i)$ означає кількість фрагментів та рівень фрагментації (відстань між фрагментами), відповідно, а π – правило перестановки:

Таблиця 1

Показники результату приховування прикладу шляхом ПЗОП

π	(4,7,16,18,22,6,12,17,5,11)(23)(24)
$O(f(n))$	20
$O(g(n))$	10
$O(h(n))$	10
$O(m(n))$	10
$\varphi(F_0)$	1
$\varphi(F_1)$	2 (6)
$\varphi(F_2)$	2 (7)
$\varphi(F_3)$	2 (7)

ПчЗОП-І

Виконання перестановки із почерговим завантаженням кластерів до оперативної пам'яті із впорядкованим розміщенням залишку кластерів, рис. 2. Далі даний метод називатимемо почерговим завантаженням до оперативної пам'яті ПчЗОП-І.

Особливість даного методу полягає у тому, що перестановка виконується почергово по ланцюгу кластерів, тобто на першій ітерації зчитується перший кластер ланцюгу, у наступній ітерації зчитується кластер, на який слідом перезаписуємо попередньо зчитаний кластер. Таким чином зростає кількість переміщень зчитуючої головки пристрою, так як доводиться "стрибати" назад та вперед по кластерах. Це означає, що кількість переміщень може бути максимум сумою чисел до числа n, де n – кількість кластерів, а отже $O(f(n^2))$, тобто складність має квадратичний характер. І так як усе одно виконується впорядкований перезапис подальших кластерів, то обчислювальна складність буде дорівнювати

$$O(B) = O(f(n^2)), +O(g(n)) + O(h(n)); n = C_{len} \quad (3)$$

де C_{len} – довжина матриці стану у кластерах, тобто загальний розмір покриваючих файлів у кластерах. Причому можуть виникати умови, коли кластер перезаписується сам у себе; у такому випадку виконувати перезапис кластеру не є необхідним. Також необхідно зазначити, що при виконанні перестановки методом ПчЗОП-І обчислювальна система потребує лише подвійного розміру кластеру у якості оперативної пам'яті, тобто $O(m(const)) = 2$, що дозволяє виконувати приховування інформації теоретично у необмежені за розміром покриваючі файли. Для даного прикладу матимемо такі показники, що зазначені у табл. 2.

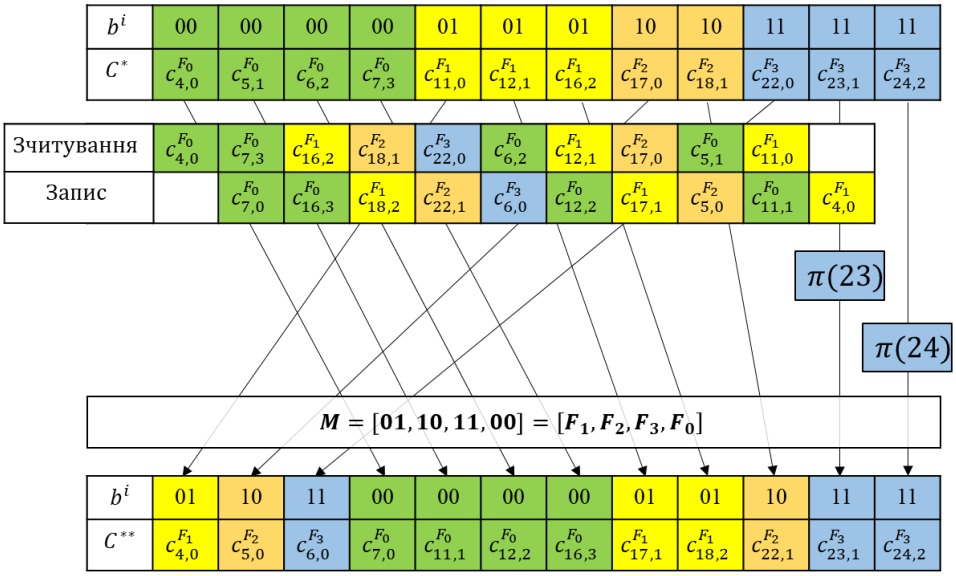


Рис. 2. Приклад перестановки кластерів із почерговим завантаженням кластерів ПчЗОП-І

Таблиця 2

Показники результату приховування прикладу шляхом ПчЗОП-І

π	(4,7,16,18,22,6,12,17,5,11)(23)(24)
$O\left(f\left(n^2\right)\right)$	34
$O\left(g\left(n\right)\right)$	10
$O\left(h\left(n\right)\right)$	10
$O\left(m\left(const\right)\right)$	2
$\varphi\left(F_0\right)$	1
$\varphi\left(F_1\right)$	2 (6)
$\varphi\left(F_2\right)$	2 (7)
$\varphi\left(F_3\right)$	2 (7)

ПчЗОП-ІІ

Виконання перестановки із почерговим завантаженням кластерів до оперативної пам'яті із переміщенням лише інформативних кластерів у нормальну послідовність, рис. 3. Далі даний метод називатимемо почерговим завантаженням до оперативної пам'яті ПчЗОП-ІІ.

Особливість даного способу приховування інформацій полягає у тому, що при розрахунку остаточної матриці стану кластерів перемішування виконується лише над кластерами, які безпосередньо беруть участь у приховуванні інформаційного повідомленні. Можуть переміщуватися неінформаційні кластері лише у випадку, коли їх заміщують інформаційні кластери. Наступним кроком є розміщення переміщених кластерів у нормальній послідовності, тобто кластери одного файлу повинні мати індекси, що зростають зліва направо, тобто не мати переплетеності між кластерами. Це дозволяє зменшити рівень фрагментації для можливо переплетених покриваючих файлів.

У даному випадку кількість переміщень зчитуючої головки та кількість зчитувань та записів кластерів вже залежить від кількості стеганоблоків – k, а не лише від кількості кластерів покриваючих файлів – n. У той час оперативній пам'яті необхідно так само лише подвійний розмір кластеру.

Для того щоб виконати перестановку, необхідно перемістити лише k кластерів, які можуть замістити собою ще k кластерів. Дані кластери можуть розміщуватися по усій довжині

матриці стану, тобто переміщення зчитуючої головки для переміщення одного кластеру може бути із крайньої лівої позиції до крайньої правої, тобто необхідно пройтись по усіх кластерах – n. А отже кількість переміщень зчитуючої головки дорівнює – $O\left(f\left(2kn\right)\right)$. Причому, якщо розмір повідомлення у стеганоблоках наближається до кількості кластерів, то обчислювальна складність переміщень зчитуючої головки наближається до квадратичної залежності – $O\left(f\left(n^2\right)\right); k \to n$.

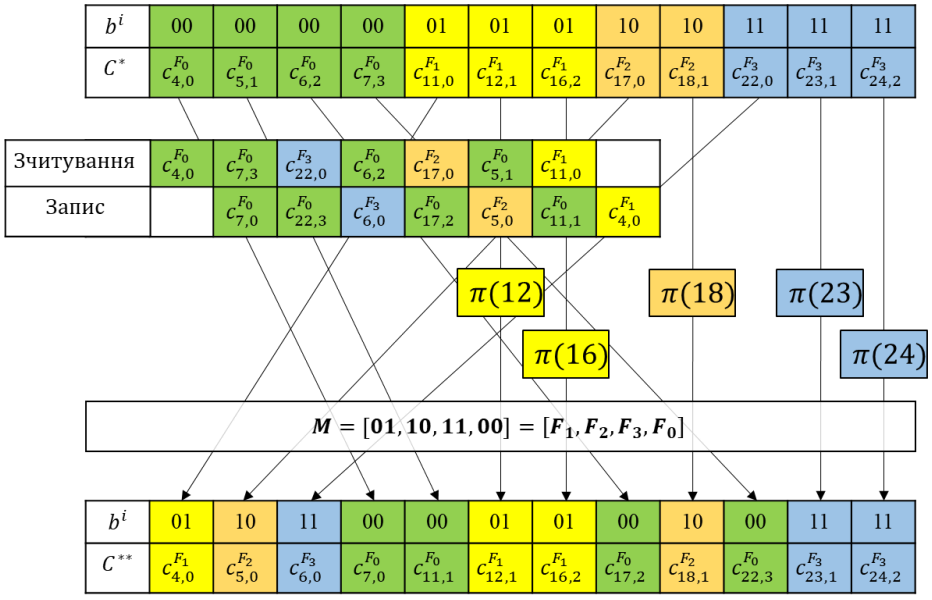


Рис. 3. Приклад перестановки кластерів із почерговим завантаженням кластерів ПчЗОП-II

Кількість зчитувань та записів кластерів фіксована та залежить лише від кількості стеганоблоків, але таких записів може бути по два, коли інформаційний кластер заміщує не інформаційній. А отже $O\left(g\left(2k\right)\right)$ та $O\left(h\left(2k\right)\right)$. Результуюча обчислювальна складність

$$O(B) = O\left(f\left(2kn\right)\right) + O\left(g\left(2k\right)\right) + O\left(h\left(2k\right)\right); n = C_{len}; k = M_{len}. \quad (4)$$

Так як не виконується подальше перерозміщення неінформативних кластерів у суцільні послідовності, то зазвичай рівень фрагментації покриваючих файлів при перерозміщенні у такий спосіб буде вищий, аніж при виконанні методу приховування інформації шляхом ПчЗОП-I. Для даного прикладу матимемо показники, що зазначені у табл. 3.

Таблиця 3

Показники результату приховування прикладу шляхом ПчЗОП-II

π	(4,7,22,6,17,5,11)(12)(16)(18)(23)(24)
$O\left(f\left(n^2\right)\right)$	34
$O\left(g\left(2k\right)\right)$	8
$O\left(h\left(2k\right)\right)$	8
$O\left(m\left(const\right)\right)$	2
$\varphi\left(F_0\right)$	3 (3)
$\varphi\left(F_1\right)$	2 (4)
$\varphi\left(F_2\right)$	2 (6)
$\varphi\left(F_3\right)$	2 (7)

ПчЗОП-III

Виконання перестановки із почерговим завантаженням кластерів до оперативної пам'яті із оптимальним переміщенням лише інформативних кластерів, рис. 4. Далі даний метод називатимемо почерговим завантаженням до оперативної пам'яті ПчЗОП-III.

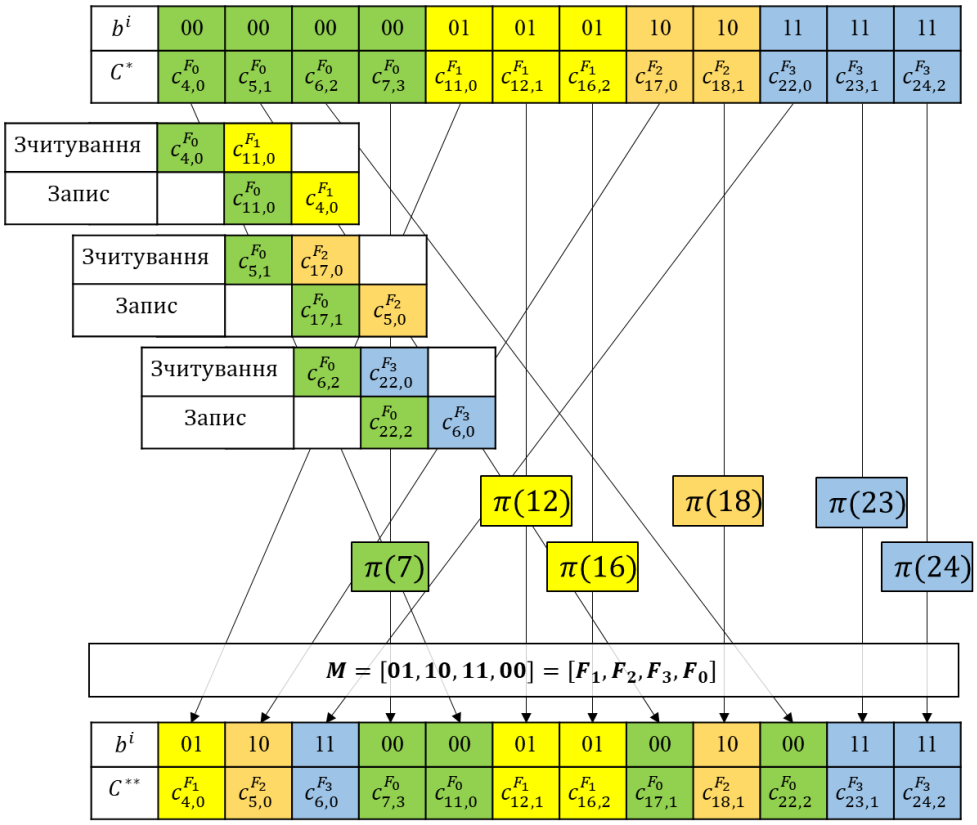


Рис. 4. Приклад перестановки кластерів із почерговим завантаженням кластерів ПчЗОП-III

Особливість даного способу приховування інформацій полягає у тому, що при розрахунку остаточної матриці стану кластерів перемішування виконується лише над кластерами, які безпосередньо беруть участь у приховуванні інформаційного повідомленні, але кластер файлу у початковому стані співпадає із кластером файлу у кінцевому стані, то такий кластер не переміщується. Така особливість може призвести до зростання переплетеності покриваючих файлів, що збільшить рівень фрагментації. Але така особливість надає перевагу, так як зменшиться кількість переміщень та перезаписів у порівнянні із способом ПчЗОП-II. Можуть переміщуватися неінформаційні кластері лише у випадку, коли їх заміщають інформаційні кластери. Також така особливість (ПчЗОП-III) має сенс, якщо використовується модифікований метод приховування інформації, так як він за визначенням призведе до зростання переплетеності.

У даному випадку кількість переміщень зчитуючої головки та кількість зчитувань та записів кластерів вже залежить від кількості стеганоблоків – k, а не лише від кількості кластерів покриваючих файлів – n. У той час оперативній пам'яті необхідно так само лише подвійний розмір кластеру.

Для того щоб виконати перестановку, необхідно перемістити лише k кластерів, які можуть замістити собою ще k кластерів. Дані кластери можуть розміщуватися по усій довжині матриці стану, тобто переміщення зчитуючої головки для переміщення одного кластеру може бути із крайньої лівої позиції до крайньої правої, тобто необхідно пройтись по усіх кластерах – n. Отже, кількість переміщень зчитуючої головки дорівнює – $O\left(f\left(2kn\right)\right)$. Причому, якщо розмір повідомлення у стеганоблоках наближається до кількості кластерів, то обчис-

лювальна складність переміщень зчитуючої головки наближається до квадратичної залежності – $O\left(f\left(n^2\right)\right); k \to n$.

Кількість зчитувань та записів кластерів фіксована та залежить лише від кількості стеганоблоків, але таких записів може бути по два, коли інформаційний кластер заміщує неінформаційній. Але можливі випадки, коли деякі кластері можна не перезаписувати, як описано вище. А отже $O\left(g\left(2k\right)\right)^{-}$ та $O\left(h\left(2k\right)\right)^{-}$. Результуюча обчислювальна складність матиме вигляд

$$O(B) = O\left(f\left(2kn\right)\right) + O\left(g\left(2k\right)\right)^{-} + O\left(h\left(2k\right)\right)^{-}; n = C_{len}; k = M_{len} \quad (5)$$

Так як не виконується подальше перерозміщення неінформативних кластерів у суцільні послідовності, то, зазвичай, рівень фрагментації покриваючих файлів при перерозміщенні у такий спосіб буде вищий, аніж при виконанні методу приховування інформації шляхом ПчЗОП-І, та через можливу переплетеність деяких файлів рівень фрагментації буде вищий за рівень фрагментації при виконанні приховування повідомлення шляхом ПчЗОП-ІІ. Але для систем, де рівень фрагментації покриваючих файлів не є значним показником, то приховування повідомлення шляхом перемішування кластерів покриваючих файлів спосіб виконання перестановки із почерговим завантаженням кластерів до оперативної пам'яті із оптимальним переміщенням лише інформативних кластерів є оптимальним. Для даного прикладу матимемо показники, що зазначені у табл. 4.

Таблиця 4.

Показники результату приховування прикладу шляхом ПчЗОП-ІІІ

π	(4,11)(5,17)(6,22)(7)(12)(16)(18)(23)(24)
$O\left(f\left(n^2\right)\right)$	36
$O\left(g\left(2k\right)\right)^{-}$	6
$O\left(h\left(2k\right)\right)^{-}$	6
$O\left(m\left(const\right)\right)$	2
$\varphi\left(F_0\right)$	4 (8)
$\varphi\left(F_1\right)$	2 (4)
$\varphi\left(F_2\right)$	2 (6)
$\varphi\left(F_3\right)$	2 (7)

Висновки

Порівняємо дані способи реалізації базового методу приховування інформації шляхом перемішування кластерів покриваючих файлів за такими показниками:

– обчислювальна складність за необхідним об'ємом вільного місця у оперативній пам'яті – $O(m)$;

– обчислювальна складність за часовими показниками – $O(f)$, $O(g)$, $O(h)$;

– захищеність від детектування, тобто за впливом на рівень фрагментації.

Порівнюючи способи реалізації за обчислювальною складністю за часовими показниками, необхідно зазначити, що переміщення зчитуючої головки пристрою займає найменше часу у абсолютних величинах. А запис кластеру займає найбільше часу. Тобто, затрачений час підпорядковується такій закономірності:

$$O(f) < O(g) < O(h) \quad (6)$$

Причому, для SSD технології час, затрачений на переміщення зчитуючої головки, наближається до нуля, так як у SSD пристроях реалізована паралельна обробка секторів, та таке визначення, як зчитуюча головка пристрою, не має сенсу. Отже, результат порівняльного аналізу способів реалізації методу зазначено у табл. 5.

Таблиця 5

Результат порівняльного аналізу способів реалізації базового методу приховування інформації

Спосіб реалізації	Необхідний об'єм ОП	Необхідний час	Захищеність від детектування
ПЗОП	--	-	++
ПчЗОП-I	++	--	++
ПчЗОП-II	++	+	+
ПчЗОП-III	++	++	-

Також відповідні результати отримано і для модифікованого методу приховування даних у структуру файлової системи за способами приховування ПЗОПм, ПчЗОП-I/II/IIIм (дані способи відповідають описаним вище способам використання базового методу).

Роблячи висновок за результатами порівняльного аналізу, можна стверджувати:

– для систем, де розмір оперативної пам'яті є достатнім (розмір покриваючих файлів цілком уміщається у оперативну пам'ять), переважним способом буде ПЗОП. Даний спосіб дозволяє досягти мінімального впливу на рівень фрагментації покриваючих файлів, але ПЗОП потребує значного часу на виконання приховування повідомлення;

– для систем, де затрачений час є критичним параметром, рекомендується використовувати способи ПчЗОП-II та ПчЗОП-III. ПчЗОП-III потребує менше часу на приховування повідомлення, але вплив на рівень фрагментації у такий спосіб найбільший;

– для систем, у яких захищеність від детектування є критичним параметром, рекомендовано використовувати способи ПЗОП та ПчЗОП-I (у залежності від доступного об'єму ОП).

Окремо можна виділити ПчЗОП-II як найоптимальніший спосіб через те, що даний спосіб дозволяє досягти задовільних показників при приховуванні повідомлення без збитку у інших показниках.

Також необхідно зазначити, якщо для приховування повідомлення буде задіяно значну кількість кластерів покриваючих файлів (тобто кількість стеганоблоків до кількості кластерів), то часові переваги способів ПчЗОП-II та ПчЗОП-III нівелюються. У такому випадку бажано використовувати ПЗОП та ПчЗОП-I у залежності від допустимого об'єму ОП.

Відповідно до отриманих досліджень було розроблено програмну реалізацію симуляції (https://github.com/ShekhaninKyryl/SteganoSimulation), яка дозволяє емпіричним шляхом оцінити обчислювальну складність методів приховування.

Узагальнюючи результати, отримані емпіричним шляхом, можна зробити наступний висновок. Для способів приховування інформації базовим методом емпірично отримана обчислювальна складність відповідає теоретично розрахованій. Особливо необхідно виділити способи ПчЗОП-II та ПчЗОП-III, так як кількість перезаписаних кластерів значно нижча, ніж при використанні ПЗОП та ПчЗОП-I. Але з іншого боку, практично отримана обчислювальна складність способів приховування інформації модифікованим методом неповністю відповідає теоретично розрахованій. А саме при використанні ПчЗОП-II/IIIм кількість зчитаних та записаних кластерів залежить від кількості кластерів покриваючих файлів – n, а не від кількості стеганоблоків – k. Частково це можна вирішити, імплементувавши вдосконалену функцію приховування модифікованої компоненти стеганоблоку. Для цього при розрахунку та перемішуванні кластерів у відповідності до базової компоненти треба помічати кластери, які не були переміщені, та за можливістю зберігати їх позиції при виконанні перемішування кластерів за допомогою модифікованої компоненти. Також необхідно виконувати такий

алгоритм рекурсивно – якщо на поточній ітерації приховати необхідне повідомлення неможливо із збереженням позицій усіх кластерів, які необхідно зберегти, то необхідно знехтувати одним таким кластером та знову спробувати приховати повідомлення. І так далі, до поки не вийде приховати усю необхідно інформацію. Узагальнююча оцінка обчислювальної складності показана у табл. 6.

Таблиця 6

Порівняння теоретично розрахованої обчислювальної складності із емпірично отриманою при використанні різних способів

Параметр ОС (теоретичне / емпіричне)	$O(f)$	$O(g)$	$O(h)$	$O(m)$
ПЗОП	$O(f(n))$ / $O(f(n))$	$O(g(n))$ / $O(g(n))$	$O(h(n))$ / $O(h(n))$	$O(m(n))$ / $O(m(n))$
ПчЗОП-I	$O(f(n^2))$ / $O(f(n^2))$	$O(g(n))$ / $O(g(n))$	$O(h(n))$ / $O(h(n))$	$O(m(2)$ / $O(m(2)$
ПчЗОП-II	$O(f(n^2))$ / $O(f(n^2))$	$O(g(2k))$ / $O(g(2k))$	$O(g(2k))$ / $O(g(2k))$	$O(m(2))$ / $O(m(2))$
ПчЗОП-III	$O(f(n^2))$ / $O(f(n^2))$	$O(g(2k))^-$ / $O(g(2k))^-$	$O(h(2k))^-$ / $O(h(2k))^-$	$O(m(2))$ / $O(m(2))$
ПЗОПм	$O(f(n))$ / $O(f(n))$	$O(g(n))$ / $O(g(n))$	$O(h(n))$ / $O(h(n))$	$O(m(n))$ / $O(m(n))$
ПчЗОП-Ім	$O(f(n^2))$ / $O(f(n^2))$	$O(g(n))$ / $O(g(n))$	$O(h(n))$ / $O(h(n))$	$O(m(2)$ / $O(m(2)$
ПчЗОП-IIм	$O(f(n^2))$ / $O(f(n^2))$	$O(g(2k))$ / $O(g(n))$	$O(g(2k))$ / $O(g(n))$	$O(m(2))$ / $O(m(2))$
ПчЗОП-IIIм	$O(f(n^2))$ / $O(f(n^2))$	$O(g(2k))^-$ / $O(g(n))$	$O(h(2k))^-$ / $O(g(n))$	$O(m(2))$ / $O(m(2))$

Список літератури:

1. Kuznetsov A. and others. Method of 3D-steganography // CS&CS E-journal. 2018. № 4. С. 4–12.
2. Kuznetsov A. and others. Information Hiding Using 3D-Printing Technology // 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). 2019a. С. 701–706.
3. Kuznetsov A. A. and others. 3D STEGANOGRAPHY INFORMATION HIDING // TRE. 2019b. Т. 78. № 12.
4. Mazurczyk W., Szczypiorski K. Steganography of VoIP Streams // arXiv:0805.2938 [cs]. 2008.
5. Fraczek W., Mazurczyk W., Szczypiorski K. Stream Control Transmission Protocol Steganography // 2010 International Conference on Multimedia Information Networking and Security. 2010. С. 829–834.
6. Fraczek W., Mazurczyk W., Szczypiorski K. How Hidden Can be Even More Hidden? // 2011 Third International Conference on Multimedia Information Networking and Security, 2011. С. 581–585.
7. Szczypiorski K. HICCUPS: Hidden communication system for corrupted networks // 2003.
8. Khan H. and others. Designing a cluster-based covert channel to evade disk investigation and forensics // Computers & Security. 2011. Т. 30. № 1. С. 35–49.
9. Khan H. and others. Evading Disk Investigation and Forensics using a Cluster-Based Covert Channel // 2012.

10. Venčkauskas A. and others. Covert Channel for Cluster-based File Systems Using Multiple Cover Files // Information Technology and Control. 2013. Т. 42. № 3. С. 260-267.

11. Shekhanin K.Yu., Kolhatin A.O., Demenko E.E., Kuznetsov A.A. On hiding data into the structure of the FAT family file systemy. Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika): Volume 78, Issue 11, 2019, Pages 973-985. https://www.scopus.com/record/display.uri?eid=2-s2.0-85070406462&origin=inward.

12. Shekhanin K., Kuznetsov A., Krasnobayev V., Smirnov, O: Detecting hidden information in FAT // International Journal of Computer Network and Information Security: Vol. 12, Issue 3, June 2020. P. 33-43. https://www.scopus.com/record/display.uri?eid=2-s2.0-85086029655&origin=inward

13. Kuznetsov A., Shekhanin K., Kolhatin, A., Mikheev I., Belozertsev I. Hiding data in the structure of the FAT family file system // Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018. 9 July 2018, Pages 337-342 https://www.scopus.com/record/display.uri?eid=2-s2.0-85050684345&origin=inward

14. Shekhanin K., Kolhatin A., Kuznetsova K., Kavun S. Steganographic hiding information in a file system structure // 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2018 // Proceeding. September 2018, P. 9047551. https://www.scopus.com/record/display.uri?eid=2-s2.0-85083488842&origin=inward

Надійшла до редколегії 15.09.2021

Відомості про авторів:

Кузнецов Олександр Олександрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, кафедра безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: kuznetsov@karazin.ua, ORCID:https://orcid.org/0000-0003-2331-6326

Шеханін Кирил Юрійович – аспірант, Харківський національний університет імені В.Н. Каразіна, кафедра безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: kyryl.shekhanin@karazin.ua, ORCID: https://orcid.org/0000-0002-1441-7814

Пшенична Світлана Вікторівна – старший науковий співробітник, Харківський національний університет імені В.Н. Каразіна, факультет радіофізики, біомедичної електроніки та комп`ютерних систем; Україна; e-mail: kyryl.shekhanin@karazin.ua, ORCID: https://orcid.org/0000-0002-6212-7280

УДК 004.056 **DOI:10.30837/rt.2021.3.206.08**

В.В. ВИЛИГУРА, В.И. ЕСИН, д-р техн. наук

МОДЕЛЬ ЗАЩИТЫ БАЗЫ ДАННЫХ НА ОСНОВЕ СИСТЕМЫ БЕЗОПАСНОСТИ С ПОЛНЫМ ПЕРЕКРЫТИЕМ

Введение

Безопасность (защищенность) является одной из важнейших характеристик качества [1] информационных систем (ИС) в целом и баз данных (БД) как их основной составляющей, в частности. Наличие системы защиты информации как комплекса программных, технических, криптографических, организационных и иных методов, средств и мероприятий, обеспечивающих целостность, конфиденциальность, аутентичность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера, является неотъемлемой чертой любой современной ИС, БД. При этом высокая степень безопасности данных должна быть обеспечена без снижения функциональности ИС, БД и практически без усложнения работы пользователя в системе [2]. Вместе с тем, чтобы можно было проверить выводы о степени обеспечения безопасности, ее необходимо каким-либо образом измерить. При этом известно [3], что обеспечить безопасность информационной системы легче, если есть четкая модель того, что нужно защищать и кому и что разрешено делать.

Поэтому, после анализа и обобщения различных подходов и достижений в области оценки безопасности информационных систем в целом и баз данных в частности было принято решение в качестве модели защиты БД, и оценки ее безопасности использовать модель Клементса – Хоффмана [4, 5], опирающуюся на теорию графов, нечетких множеств, вероятностей, и традиционно считающуюся основой формального описания систем защиты.

Формализация задачи обеспечения безопасности баз данных

Основным положением *модели системы безопасности с полным перекрытием* (модель Клементса – Хоффмана) является тезис о том, что система, спроектированная на ее основе, должна иметь, по крайней мере, одну меру (механизм, метод, средство) для обеспечения безопасности на каждом возможном пути проникновения в систему. В модели рассматривается взаимодействие «области угроз», «защищаемой области» и «системы защиты». Считается, что несанкционированный доступ (как любой доступ, нарушающий заявленную политику безопасности [6]) к каждому из набора объектов O защищаемой области сопряжен с некоторой величиной ущерба, который может быть определен количественно (в противном случае его полагают равным некоторой условной величине). При этом количественная категория ущерба может быть выражена в стоимостном эквиваленте (сумма финансовых потерь), либо в терминах, связанных с целевой функцией системы (например, времени, необходимом для восстановления функциональных возможностей ИС в целом, и БД в частности, после злоумышленного воздействия) [7].

Для описания системы безопасности с полным перекрытием применительно к базам данным введем следующие обозначения:

– $T=\{t_i\}$, $i=1..I$ – множество угроз безопасности БД. Для формирования набора угроз, направленных на нарушение безопасности, по возможности, определяются все потенциальные злоумышленные действия по отношению ко всем объектам безопасности;

– $O=\{o_j\}$, $j=1..J$ – множество защищаемых объектов БД;

– $W=\{w_k\}$, $k=1..K$ – множество мер обеспечения безопасности (в том числе, методов, средств, механизмов, обеспечивающих реализацию политик безопасности, формальным представлением которых являются модели безопасности, методов и примитивов для защиты информации БД, основанных на криптографии).

Элементы всех перечисленных множеств находятся между собой в определенных отношениях, причем связь между угрозами и объектами не является связью «один к одному». Угроза $t_i \in T$ может распространяться на любое число объектов O, а объект $o_j \in O$ может быть уязвим со стороны более чем одной угрозы T. Для лучшего понимания систему защиты в рамках данной формализации целесообразно представить двухдольным графом (рис. 1), в котором множество отношений «угроза – объект» представляется в виде дуг (t_i, o_j), существующих только тогда, когда t_i является угрозой, направленной на нарушение безопасности объекта $o_j \in O$.

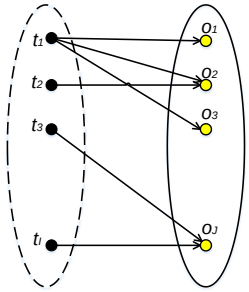


Рис. 1. Представление отношения «объект – угроза»

Защита обеспечивается путем перекрытия всех возможных дуг графа, за счет создания соответствующего барьера (средства обеспечения безопасности $w_k \in W$) на каждом пути. В результате двухдольный граф преобразуется в трехдольный (рис. 2).

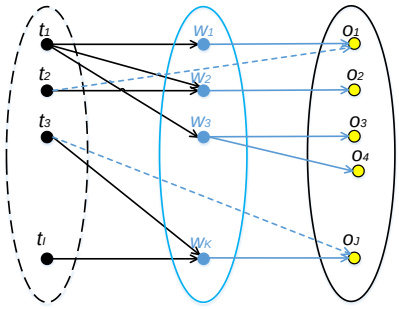


Рис. 2. Представление отношений между угрозами, средствами обеспечения безопасности и объектами

В защищенной системе все дуги модели представляются в виде (t_i, w_k) и (w_k, o_j). Любая дуга (t_i, o_j) определяет незащищенный объект (дуги (t_2, o_1) и (t_3, o_J) на рис. 2). При этом следует заметить, что одно и то же средство обеспечения безопасности может перекрывать более одной угрозы и/или защищать более одного объекта.

В дальнейшем для построения модели воспользуемся так называемой базовой системой обеспечения безопасности Клементса, описанной в работах [4, 5], в виде 5-мерного кортежа (пятерки): $S = \{O, T, W, V, B\}$, которая предполагает включение набора уязвимостей V (представляющих собой пути реализации угроз T в отношении объектов O), определяемого подмножеством декартова произведения $V = T \times O$ (набором упорядоченных пар $v_r = (t_i, o_j)$, $r = 1..R$) и набора барьеров (представляющих собой точки, в которых требуется осуществлять защиту) B, определяемого подмножеством декартова произведения $B = V \times W = T \times O \times W = \{b_l = (t_i, o_j, w_k),\ l = 1..\Lambda\}$ как отображение $T \times O \times W$ на набор упорядоченных троек $b_l = (t_i, o_j, w_k)$.

Для данной модели условие полного перекрытия можно записать в следующем виде: $\forall (v_r = (t_i, o_j)) \in V$, $\exists (b_l = (t_i, o_j, w_k)) \in B$. Это условие означает, что для каждого пути реали-

зации угроз T в отношении объектов O средством безопасности $w_k \in W$ создается барьер $b_l \in B$, устраняющий эту угрозу для конкретного объекта.

В идеале каждый механизм защиты (меры безопасности) должен исключать соответствующий путь реализации угрозы. На практике эти механизмы обеспечивают лишь некоторую степень сопротивляемости угрозам безопасности (например, пароли имеют конечную длину; шифры имеют различную криптографическую стойкость; различная частота точек синхронизации между базой данных и журналом транзакций приводит к всевозможным, иногда неприемлемым, временам восстановления при сбоях, отказах; зависимость защищенности от актуальности и своевременности устанавливаемых параметров конфигурации и т. д.).

Показатель защищенности базы данных

Чтобы иметь некоторую количественную оценку уровня защищенности объектов, авторы модели системы безопасности с полным перекрытием [4, 5] считают, что можно измерить степень обеспечения безопасности системы. В качестве подходящей структуры для выражения таких мер они предлагают лингвистическую переменную, которая принимает значения в виде слов, а не чисел. Для этого они переопределяют барьеры безопасности B, каждый из которых ($b_l \in B$) представляют в виде составной лингвистической переменной, компонентами которой являются лингвистические переменные: P_l – вероятность возникновения угрозы; L_l – величина ущерба при успешной реализации угрозы в отношении защищаемого объекта; R_l – степень сопротивляемости средства защиты w_k, характеризующаяся вероятностью его преодоления. При этом отмечается, что эти компоненты оцениваются в контексте специфического барьера ($b_l = (t_i, o_j, w_k)$), который они формируют (индексы у P_l, L_l, R_l такие же, как индекс барьера, а не такие, как у компонентов барьера $b_l = (t_i, o_j, w_k)$ в базовой системе защиты – угрозы, объекты и средства защиты). Авторы поясняют, что значение сопротивляемости определяет степень повышения или снижения общей безопасности системы, а неформальная комбинация вероятности и величины потерь дает важность (вес) барьера в сводном рейтинге (оценке), и в целом эти значения определяют вклад барьера в общую безопасность системы. При этом они ничего не говорят о конкретных способах их получения (оценивания), а также о существовании, виде и использовании интегрального показателя, позволяющего оценивать защищенность объектов и системы в целом. Поэтому, после анализа различных подходов, изложенные в релевантных источниках [8 – 10], в качестве такого показателя был выбран остаточный риск Rr, связанный с возможностью реализации угрозы $t_i \in T$ в отношении объекта БД $o_j \in O$ при использовании средства обеспечения безопасности $w_k \in W$. Величину остаточного риска, характеризующего стойкость (прочность) барьера $b_l \in B$, можно определить следующим образом [8, 9]:

$$Rr_l = P_l L_l (1 - R_l). \tag{1}$$

Остаточный риск, по сути, является мерой незащищенности актива. Тогда величину защищенности БД можно определить путем вычисления обратной величины суммарного остаточного риска подобно [8, 9]:

$$S = \sum_{\forall b_l \in B} \frac{1}{P_l L_l (1 - R_l)}, \tag{2}$$

где $P_l, L_l \in (0,1)$, $R_l \in [0,1)$.

При отсутствии в системе барьеров b_l, перекрывающих определенные пути реализации угроз в отношении объектов, степень сопротивляемости механизма защиты R_l принимается равной нулю. С формальной стороны это можно представить путем ввода так называемого средства защиты с нулевой степенью обеспечения безопасности (w_o), добавляемого ко множеству W [4, 5]. Каждому незащищенному объекту приписывается такое средство. Таким образом, для $\forall(t_i, o_j) \in V$, для которого $(\forall k \in K)\ (t_i, o_j, w_k) \notin B$, к B добавляется барьер (t_i, o_j, w_o).

Особенности предлагаемой модели защиты БД

Следует отметить еще одну особенность рассматриваемой модели. Авторы [5], вводя понятие уязвимости (англ. vulnerability), формально представляют его как отображение $T \times O$ на набор упорядоченных пар $v_r = (t_i, o_j)$, а не отдельно объективно существующую категорию уязвимости как слабого места актива или средства управления, которое может быть использовано одной или более угрозой [11]. Угрозы существуют отдельно от слабых мест актива. Уязвимость сама по себе не наносит ущерба, это только условие или набор условий, позволяющих угрозе причинить ущерб активам. При реализации угрозы может использоваться одна или более уязвимостей актива [12]. При этом один тип уязвимости может привести к множеству угроз безопасности различной направленности. Поэтому угрозы и уязвимости целесообразно рассматривать в комплексе. Только вместе они могут стать причиной нежелательного инцидента, который может причинить вред системе (активам). И в этом случае необходимо четко определить угрозы, уязвимости и взаимосвязь между ними.

В связи с этим расширим представленную выше модель с полным перекрытием до 6-мерного кортежа (шестерки) за счет включения множества уязвимостей (слабых мест) объектов (Γ):

$$S' = \{O, T, \Gamma, W, V, B\}. \tag{3}$$

Тогда после соответствующего уточнения модели под набором V будем понимать множество упорядоченных троек $v_r = (t_i, \gamma_\psi, o_j)$, $\psi = 1..\Psi$, где $\gamma_\psi \in \Gamma$ – уязвимость (как некоторый ее тип), используемая угрозой $t_i \in T$, направленной на нарушение безопасности объекта $o_j \in O$. Набор барьеров будет соответственно определяться как: $B = V \times W = T \times \Gamma \times O \times W = \{b_l = (t_i, \gamma_\psi, o_j, w_k),\ l = 1..L\}$. А условие обеспечения полной защищенности для данной модели примет следующий вид: $\forall(v_r)$, $\exists(b_l = (t_i, \gamma_\psi, o_j, w_k)) \in B$. Это условие означает, что для каждой тройки (t_i, γ_ψ, o_j) из множества V создается барьер $b_l \in B$, что делает невозможным реализацию нежелательного инцидента (реализацию угрозы $t_i \in T$, использующей уязвимость $\gamma_\psi \in \Gamma$) в отношении объекта защиты $o_j \in O$.

Средство защиты с нулевой степенью обеспечения безопасности (w_o), добавляемое к множеству W и приписываемое к незащищенному объекту, формально можно выразить следующим образом: для $\forall(t_i, \gamma_\psi, o_j) \in V$, для которого $(\forall k \in K)\ (t_i, \gamma_\psi, o_j, w_k) \notin B$, к B добавляется барьер $(t_i, \gamma_\psi, o_j, w_o)$.

Соответственно в выражениях (1), (2) под вероятностью P_l будет пониматься вероятность нежелательного инцидента (реализации угрозы) как произведение вероятности возникновения угрозы P_{t_i} на вероятность использования (удачного) уязвимости P_{γ_ψ}: $P_l = P_{t_i} \cdot P_{\gamma_\psi}$ [10, 13]. То есть в данном случае используется так называемая двухфакторная

модель оценки вероятности [14], выделяющая два компонента (фактора), один из которых отображает мотивационную составляющую возникновения угрозы, а второй учитывает существующие уязвимости. Величину ущерба L_l в отношении защищаемого объекта следует рассматривать с позиции успешной реализации угрозы t_i, использующей уязвимость γ_ψ.

Исходя из сказанного, для описания системы безопасности с полным перекрытием применительно к базам данным конкретизируем элементы множеств защищаемых объектов БД, угроз и уязвимостей, характерных для БД, мер (средств контроля) обеспечения безопасности. А именно, определим объекты защиты БД $o_j \in O$ с характерным для них списком угроз $t_i \in T$ и уязвимостей $\gamma_\psi \in \Gamma$, благодаря которым становится возможной реализация соответствующей угрозы, а также идентифицируем реализованные средства/меры обеспечения безопасности $w_k \in W$.

Учитывая, что системы БД являются информационными продуктами с двойственной природой – двумя компонентами (активами) в виде программных средств СУБД, независимых от сферы их применения, структуры, смыслового содержания накапливаемых и обрабатываемых данных и собственно хранимых данных, возможность вредоносного воздействия на эти активы, целесообразным является обеспечение безопасности их обоих. Для реляционных БД, как получивших наибольшее распространение (этот тезис подтверждают результаты DB-Engines и PYPL рейтингов [15, 16], а также отчеты экспертов всемирно известной компании Gartner, Inc. [17, 18]), с учетом возможности различной степени детализации этих компонент можно выделить следующие объекты защиты [19, 20]:

– базу данных в целом – o_1;

– таблицы – o_2;

– представления (views) – o_3;

– картежи (строки) таблиц – o_4;

– отдельные поля (значения атрибутов) строк – o_5;

– триггеры – o_6;

– постоянно хранимые модули – o_7 и некоторые другие.

Основными наиболее крупными и важными угрозами (типами угроз) безопасности баз данных, носителями которых являются различные источники угроз (в большей мере нас будут интересовать антропогенные – люди или группы лиц, в результате действий либо бездействия которых произошло нарушение безопасности рассматриваемой системы [21], в том числе с возможными сценариями действий злоумышленников (на примере СУБД Oracle), представленными на рис. 3), согласно [19, 22 – 27] являются:

– чрезмерные и неиспользуемые привилегии. Для определенности обозначим этот тип угрозы как t_1;

– злоупотребление законными привилегиями – t_2;

– инъекции ввода – t_3;

– вредоносное программное обеспечение – t_4;

– недостаточность мер по аудиту данных (слабые аудиторские следы) – t_5;

– незащищенность носителей (резервных копий) информации – t_6;

– эксплуатация уязвимых, неверно сконфигурированных баз данных – t_7;

– неуправляемые конфиденциальные данные – t_8;

– логический вывод – t_9;

– отказ в обслуживании – t_{10};

– недостаток знания и опыта в вопросах информационной безопасности – t_{11} и некоторые другие.

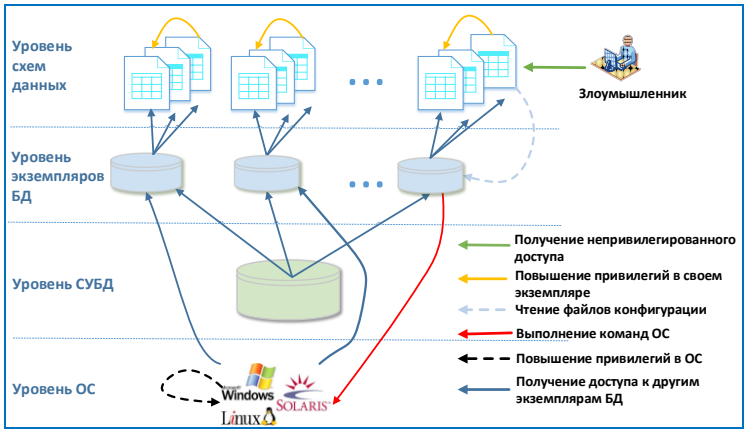


Рис. 3. Схема возможных действий злоумышленника

На основе анализа существующих таксономий уязвимостей, имеющих отношение к конкретному экземпляру продукта или системы (а не к основным недостаткам), которые могут быть непосредственно использованы злоумышленником для реализации угроз безопасности [28], общих слабых мест (англ. weakness) программного и аппаратного обеспечения, которые могут привести к возникновению уязвимостей [29, 30], а также некоторых других классификаций уязвимостей и недостатков безопасности активов [21, 31, 32] был определен перечень основных общих слабых мест (недостатков) как некоторых типов уязвимостей. За основу взята спецификация из Common Weakness Enumeration (CWE), точнее, классификация абстрактного представления Концепции исследования (Research Concepts) CWE [33], используемая академическими исследователями, аналитиками уязвимостей, поставщиками средств оценки. С учетом специфики рассматриваемых аспектов, обусловленных характерными особенностями обеспечения безопасности, присущими базам данных и СУБД (не принимая в расчет возможности реализации угроз посредством уязвимостей, связанных с недостатками в программном обеспечении, архитектуре и конфигурировании сетей и операционных систем), в их число вошли основные слабые места достаточно высокого уровня абстракции:

1) *неправильное управление привилегиями*: неправильное назначение привилегий, повышение (эскалация) привилегий, выполнение операций с излишними привилегиями;

2) *неправильная авторизация*: неправильное назначение разрешений для критического ресурса, отсутствует авторизация, некорректная авторизация, раскрытие конфиденциальной информации через метаданные, раскрытие конфиденциальной информации посредством запросов данных. Не выполняется или неправильно выполняется проверка авторизации, когда субъект пытается получить доступ к ресурсу или выполнить некоторое действие;

3) *неправильная аутентификация*: слабый пароль, устаревший пароль, обход аутентификации, неправильная реализация алгоритма аутентификации, несоответствующий срок действия сеанса и т. д.;

4) *неконтролируемое потребление ресурсов*: надлежащим образом не контролируется распределение ограниченного ресурса, тем самым позволяя субъекту влиять на количество потребляемых ресурсов, что в конечном итоге приводит к их исчерпанию;

5) *хранение конфиденциальной информации в открытом виде*;

6) *недостаточная стойкость шифрования*;

7) *неправильная очистка конфиденциальных данных с выведенного из эксплуатации устройства*: очистка может отсутствовать, быть недостаточной или некорректной;

8) *использование взломанного или опасного криптографического алгоритма*: использование нестандартного, с недоказанной стойкостью криптографического примитива;

9) *использование недостаточно случайных значений*;

10) *недостаточная проверка подлинности данных*: загрузка кода без проверки целостности, неправильная проверка (отсутствие проверки) значения контрольной суммы, неправильная проверка (отсутствие проверки) криптографической подписи;

11) *неправильная проверка ввода*: неправильная проверка синтаксической правильности входных данных, неправильная проверка указанного типа входных данных, неправильная проверка согласованности входных данных, неправильная проверка небезопасной эквивалентности входных данных. Входные данные или не проверяются, или проверяются неправильно – без гарантии того, что их использование не приведет в дальнейшем к неправильной и небезопасной обработки данных;

12) *использование запрещенного кода*: используются функции, библиотеки или сторонние компоненты, которые были явно запрещены разработчиком или заказчиком;

13) *встроенный вредоносный код*;

14) *нарушение принципов безопасного проектирования*: ненужная сложность в механизме защиты (используется более сложный механизм, чем необходимо); опора на единственный фактор при принятии решения о безопасности; недостаточно разделяются функциональность или процессы, требующие различных уровней привилегий, прав или разрешений; не предусмотрена проверка доступа к защищаемому объекту, выполняемая каждый раз при обращении субъекта к этому объекту; недостаточная психологическая приемлемость (сложность и неудобство использования механизма защиты зачастую побуждает пользователей незлоумышленников отключать или обходить его случайно или намеренно); опора на безопасность через неизвестность (используется механизм защиты, сила которого в значительной степени зависит от его неизвестности); несовершенство механизма поддержки целостности данных;

15) *некорректное предоставление указанной функциональности*: код не работает в соответствии с опубликованными спецификациями, что может привести к неправильному использованию;

16) *скрытая функциональность*: имеется функциональность, которая не задокументирована, не являются частью спецификации и недоступна через интерфейс или последовательность команд. Скрытая функциональность может принимать разные формы, в том числе, например, такие, как преднамеренно вредоносный код;

17) *неполная документация*: нет описаний всех соответствующих элементов продукта, таких как его использование, структура, интерфейсы, проектирование, реализация, конфигурация, эксплуатация и т. д., что усложняет обслуживание, косвенно влияя на безопасность из-за недостаточной осведомленности, затрудняя поиск и/или исправление уязвимостей или отнимая много времени, что также может упростить внедрение уязвимостей;

18) *изъян конфигурации*: несоблюдение требований безопасности при инсталляции и конфигурации БД (установлены административные, вспомогательные, учебные учетные записи, прописываемые в БД по умолчанию без надлежащего их анализа и смены паролей по умолчанию, не установлены ограничения на длину и сложность паролей, не заблокированы неиспользуемые учетные записи, не установлены критические обновления, ненадлежащим образом настроена система аудита событий и т. д.).

Для определенности обозначим их соответственно как $\gamma_1,...,\gamma_{18}$.

После идентификации угроз и уязвимостей, а также оценки возможности их связывания необходимо определить вероятности нежелательного инцидента (реализации угрозы) для соответствующих пар «угроза-уязвимость» (t_i, γ_ψ), где $i=\overline{1,11};\ \psi=\overline{1,18}$ как произведение вероятности возникновения соответствующей угрозы P_{t_i} на вероятность соответствующей уязвимости P_{γ_ψ} : $P_l = P_{t_i} \cdot P_{\gamma_\psi}$.

Метод оценивания основных компонент барьеров безопасности и защищенности базы данных в целом

Нетрудно видеть, что при известных значениях вероятности нежелательного инцидента (реализации угрозы) P_l, величины ущерба L_l (при удачном осуществлении угрозы в отношении защищаемого объекта), степени сопротивляемости соответствующего средства защиты R_l можно оценить защищенность БД, воспользовавшись выражением (2).

Однако получение точных значений P_{t_i}, P_{γ_ψ}, L_l, R_l непростая задача. Зачастую на практике это не представляется возможным [12]. К тому же, перефразируя Заде [34], по мере увеличения сложности системы аналитическая точность уменьшается [5]. Поэтому, как правило, в таких случаях целесообразно прибегнуть к числовым оценкам в некотором диапазоне величин, тем более, что каждому количественному диапазону можно сопоставить определенную качественную шкалу, с которой при определенных потребностях работать существенно проще. Подходящей структурой для выражения таких величин, как отмечалось выше, может служить лингвистическая переменная. По этим причинам, в первую очередь, в соответствии с введенными изменениями модели переопределим барьеры безопасности B, каждый из которых ($b_l \in B$) представим в виде составной лингвистической переменной, компонентами которой являются лингвистические переменные: вероятность возникновения угрозы P_t, вероятность использования уязвимости P_γ, величина ущерба L при удачном осуществлении угрозы в отношении защищаемого объекта, степень сопротивляемости средства защиты R, характеризующаяся вероятностью его преодоления. При этом замечаем, что данные компоненты оцениваются в контексте специфического барьера, который они формируют. (Индексы у $P_l = f(P_{t_i}, P_{\gamma_\psi}), L_l, R_l$ такие же, как индекс барьера, а не такие, как у компонентов барьера $b_l = (t_i, \gamma_\psi, o_j, w_k)$ – угрозы, уязвимости, объекта и средства защиты в базовой системе защиты.)

Формализацию соответствующих компонент начнем с вероятности возникновения угрозы P_t, которая может быть представлена в виде лингвистической переменной:

$$\langle name, T, X, G, M \rangle, \tag{4}$$

где $name$ – наименование лингвистической переменной (в нашем случае – это вероятность возникновения угрозы P_t); T – множество значений лингвистической переменной (терм-множество), представляющих собой наименования нечетких переменных (α_ε, где $\varepsilon = 1, 2, ...$ ($\varepsilon \in \mathbb{N}^*_{<n}$), n – максимальное число нечетких переменных), областью определения каждой из которых является множество X – универсальное множество или универсум (в рассматриваемом случае это числовые значения вероятности возникновения угрозы); G – некоторая синтаксическая процедура, позволяющая оперировать элементами терм-множества T, в частности – генерировать новые термы (значения); M – семантическая процедура, позволяющая превратить каждое новое значение лингвистической переменной, получаемое с помощью процедуры G, в нечеткую переменную, то есть сформировать соответствующее нечеткое множество. В рассматриваемом случае можно ограничиться предположением о тривиальном характере G и M, то есть никаких логических связок и модификаторов использоваться не будет.

Вероятность возникновения той или иной угрозы информации определяется экспертным путем на основании показателя, характеризующего, насколько вероятно возникновение угрозы безопасности в рассматриваемой системе с учетом особенностей ее структуры и функционирования. На практике для вычисления риска зачастую используется не математическая вероятность угрозы, а примерная частота ее реализации за определенный период времени.

Чтобы не было путаницы, вместо математического термина *probability* в стандартах намеренно используется понятие *likelihood*, которое также переводится как «вероятность». При этом эксперты не определяют функцию правдоподобия в статистическом смысле. Вместо этого они на основе имеющихся данных, опыта и экспертных суждений определяют балл (рейтинг – англ. score) вероятности [35].

Анализ различных авторитетных источников по проблемам управления информационными рисками [12, 35 – 39] показал, что для оценки P_t достаточно ввести три вербальные градации с соответствующими приблизительными количественными оценками, без которых любая качественная шкала лишается смысла:

– низкая вероятность (Н). Возникновение данной угрозы маловероятно. Не существует инцидентов, статистики, мотивов, которые указывали бы на то, что это может произойти. Ожидаемая частота угрозы не превышает одного раза в пять лет;

– средняя вероятность (С). Существуют предпосылки к появлению угрозы (зафиксированы случаи, в прошлом происходили инциденты), существует статистика или имеется другая информация, указывающая на возможность возникновения данной угрозы, у злоумышленника есть мотивация для реализации соответствующих действий. Ожидаемая частота появления данной угрозы – примерно один раз в год;

– высокая вероятность (В). Имеются объективные предпосылки для возникновения угрозы. Существуют инциденты, статистика или другая информация, указывающая на то, что угроза, скорее всего, осуществится, у злоумышленника есть мотивы для реализации соответствующих действий. Ожидаемая частота появления угрозы – в среднем один раз в четыре месяца или чаще.

Такой трехуровневой шкалы обычно достаточно для первоначальной высокоуровневой оценки. В дальнейшем ее можно расширить, добавив еще несколько промежуточных уровней. При этом следует отметить, что оценки ожидаемой частоты возникновения угрозы от уровня к уровню по качественной шкале различаются в разы, поэтому маловероятно, чтобы компетентные эксперты сильно ошибались бы в своих оценках.

С другой стороны, частотную оценку имеющейся величины можно преобразовать в числовой эквивалент вероятности возникновения угрозы, соответствующий некоторому диапазону значений. Под термином «вероятность» в данном случае понимается так называемая субъективная вероятность – мера уверенности некоторого человека или группы людей (агентов) в том, что данное событие в действительности будет иметь место [37, 40].

Исходя из обобщения проанализированных источников [37, 38, 41], будем полагать, что в числовом эквиваленте вероятность возникновения такой угрозы на соответствующем уровне может находиться в соответствующем ей диапазоне:

– для уровня Н – $P_t = [0, 0.2]$;

– уровня С – $P_t = [0.2, 0.6]$;

– уровня В – $P_t = [0.6, 1]$.

Тогда, воспользовавшись применяемыми при оценке рисков информационной безопасности известными качественными шкалами [12, 35 – 37, 39], в частности трехуровневой качественной шкалой, определим наименования нечетких переменных – множество значений терм-множества T: T ={«низкая вероятность», «средняя вероятность», «высокая вероятность»}={«Н», «С», «В»}, то есть α_1=«Н», α_2 = «С», α_3=«В».

Как известно, когда речь идет о нечеткой переменной α, всегда имеется в виду некоторое нечеткое множество $A = \{\mu_A(x) / x\}$, которое определяет ее возможные значения, где $\mu_A(x)$ – *функция принадлежности* ($\mu_A(x) \in [0,1]$; $\mu_A(x): X \to [0,1]$), которая указывает степень принадлежности элемента x нечеткому множеству A.

Наибольшее распространение при построении функций принадлежности нечетких множеств получили прямые и косвенные методы [42, 43]. Ввиду того, что $x \in X$ могут быть из-

мерены в количественной шкале, воспользуемся прямым методом, когда эксперт либо группа экспертов задают для каждого $x \in X$ значение функции принадлежности $\mu_A(x)$. При этом, как отмечается в работе [42], теория нечетких множеств при использовании прямых методов построения функции принадлежности не требует абсолютно точного ее задания. Очень часто бывает достаточно зафиксировать лишь наиболее характерные значения и вид (тип) функции $\mu_A(x)$. Сама же функция принадлежности может быть определена [44]: графически (график, диаграмма); аналитически (формулы); в виде таблицы, суммы или интеграла, вектора степеней принадлежности. Как показывает опыт, удобно использовать те функции принадлежности, которые допускают аналитическое представление в виде некоторой простой математической функции [42].

На основании анализа основных функций принадлежности, использующихся для представления таких свойств нечетких множеств, которые характеризуются неопределенностью типов «небольшое значение», «незначительная величина»; «расположен в интервале», «приблизительно равно»; «большое значение», «значительная величина», для рассматриваемых нечетких переменных «Н», «С», «В» были выбраны трапециевидная, линейная Z- и линейная S-образные функции. Каждая из этих функций может быть представлена так:

– линейная Z-образная функция принадлежности нечеткого множества $A_{\text{Н}} = \{\mu_{\text{Н}}(x)/x\}$, соответствующего нечеткой переменной «Н» для лингвистической переменной – вероятность возникновения угрозы P_t:

$$\mu_{\text{Н}}(x;a,b) = \begin{cases} 1, & x \le a, \\ \dfrac{b-x}{b-a}, & a < x < b, \\ 0, & b \le x, \end{cases} \tag{5}$$

где a, b – упорядоченные отношением $a \le b$, числовые параметры;

– трапециевидная функция принадлежности нечеткого множества $A_{\text{С}} = \{\mu_{\text{С}}(x)/x\}$, соответствующего нечеткой переменной «С» для лингвистической переменной P_t:

$$\mu_{\text{С}}(x;a,b,c,d) = \begin{cases} 0, & x \le a, \\ \dfrac{x-a}{b-a}, & a \le x \le b, \\ 1, & b \le x \le c, \\ \dfrac{d-x}{d-c}, & c \le x \le d, \\ 0, & d \le x, \end{cases} \tag{6}$$

где a, b, c, d – упорядоченные отношением: $a \le b \le c \le d$, числовые параметры;

– линейная S-образная функция принадлежности нечеткого множества $A_{\text{В}} = \{\mu_{\text{В}}(x)/x\}$, соответствующего нечеткой переменной «В» для лингвистической переменной P_t:

$$\mu_B(x;c,d) = \begin{cases} 0, & x \le c, \\ \dfrac{x-c}{d-c}, & c < x < d, \\ 1, & d \le x, \end{cases} \tag{7}$$

где c, d – числовые параметры ($c \le d$).

На рис. 4 представлены все три графика функций принадлежности нечетких переменных, используемых для задания лингвистической переменной – вероятность возникновения угрозы P_t.

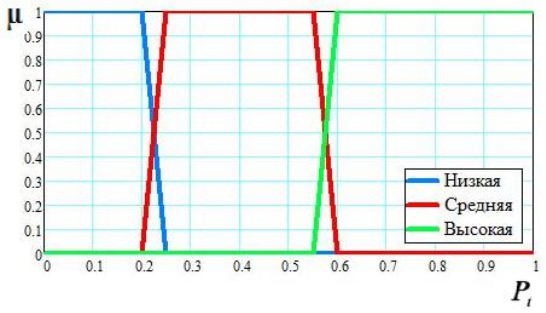


Рис. 4. Графики функции принадлежности нечетких множеств $A_{\text{Н}}$, $A_{\text{С}}$, $A_{\text{В}}$

Эксперт на основании априорных знаний присваивает лингвистические значения, представляющие собой наименования нечетких переменных, для каждой вероятности возникновения угрозы P_{t_i} как компоненты соответствующего специфического барьера b_l. В данном случае эти значения могут представляться вербально как: «низкая вероятность», «средняя вероятность», «высокая вероятность» (или «Н», «С», «В»). Поскольку с каждым таким значением связывается соответствующая функция принадлежности с соответствующими приблизительными количественными оценками, то, в принципе, для каждой угрозы $t_i \in T$ можно определить с ограниченной степенью точности численное значение этой вероятности P_{t_i}, например, как *модальное значение нечеткого множества*. Если ядро нечеткого множества содержит более одного элемента, то для такого множества модальное значение определяется как среднее значение элементов ядра. *Ядро нечеткого множества* A представляет собой четкое подмножество области определения X, содержащее все элементы, принадлежащие множеству A со степенью, равной 1 [44].

Далее, воспользовавшись изложенным подходом, представим в виде соответствующей лингвистической переменной вероятность использования уязвимости – P_γ (вероятность того, что в случае реализации угрозы в отношении актива эта угроза будет реализована успешно с использованием данной уязвимости). Уязвимости так же, как и угрозы, могут быть оценены по трехуровневой качественной шкале. Для оценки P_γ введем три вербальные градации с соответствующими приблизительными количественными оценками:

– высокая (В). Уязвимость легко использовать, и существует слабая защита или защита вообще отсутствует. Вероятность использования уязвимости (вероятность успешной реализации угрозы за счет данной уязвимости) находится в диапазоне [0.7, 1];

– средняя (С). Уязвимость может быть использована, но существует определенная защита. Вероятность использования уязвимости находится в диапазоне [0.3, 0.7];

– низкая (Н). Уязвимость сложно использовать, и существует хорошая защита. Вероятность использования уязвимости находится в диапазоне [0, 0.3].

Так же, как и с угрозами, для первоначальной высокоуровневой оценки уязвимостей вполне может хватить такой трехуровневой шкалы. В дальнейшем для более детальной оценки ее можно расширить.

Воспользовавшись введенными обозначениями, определим наименования нечетких переменных (β_ε, где $\varepsilon \in \square^*_{<n}$) – множество значений терм-множества T_γ лингвистической переменной P_γ: T_γ={«высокая уязвимость», «средняя уязвимость», «низкая уязвимость»}={«В», «С», «Н»}, то есть β_1=«В», β_2= «С», β_3=«Н». Областью определения каждой из нечетких переменных является множество числовых ($X \in [0,1]$) значений вероятности использования уязвимости. В рассматриваемом случае тоже можно ограничиться предположением о тривиальном характере G_γ и M_γ (без логических связок и модификаторов).

На основании анализа основных функций принадлежности, подобно приведенному выше, для рассматриваемых нечетких переменных β_1=«В», β_2= «С», β_3=«Н» были выбраны трапециевидная, линейная Z- и линейная S-образные функции. Каждая из этих функций может быть представлена как:

– линейная Z-образная функция принадлежности нечеткого множества $A_{\text{Н}}^{v} = \{\mu_{\text{Н}}^{v}(x)/x\}$, соответствующего нечеткой переменной «Н» для лингвистической переменной P_γ:

$$\mu_{\text{Н}}^{v}(x;a,b) = \begin{cases} 1, & x \le a, \\ \dfrac{b-x}{b-a}, & a < x < b, \\ 0, & b \le x; \end{cases} \tag{8}$$

– трапециевидная функция принадлежности нечеткого множества $A_{\text{С}}^{v} = \{\mu_{\text{С}}^{v}(x)/x\}$, соответствующего нечеткой переменной «С» для лингвистической переменной P_γ:

$$\mu_{\text{С}}^{v}(x;a,b,c,d) = \begin{cases} 0, & x \le a, \\ \dfrac{x-a}{b-a}, & a \le x \le b, \\ 1, & b \le x \le c, \\ \dfrac{d-x}{d-c}, & c \le x \le d, \\ 0, & d \le x; \end{cases} \tag{9}$$

– линейная S-образная функция принадлежности нечеткого множества $A_{\text{В}}^{v} = \{\mu_{\text{В}}^{v}(x)/x\}$, соответствующего нечеткой переменной «В» для лингвистической переменной P_γ:

$$\mu_{B}^{v}(x;c,d) = \begin{cases} 0, & x \le c, \\ \dfrac{x-c}{d-c}, & c < x < d, \\ 1, & d \le x. \end{cases} \tag{10}$$

На рис. 5 представлены три графика функций принадлежности нечетких переменных, используемых для задания лингвистической переменной – вероятность использования уязвимости P_γ.

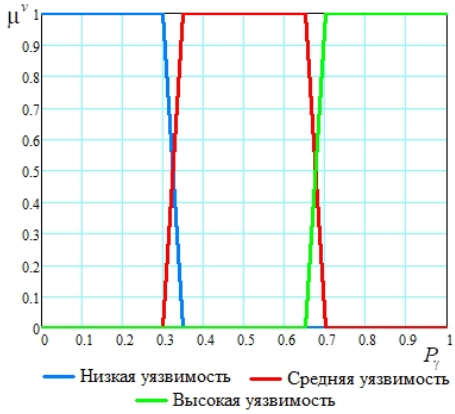


Рис. 5. Графики функции принадлежности нечетких множеств $A_{\text{Н}}^{v}$, $A_{\text{С}}^{v}$, $A_{\text{В}}^{v}$

Эксперт на основании априорных знаний присваивает лингвистические значения, представляющие собой наименования нечетких переменных, для каждой вероятности использования уязвимости P_γ как компоненты соответствующего барьера b_l, благодаря которой становится возможной реализация соответствующей угрозы t_i. Эти значения представляются вербально как: «Н», «С», «В». Так как с каждым таким значением связывается соответствующая функция принадлежности с соответствующими приблизительными количественными оценками, то для каждой уязвимости γ_ψ можно вычислить с ограниченной степенью точности численное значение этой вероятности P_{γ_ψ}, например, как модальное значение соответствующего нечеткого множества.

По аналогии можно определить степень сопротивляемости средств защиты (называемых в литературе [8, 11, 12, 45 – 48] также как механизмы, меры, средства контроля (англ. controls), к которым относится любой процесс, политика, устройство, установившаяся практика или другие действия, которые изменяют риск [11]), характеризующуюся вероятностью их преодоления ($P_l^{ov} = 1 - R_l$). Соответствующие уровни контроля (степень сопротивляемости) могут быть определены следующим образом:

– В – высокая степень сопротивляемости средства (меры, механизма) защиты (высокий уровень контроля). Маловероятно, что такой механизм удастся преодолеть. Вероятность преодоления (обхода) такого механизма находится в диапазоне – $P_l^{ov} \in [0,\ 0.4]$;

– С – средняя степень сопротивляемости средства защиты. Такое средство (мера) обеспечивает определенную защиту, однако есть возможность его преодолеть, затратив определенные усилия. Вероятность преодоления соответствующей меры защиты находится в диапазоне [0.4, 0.8];

– Н – низкая степень сопротивляемости средства защиты. Такое средство (меру) довольно просто преодолеть. Вероятность преодоления соответствующей меры защиты находится в диапазоне [0.8, 1].

Тогда, воспользовавшись этой шкалой, определим наименования нечетких переменных (δ_ε, где $\varepsilon \in \square^*_{<n}$) – множество значений терм-множества T_R лингвистической переменной R: T_R ={«высокая степень сопротивляемости», «средняя степень сопротивляемости», «низкая степень сопротивляемости»}={«В», «С», «Н»}, то есть δ_1=«В», δ_2 =«С», δ_3=«Н». Областью определения каждой из нечетких переменных является множество числовых значений ($X \in [0,1]$) вероятности преодоления средств защиты. В рассматриваемом случае также ограничимся предположением о тривиальном характере G_R и M_R (без логических связок и модификаторов).

Подобно приведенному выше подходу для рассматриваемых нечетких переменных δ_1=«В», δ_2 = «С», δ_3=«Н» (с которыми связываются соответствующие нечеткие множества, определяющие их возможные значения: $A_{\text{Н}}^{ov} = \{\mu_{\text{Н}}^{ov}(x)/x\}$, $A_{\text{С}}^{ov} = \{\mu_{\text{С}}^{ov}(x)/x\}$, $A_{\text{В}}^{ov} = \{\mu_{\text{В}}^{ov}(x)/x\}$) были выбраны трапециевидная, линейная Z- и линейная S-образные функции принадлежности ($\mu_{\text{Н}}^{ov}(x)$, $\mu_{\text{С}}^{ov}(x)$, $\mu_{\text{В}}^{ov}(x)$). На рис. 6 представлены три графика функций принадлежности нечетких переменных, используемых для определения лингвистической переменной, – степени сопротивляемости средства защиты R ($R = 1 - P^{ov}$; в некоторых источниках [45] P^{ov} называют обратной силой контроля (англ. reverse of the control strength)).

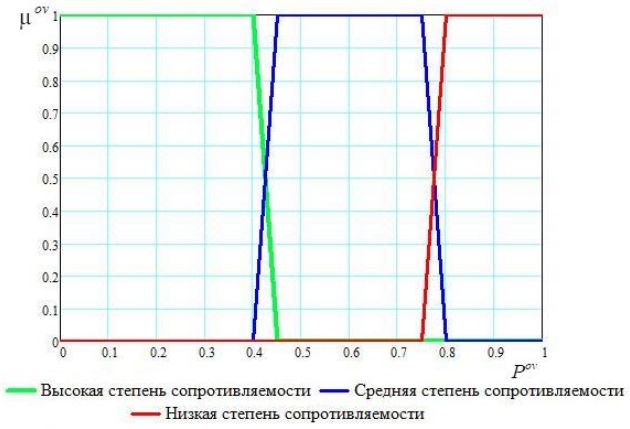


Рис. 6. Графики функции принадлежности нечетких множеств $A_{\text{Н}}^{ov}$, $A_{\text{С}}^{ov}$, $A_{\text{В}}^{ov}$

Эксперт на основании априорных знаний об используемых средствах защиты (защитных мерах), затрудняющих использование соответствующей уязвимости γ_ψ, благодаря которой становится возможной реализация соответствующей угрозы t_i, присваивает лингвистические значения «высокая степень сопротивляемости», «средняя степень сопротивляемости», «низкая степень сопротивляемости» или «В», «С», «Н» для каждой R_l как компоненты соответствующего барьера b_l. Ввиду того, что с каждым таким значением связывается соответствующая функция принадлежности с соответствующими приблизительными количественными оценками, то для каждого средства обеспечения безопасности $w_k \in W$ барьера b_l можно определить численное значение как P_l^{ov}, так и $R_l = 1 - P_l^{ov}$. Опять же, как модальное значение соответствующего нечеткого множества.

Ущерб (как убыток, урон, потеря), причиняемый в результате инцидентов безопасности, связывается с целевой функцией системы – одним из соответствующих показателей, таким как упущенная выгода, потеря конкурентных преимуществ, ухудшение репутации организации, причинение вреда интересам третьей стороны, финансовые потери, связанные с восстановлением ресурсов, дезорганизация деятельности в связи с недоступностью данных и т. д. Для разных организаций важность каждого из них может иметь существенно разное значение.

С экономической точки зрения ущерб активам удобно представлять в терминах финансовых потерь. Однако на практике получение точных количественных значений ущерба часто затруднено или вообще невозможно [10]. Тем не менее, большинство не поддающихся количественному описанию потерь можно представить в численном виде путем использования эмпирической шкалы уровня ущерба – качественной шкалы измерения, разделенной на области (ранги), соответствующие различным степеням удовлетворения рассматриваемых требований, например, пятибалльной шкалы: от 1 до 5. Каждому из таких уровней (рангов) можно сопоставить значение терм-множества T_L (T_L={«Очень низкий», «Низкий», «Средний», «Высокий», «Очень высокий»}={«VL», «L», «M», «H», «VH»}) лингвистической переменной – величина ущерба L. Областью определения каждой из нечетких переменных является множество числовых значений величины ущерба/уровня ущерба (в баллах) $X \in (0,6)$. В рассматриваемом случае можно ограничиться предположением о тривиальном характере G_L и M_L.

Для рассматриваемых нечетких переменных ρ_1=«VH», ρ_2=«H», ρ_3=«M», ρ_4=«L», ρ_5=«VL» (с которыми связываются соответствующие нечеткие множества, определяющие их возможные значения: $A_{\text{VH}}^L = \{\mu_{\text{VH}}^L(x)/x\}$, $A_{\text{H}}^L = \{\mu_{\text{H}}^L(x)/x\}$, $A_{\text{M}}^L = \{\mu_{\text{M}}^L(x)/x\}$,

$A_{\text{L}}^{L}=\{\mu_{\text{L}}^{L}(x)/x\}$, $A_{\text{VL}}^{L}=\{\mu_{\text{VL}}^{L}(x)/x\}$) были выбраны треугольные, линейная Z- и линейная S-образные функции принадлежности ($\mu_{\text{VH}}^{L}(x)$, $\mu_{\text{H}}^{L}(x)$, $\mu_{\text{M}}^{L}(x)$, $\mu_{\text{L}}^{L}(x)$, $\mu_{\text{VL}}^{L}(x)$):

$$\mu_{\text{VL}}^{L}(x;a,b)=\begin{cases}1, & x\le a,\\ \dfrac{b-x}{b-a}, & a<x<b,\\ 0, & b\le x,\end{cases}\qquad \text{где } a=1;\ b=2. \tag{11}$$

– $$\mu_{\text{H}}^{L}(x;a,b,c,d),\mu_{\text{M}}^{L}(x;a,b,c,d),\mu_{\text{L}}^{L}(x;a,b,c,d)=\begin{cases}0, & x\le a,\\ \dfrac{x-a}{b-a}, & a\le x\le b,\\ \dfrac{c-x}{c-b}, & b\le x\le c,\\ 0, & c\le x,\end{cases} \tag{12}$$

где для μ_{H}^{L} a=1, b=2, c=3; для μ_{M}^{L} a=2, b=3, c=4; для μ_{L}^{L} a=3, b=4, c=5;

– $$\mu_{\text{VH}}^{L}(x;c,d)=\begin{cases}0, & x\le c,\\ \dfrac{x-c}{d-c}, & c<x<d,\\ 1, & d\le x,\end{cases}\qquad \text{где } c=4;\ d=5. \tag{13}$$

На рис. 7 представлены графики функций принадлежности нечетких переменных, используемых для задания лингвистической переменной – величина ущерба L.

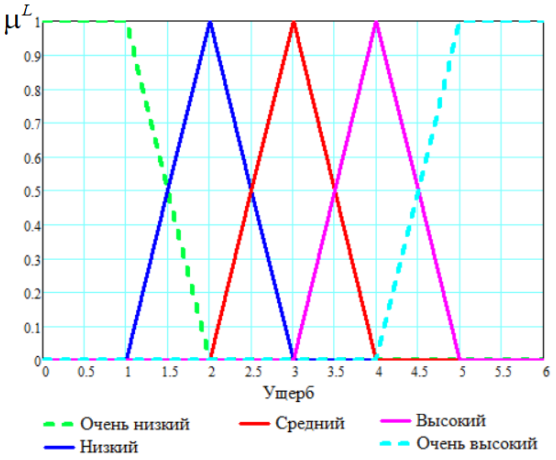


Рис. 7. Графики функции принадлежности нечетких множеств A_{VH}^{L}, A_{H}^{L}, A_{M}^{L}, A_{L}^{L}, A_{VL}^{L}

В табл. 1 представлена оценка величины ущерба в пятибалльной шкале и его семантическая характеристика.

Таблица 1

Уровень ущерба	**Значение терм-множества T_L**	**Семантическая характеристика значения показателя величины ущерба**
1	Очень низкий	Ущербом можно пренебречь.
2	Низкий	Ущерб легко устраним, затраты на ликвидацию последствий реализации угрозы невелики.
3	Средний	Ликвидация последствий реализации угрозы не связана с крупными затратами.
4	Высокий	Ликвидация последствий реализации угрозы связана со значительными финансовыми потерями.
5	Очень высокий	Организация прекращает существование.

Для того чтобы оценка ценности активов имела экономический смысл, качественную шкалу оценки ущерба целесообразно соотнести с размером прямых финансовых потерь. Однако установление такого соответствия требует дополнительных исследований в каждом конкретном случае и зависит от многих факторов для рассматриваемых систем. Возможная шкала оценки прямых финансовых потерь может выглядеть подобно той, что показана в табл. 2. Все зависит от задач, решаемых организацией, областью, характером и масштабами ее деятельности, формой собственности, стоимости активов, тяжести последствий нарушения их безопасности и ряда других факторов.

Таблица 2

Уровень ущерба	**Значение терм-множества T_L**	**Финансовые потери**
1	Очень низкий	менее 100 $
2	Низкий	(100-1000) $
3	Средний	(1000-10 000) $
4	Высокий	(10 000-100 000) $
5	Очень высокий	свыше 100 000 $

Таким образом, располагая соответствующими данными, воспользовавшись выражением (2), можно определить величину защищенности анализируемой БД.

Выводы

1. Исходя из анализа и обобщения различных подходов и достижений в области оценки безопасности информационных систем в целом и баз данных в частности было принято решение модель защиты БД и ее оценку строить на основе известной модели системы безопасности с полным перекрытием, опирающуюся на теорию графов, нечетких множеств, вероятностей, и традиционно считающуюся основой формального описания систем защиты.

2. В результате формализации задачи обеспечения безопасности баз данных:

– определены основные объекты защиты реляционных БД (с учетом двойственной природы системы БД и различной степени детализации ее компонент);

– выявлены основные значимые антропогенные угрозы безопасности баз данных;

– определен (на основе анализа существующих таксономий) перечень основных общих слабых мест (недостатков) как некоторых типов уязвимостей;

– определен показатель защищенности БД (эффективности/результативности безопасности) как величина обратная суммарному остаточному риску, составные компоненты которого представляются в виде соответствующих лингвистических переменных.

3. Разработан метод оценивания основных компонент барьеров безопасности и защищенности базы данных в целом, опирающийся на теорию нечетких множеств и риска.

4. Предлагаемая модель защиты, в которой в явном виде учитывается понятие уязвимости как отдельно объективно существующей категории (слабого места актива или средства управления, которое может быть использовано одной или более угрозой), что позволяет более адекватно оценивать вероятность нежелательного инцидента (реализации угрозы) в двухфакторной модели (в которой один из факторов отображает мотивационную составляющую возникновения угрозы, а второй учитывает существующие уязвимости), а следовательно, и оценку защищенности БД в целом, является дальнейшим развитием модели Клементса – Хоффмана.

Список литературы:

1. ISO/IEC 25010:2011 Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). System and software quality models. URL: https://www.iso.org/standard/35733.html/. (accessed on 12 August 2021).
2. Смирнов С. Н. Безопасность систем баз данных. Москва : Гелиос АРВ, 2007. – 352 с.
3. Tanenbaum A. S., Bos H. Modern Operating Systems. Fourth edition. Pearson, 2015. 1136 p.
4. Хоффман, Л. Дж. Современные методы защиты информации. Москва : Сов. радио, 1980. 264 с.

5. Hoffman L. J., Clements D. Fuzzy computer security metrics: A preliminary report. Memorandum No. ERL-M77/6 27 January 1977. Electronics research laboratory. College of Engineering University of California, Berkeley. 20 p. https://www2.eecs.berkeley.edu/Pubs/TechRpts/1977/ERL-m-77-6.pdf. (accessed on 12 August 2021).
6. Committee on National Security Systems (CNSS) Glossary. CNSSI No. 4009, 2015. URL: h https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. (accessed on 12 August 2021).
7. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Москва : Книжный мир, 2009. 352 с.
8. Астахов А. Анализ защищенности корпоративных систем // Открытые системы. 2002. № 7-8. URL: https://www.osp.ru/os/2002/07-08/181720. (accessed on 12 August 2021).
9. Аверченков В. И., Рытов М. Ю., Гайнулин Т. Р. Оптимизация выбора состава средств инженерно-технической защиты информации на основе модели Клементса – Хоффмана // Вестн. Брянск. гос. техн. ун-та. 2008. № 1(17). С. 61-66.
10. Карпычев В. Ю. Экономический анализ нормативно-технического обеспечения информационной безопасности // Экономический анализ: теория и практика. 2011. №35 (242). С. 2-18.
11. ISO/IEC 27000:2018 Information technology. Security techniques. Information security management systems. Overview and vocabulary. URL: https://www.iso.org/standard/73906.html. (accessed on 12 August 2021).
12. Астахов А. М. Искусство управления информационными рисками. Москва : ДМК Пресс, 2010. 312 с.
13. Скиба А. В., Архипов А. Е. Информационные риски: модели рисков, исследование и использование // Інвестиції: практика та досвід. 2016. № 1. С. 51-60.
14. Архипов А. Е. Экспертно-аналитическое оценивание информационных рисков и уровня эффективности системы защиты информации // Радіоелектроніка. Інформатика. Управління. 2009. № 2. С. 111-115.
15. DB-Engines Ranking. URL: https://db-engines.com/en/ranking. (accessed on 12 August 2021).
16. TOPDB Top Database index. URL: https://pypl.github.io/DB.html. (accessed on 12 August 2021).
17. Gartner, Magic Quadrant for Operational Database Management Systems, Merv Adrian, Donald Feinberg, Nick Heudecker, 25 November 2019 – ID G00376881. URL: https://www.gartner.com/en/documents/3975492/magic-quadrant-for-operational-database-management-syste. (accessed on 12 August 2021).
18. Critical Capabilities for Cloud Database Management Systems for Operational Use Cases. Published 24 November 2020 – ID G00468197. Merv Adrian, Donald Feinberg, Rick Greenwald, Adam Ronthal, Henry Cook, https://www.oracle.com/explore/adw-ocom/gartner-cloud-database-management/?source=:ow:o:p:mt:::RC_WWMK200720P00100:Gartnerdatabase&intcmp=:ow:o:p:mt:::RC_WWMK200720P00100:Gartnerdatabase&lb-mode=overlay; https://www.oracle.com/database/gartner-dbms.html. (accessed on 12 August 2021).
19. Sandhu R. S., Jajodia S. Data and database security and controls // Handbook of information security management, Auerbach Publishers. 1993. P. 481-499.
20. Groff J., Weinberg P., Oppel A. SQL. The Complete Reference. 3rd ed. New York, NY, USA: McGraw-Hill, Inc.; 2010. – 912 p.
21. Муханова А., Ревнивых А. В., Федотов А. М. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах // Вестн. Новосибир. гос. ун-та. Сер.: Информационные технологии. 2013. Т. 11, № 2. С. 55-72.
22. Kulkarni S., Urolagin S. Review of attacks on databases and database security techniques // International Journal of Emerging Technology and Advanced Engineering. 2012. Vol. 2, Issue 11. P. 2250-2459.
23. Rohilla S., Mittal P. K. Database Security: Threads and Challenges // International Journal of Advanced Research in Computer Science and Software Engineering. 2013, Vol. 3, Issue 5. P. 810–813.
24. Pfleeger C. P., Pfleeger S. L., Margulies J. Security in Computing. Fifth Edition. Prentice Hall. 2015. 944 p.
25. Imperva Whitepaper. Top ten database security threats. 2015. – URL: https://files.meetup.com/5631682/WP_TopTen_Database_Threats.pdf. (accessed on 12 August 2021).
26. Imperva Whitepaper. Top 5 Database Security Threats. 2016. URL: https://www.imperva.com/docs/gated/WP_Top_5_Database_Security_Threats.pdf. (accessed on 12 August 2021).
27. Вілігура В. В. Систематизація загроз і вразливостей характерних для баз даних і СУБД // Праці 7-ої Міжнар. конф. «Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2021), 21-23 квітня 2021 р. Харків : Харк. нац. ун-т імені В. Н. Каразіна, 2021. С. 83-86.
28. MITRE. CVE. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org/data/downloads/allitems.html. (accessed on 12 August 2021).
29. MITRE. CWE Version 4.2. 2020-08-20. URL: https://cwe.mitre.org/data/published/cwe_v4.2.pdf. (accessed on 12 August 2021).
30. MITRE. Common Weakness Enumeration. CWE List Version 4.2. URL: https://cwe.mitre.org/data/index.html. (accessed on 12 August 2021).
31. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. URL: https://docs.cntd.ru/document/1200123702. (accessed on 12 August 2021).
32. Марков А. С., Фадин А. А. Систематика уязвимостей и дефектов безопасности программных ресурсов // Защита информации. Инсайд. 2013. № 3. С. 2-7.

33. MITRE. CWE VIEW: Research Concepts. URL: https://cwe.mitre.org/data/definitions/1000.html. (accessed on 12 August 2021).
34. Zadeh L. A. The concept of a linguistic variable and its application to approximate reasoning – I // Information sciences. 1975. Vol. 8, Issue 3. P. 199-249.
35. NIST Special Publication 800-30 Revision 1. September 2012. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. (accessed on 12 August 2021).
36. Нестеров С. А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft. Москва : Национальный Открытый Университет "ИНТУИТ", 2016. 251 с.
37. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. Москва : Академия АйТи : ДМК Пресс, 2004. – 384 с.
38. Корниенко А. А., Никитин А. Б., Диасамидзе С. В., Кузьменкова Е. Ю. Моделирование компьютерных атак на распределенную информационную систему // Изв. Петербург. ун-та путей сообщения. 2018. Т. 15. № 4. С. 613-628.
39. Talabis M., Martin J. Information Security Risk Assessment Toolkit Practical Assessments through Data Collection and Data Analysis. Waltham, MA, USA : Syngress, 2012. 258 p.
40. Hajek A. Interpretations of probability. In The Stanford Encyclopedia of Philosophy. URL: https://plato.stanford.edu/entries/probability-interpret/. (accessed on 12 August 2021).
41. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. 2008. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god. (accessed on 12 August 2021).
42. Леоненков А. В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. СПб. : БХВ Петербург, 2005. 736 с.
43. Круглов В. В., Дли М. И., Голунов Р. Ю. Нечеткая логика и искусственные нейронные сети. Москва : Физматлит, 2001. 201 с.
44. Piegat A. Fuzzy Modeling and Control. Heidelberg ; New York: Physica-Verlag, 2001. 733 p.
45. Talabis M., Martin J. Information Security Risk Assessment Toolkit Practical Assessments through Data Collection and Data Analysis. Waltham, MA, USA : Syngress, 2012. 258 p.
46. Whitman M. E., Mattord H. J. Principles of Information Security, 6th Edition. Boston, MA, USA : Cengage Learning, 2017. 656 p.
47. NIST Special Publication 800-53 Revision 5. (2020). Security and Privacy Controls for Information Systems and Organizations. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. (https://doi.org/10.6028/NIST.SP.800-53r5). (accessed on 12 August 2021).
48. ISO/IEC 27002:2013 Information technology. Security techniques. Code of practice for information security controls. URL: https://www.iso.org/standard/54533.html. (accessed on 12 August 2021).

Поступила в редколлегию 22.09.2021

Сведения об авторах:

Вилигура Владислав Викторович – аспирант, Харьковский национальный университет имени В.Н. Каразина, кафедра безопасности информационных систем и технологий, факультета компьютерных наук; Украина; e-mail: viligura93@gmail.com; ORCID: https://orcid.org/0000-0002-1137-2382

Есин Виталий Иванович – д-р техн. наук, доцент, Харьковский национальный университет имени В.Н. Каразина, профессор, кафедра безопасности информационных систем и технологий, факультета компьютерных наук; Украина; e-mail: v.i.yesin@karazin.ua; ORCID: https://orcid.org/0000-0003-1977-7269

УДК 621.391:519.2 **DOI:10.30837/rt.2021.3.206.09**

Є.В. КОТУХ, канд. техн. наук, Т.О. ОХРІМЕНКО, канд. техн. наук,
О.Ф. ДЯЧЕНКО, канд. пед. наук, Н.Ю. РОТАНЬОВА, канд. пед. наук,
Л.С. КОЗІНА, Д.В. ЗЕЛЕНСЬКИЙ

КРИПТОАНАЛІЗ СИСТЕМ НА ОСНОВІ ПРОБЛЕМИ СЛОВА З ВИКОРИСТАННЯМ ЛОГАРИФМІЧНИХ ПІДПИСІВ

Стрімкий розвиток та досягнення у сфері квантових комп'ютерів сприяє розвитку криптосистем з відкритим ключем на основі математично складних або важко вирішуваних задач, адже загроза використання квантових алгоритмів для зламу сучасних традиційних криптосистем стає набагато реальнішою з кожним днем. Варто зазначити, що класичні математично складні проблеми факторизації цілих чисел та дискретних логарифмів більш не вважаються складними для квантових обчислень [1]. Десятки криптосистем були розглянуті та запропоновані з різних складних проблем теорії груп у 2000 -х роках [2 - 11].Одною з таких складних проблем є проблема слова [1]. Одна з перших реалізацій криптосистеми на основі проблеми слова була запропонована Магліверасом [5] з використанням логарифмічних підписів для кінцевих груп перестановок та надалі запропонована Лемпкеном та ін. для асиметричної криптографії з випадковими покриттями [2]. Новаторство цієї ідеї полягає у поширенні важко вирішуваної проблеми слова на велику кількість груп. Перша реалізація такої криптосистеми була запропонована для групи Сузукі під назвою MST_3. Кілька поліпшень MST_3 з групою Сузукі були зроблені в [12 - 13]. У 2010 р. Сваба та ін. [12] проаналізували всі опубліковані посилання на атаки на криптографію MST_3 та створили більш безпечну криптосистему $eMST_3$, додавши секретне гомоморфне покриття. У 2018 р. Т. ван Транг [14] запропонував загальний метод побудови сильних апериодичних логарифмічних сигнатур для абелевих р-груп, що є подальшим внеском у практичне застосування криптосистем MST_3.

У статті узагальнимо відомі результати криптоаналізу базових конструкцій криптосистеми MST_3 та визначимо рекомендації для напрямків покращення криптографічних властивостей конструкцій MST_3 та використання некомутативних груп у якості базових конструкцій.

Аналіз безпеки базової конструкції

У цьому розділі розглянуто попередні роботи, що присвячені безпеці MST_3, та зроблено деякі елементарні висновки щодо безпеки базової конструкції системи. Надалі для простоти будемо називати базову конструкцію платформою.

У [8] автори MST_3 дають стислий огляд безпеки схеми та дають атаку на криптосистему в пасивній моделі супротивника зі складністю приблизно q^2, коли використовуються Сузукі 2-групи, де $q = |Z| = |G/Z|$ (зауважимо, що q є експоненціальним параметром безпеки, тому атаки, які є поліноміальними за q, насправді мають експоненціальну складність). В роботі накладається додаткова умова на α, коли 2-групи Сузукі використовують як платформу для MST_3, а саме, що не повинно бути двох елементів набору A_i в одному класі суміжності Z. Оскільки ця умова виконується для переважної кількості ключів – ігноруємо її заради простоти.

Магліверас та співавтори [5] забезпечують кращу атаку складності $O(q)$. Вони стверджують, що їх атака застосовувана для платформи Сузукі 2-групи, але насправді їх атака працює для будь-якої платформи. В цій роботі автори далі показують, що MST_3 небезпечно, якщо β – це канонічний логарифмічний підпис (насправді їх атака не працює в цікавому окремому випадку, коли $d_i = 1$ для усіх i, так як їм потрібно, щоб сума векторів в підпросторі дорівнювала нулю, криптоаналіз покриває цей окремий випадок). Зауважимо, що можна запобігти атаці в [5]: або шляхом вибору $d_i = 1$ для усіх i, або створенням зведеного поперечного логарифмічного підпису (ATLS), який навряд чи буде канонічним. В попередній роботі автори давали визначення типів та особливостей генерації логарифмічних підписів. Автори MST_3 припускають [9], що випадково обране накриття α в кінцевій групі буде (з переважною ймовірністю) індукувати однобічну функцію $\breve{\alpha}$.

Це розумне припущення, але автори стверджують, що це припущення фактично не потрібне для встановлення безпеки MST_3 (в пасивній моделі). Гонсалес Васко та автори [3] дають переконливі докази того, що це останнє твердження невірне, показуючи, що коли α не індукує однобічну функцію, MST_3 небезпечна, якщо частка $|Z|/|J|$ є більшою. Потім вони наводять експериментальні докази того, що $|Z|/|J|$ – зазвичай доволі мала. В роботі показано, що рандомізована версія MST_3 небезпечна в сенсі нерозрізненості навіть для пасивних супротивників. Проблема генерації β глибоко не обговорюється в роботі [4], але припустимо, що β буде побудована як ATLS. Це найзагальніший з відомих, практичний метод для генерації слабких логарифмічних підписів для Z. Неперіодичні покриття типу (r_1, r_2) є надто ресурсномісткими з точки зору зберігання. Більш того, незрозумілими з огляду на безпеку є результати розкладання неперіодичного розбиття на логарифмічний підпис типу $(r_1, ..., r_s)$ для $s > 2$. Знову з міркувань зберігання кількість операцій злиття в конструкції ATLS має бути невеликою: об'єднання збільшує кількість елементів, які повинно бути збережено $|E_i||E_j| - (|E_i| + |E_j|)$ та тому невибіркове використання об'єднання може привести до експоненціальної вимоги до зберігання. З точки зору ефективності генерації ATLS типу $(2, 2, ..., 2)$ дуже приваблива. Однак це означає, що неможливо використовувати об'єднання для їх створення.

Попередні дослідження залишають відкритим питання про те, чи безпечно MST_3 на практиці, якщо запобігти канонічних поперечних логарифмічних підписів при генерації часткового ключа. Далі покажемо практичний криптоаналіз криптосистеми MST_3 в тому числі коли часткові ключі генеруються з використанням методу ATLS.

Звертаємо увагу, що хоча секретний ключ складається з простого логарифмічного підпису β та $s+1$ випадково генеровані елементи $\{t_0, ..., t_s\}$, $s-1$ елементи $t_1, ..., t_{s-1}$ насправді не потрібні: тільки β та t_0, t_s використовуються для дешифрування.

Зазначимо, що будь-який триплет форми $(\beta, g \cdot t_0, g \cdot t_s)$, де g є централізатором J (у тому числі, якщо $g \in Z$), може бути використаний для дешифрування шифртексту. Таким чином, існує багато еквівалентних секретних ключів. Задача криптоаналізу може бути спрощена при розгляді значно меншого класу відкритих та закритих ключів, чим у вихідному ви-

значенні. Це спрощення працює для усіх відповідних груп платформ, а не тільки для розглянутих вище Сузукі 2-груп.

Нехай (α,γ) буде відкритим ключем для MST_3 с $(\beta,(t_0,t_1,...,t_s))$ – відповідним секретним ключем. Запам'ятаємо, що $\alpha=[A_1,A_2,...,A_s]$ и $\beta=[B_1,B_2,...,B_s]$ та визначимо підмножини H_i через $\gamma=[H_1,H_2,...,H_s]$. Зазначимо, що алгоритм для отримання γ із закритого ключа передбачає, що $\gamma_{ij}=\beta_{ij}t_{i-1}^{-1}\alpha_{ij}t_i$. Визначимо елементи p_i,q_i та z_i через призначення $p_0=q_0=z_0=1$ та для $i\in\{1,2,...,s\}$ визначимо $p_i=\prod_{k=1}^{i}\alpha_{k1}, q_i=\prod_{k=1}^{i}\gamma_{k1}, z_i=\prod_{k=1}^{i}\beta_{k1}$.

Зауважимо, що факт того, що елементи β_{ij} знаходяться в центрі, передбачає, що

$$q_i=\prod_{k=1}^{i}\left(\beta_{k1}t_{k-1}^{-1}a_{k1}t_k\right)=z_it_0^{-1}p_it_i.$$

Визначимо $\alpha'=[A_1',A_2',...,A_s'],\gamma'=[H_1',H_2',...,H_s'],\beta'=[B_1',B_2',...,B_s']$ через

$$A_i'=p_{i-1}A_ip_i^{-1},$$
$$H_i'=q_{i-1}H_iq_i^{-1},$$
$$B_i'=z_{i-1}B_iz_i^{-1}.$$

Лема 1. Використовуємо позначене вище. Для усіх $i\in\{1,2,...,s\}$, перші елементи $\alpha_{i1}',\gamma_{i1}',\beta_{i1}'$ множин A_i',H_i',B_i' – усі дорівнюють одиниці.

Більш того, $\breve{\alpha}'(x)=\breve{\alpha}(x)p_s^{-1},\breve{\gamma}'(x)=\breve{\gamma}(x)q_s^{-1},\breve{\beta}'(x)=\breve{\beta}(x)z_s^{-1}$.

Зокрема, β' – логарифмічний підпис для Z та α' – покриття для деякої підмножини J' групи G.

Лема 2. Нехай (α,γ) буде відкритий ключ для MST_3 с $(\beta,(t_0,t_1,...,t_s))$ – відповідний закритий ключ. Визначимо α',γ' та β', як це зроблено раніше, та нехай $t_0'=t_1'=...=t_s'=t_0$. Тоді (α',γ') – публічний ключ для MST_3 із відповідним закритим ключем – $(\beta',(t_0',t_1',...,t_s'))$.

Доведення. Припустимо, що використовуємо α',β' та $t_0',t_1',...,t'$ для генерації відкритого ключа (α',δ), де $\delta=[D_1,D_2,...,D_s]$, тоді $\delta_{ij}=\beta_{ij}'(t_{i-1}')^{-1}\alpha_{ij}'t_i'$. Достатньо показати, що $\delta=\gamma'$, але

$$\delta_{ij}=\beta_{ij}'t_0^{-1}\alpha_{ij}'t_0=z_{i-1}\beta_{ij}z_i^{-1}t_0^{-1}\alpha_{ij}'t_0=z_{i-1}\beta_{ij}z_i^{-1}t_0^{-1}p_{i-1}\alpha_{ij}p_i^{-1}t_0$$
$$=\beta_{ij}z_{i-1}z_i^{-1}t_0^{-1}p_{i-1}\alpha_{ij}p_i^{-1}t_0=\beta_{ij}\beta_{i1}^{-1}t_0^{-1}p_{i-1}\alpha_{ij}p_i^{-1}t_0.$$

$t_0^{-1}p_{i-1}=z_{i-1}^{-1}q_{i-1}t_{i-1}^{-1}$ та $p_i^{-1}t_0=t_iq_i^{-1}z_i$.

Таким чином, $\delta_{ij}=\beta_{ij}\beta_{i1}^{-1}z_{i-1}^{-1}q_{i-1}t_{i-1}^{-1}\alpha_{ij}t_iq_i^{-1}z_i=\beta_{ij}q_{i-1}t_{i-1}^{-1}\alpha_{ij}t_iq_i^{-1}$.

З визначення z_i і, оскільки z_i є централом. Але $\gamma_{ij}'=q_{i-1}\gamma_{ij}q_i^{-1}=q_{i-1}\beta_{ij}t_{i-1}^{-1}\alpha_{ij}t_iq_i^{-1}$. Оскільки β_{ij} – є центром, маємо, що $\gamma_{ij}'=\delta_{ij}$, що та потрібно було довести.

Визначаємо проблему обмеження для MST_3 наступним чином. Вхід є відкритим ключем (α,γ) для MST_3 та випробуваний шифротекст (y_1,y_2). Відкритий ключ повинен мати додаткову властивість, що $\alpha_{i1}=\gamma_{i1}=1$ для $1\le i\le s$; відповідний закритий ключ повинен мати

властивість, що $t_0 = t_1 = ... = t_s$ та також, що $\beta_{i1} = 1$ для $1 \le i \le s$. Вихід є відкритим текстом p, що відповідає закритому (y_1, y_2).

Теорема 1. Існує скорочення поліноміального часу від проблеми OWE для MST_3 (для загальних ключів) до проблеми обмеженого OWE для MST_3 (дійсно, потрібен тільки один виклик оракла з обмеженим OWE).

Доведення. Нехай $O(\alpha, \gamma, y_1, y_2)$ буде ораклом для проблеми обмеженого OWE для MST_3. Показуємо, що цей оракл може бути використаний для вирішення проблеми OWE для MST_3 для загальних ключів.

Припустимо (α, γ) є (необмеженим) відкритим ключем із відповідним закритим ключем $(\beta, (t_0, t_1, ..., t_s))$. Нехай (y_1, y_2) випробуваним шифртекстом із відповідним повідомленням p. Припустимо, що отримаємо (α, γ) та (y_1, y_2). Визначимо (α', γ'), як це зроблено вище. Зауважимо, що α' та γ' може бути ефективно побудовано з α та γ з використанням тільки відкритої частини інформації. З Лем 1 та 2 (α', γ') є відкритим ключем із відповідним закритим ключем $(\beta', (t_0, t_0, ..., t_0))$, такі ключі задовольняють обмеженням. Визначимо $y_1' = y_1 p_s^{-1}$ та $y_2' = y_2 q_s^{-1}$. Зазначимо знову, що p_s та q_s визначені з використанням відкритої інформації, то що y_1' та y_2' можуть бути ефективно обчислені з отриманої інформації. Викликаємо оракла O на $(\alpha', \gamma', y_1', y_2')$ та отримаємо повідомлення p таке, що $(\alpha'(p), \gamma'(p)) = (y_1', y_2')$.

Тоді p – повідомлення, яке було нам необхідним, оскільки

$$\breve{\alpha}(p) = \breve{\alpha}'(p) p_s = y_1' p_s = y_1 p_s^{-1} p_s = y_1$$
$$\breve{\gamma}(p) = \breve{\gamma}'(p) \mathrm{q}_s = y_2' q_s = y_2 q_s^{-1} q_s = y_2 .$$

Практичні атаки на логарифмічні підписи

Нехай $m = 81$. Базової групою є Сузукі 2-група над полем F_q, де $q = 2^m$. Загальна атака потребує знаходження розміру q для успішності: фіксуємо $m = 81$, так, що ця загальна атака стає невідтворюваною. Зауважимо, що відкритий ключ вже доволі довгий, коли $m = 81$: у найбільш ефективному випадку розглянемо (дивиться приклад 1 нижче), нам потрібно більше 19 000 біт для зберігання елементів, які не є ідентифікаторами, в логарифмічних підписах α та γ. Методи суттєво не залежать від автоморфізму θ у визначенні Сузукі 2-групи, тому зафіксуємо θ такою, що дорівнює квадратичному автоморфізму в усіх експериментах.

Побудуємо логарифмічний підпис β та згенеруємо логарифмічні підписи типу $(r_1, r_2, ..., r_s)$, де $\prod_{i=1}^{s} r_i = 2^m$. Зауважимо, що цілі числа r_i повинні бути достатньо малими, щоб ефективно зберігати логарифмічні підписи. Першим кроком достатньо розглянути логарифмічні підписи, які мають додаткову властивість: елементи β_{i1} дорівнюють одиниці, тобто від самого початку генеруємо β з цією властивістю, та ніякий загал не втрачається під час генерації логарифмічних підписів таким чином.

У рамках задач криптоаналізу розглядаємо успішність атаки лише, якщо ми отримаємо дійсний закритий ключ після застосування невеликої кількості спроб вгадати t' за початкових умов для t як наслідок того, що β - бієктивне. Потім обираємо t' випадковим чином за цих умов.

Нагадаємо позначення $S(a,b)$ для елемента в Сузукі 2-групи, визначене в [2]. Спираючись на зауваження в [8], вважаємо, що $t = S(x,0)$, де $x \in \mathrm{F}_q$ невідомо, та тому обмежуємо припущення t' формою $S(y,0)$ для деяких $y \in \mathrm{F}_q$. Умови на t, які отримуємо, є F_2- лінійними умовами, тому легко обрати t', яке задовольняє цим умовам випадковим чином. Точні умови на t, які отримаємо, будуть залежати від кількості компонентів r_i типу β, що дорівнюють 2: коли таких компонентів багато, умова, яку отримаємо, слабкіше. З цієї причини приводимо ти випадки для ілюстрації методів. У прикладі 1 $r_i = 2$ для усіх i. У цьому випадку не знаходимо умов на t, але просто випадковий вибір невеликої кількості значень для t' призводить до успішної атаки. У прикладі 2 $r_i \neq 2$ для усіх i. У цьому випадку знаходимо, що кожна умова, яку отримаємо, обмежує t' такою невеликою кількістю можливостей, що можна провести незначний вичерпний пошук. Приклад 3 з приблизно половиною компонентів типу β, що дорівнює 2, ілюструє проміжний випадок. Тут кожна умова обмежує кількість можливостей для t' значно (приблизно до 2^{40} можливостей). Дуже небагато спроб вгадати t' можуть одночасно задовольняти двом з цих умов, тому поєднання двох умов дозволяє отримати еквівалентний закритий ключ шляхом незначного вичерпного пошуку.

Розглянемо приклад 1 для β типу $(2,2,...,2)$. У цьому випадку припускаємо, що β складається з 81 блоку довжиною 2. Такі логарифмічні підписи привабливі з точки зору ефективності: нам необхідно зберігати тільки 81 нетривіальний елемент в множині B_i, більш того, ці елементи формуються з базису Z, коли Z розглядається як 81-й мірний векторний простір над F_2 та обчислення з β можуть бути проведені з використанням простої лінійної алгебри (зауважимо, що це приклад канонічного логарифмічного підпису, як визначено в [8], однак атака, описана в цій статті, не працює в даному конкретному випадку).

Отримаємо відкриті й секретні ключі для MST_3 наступним чином. Довільно обираємо множину, що породжує $\{z_1,...,z_{81}\}$, для Z. Визначаємо елементи $d_{i2} \in \mathrm{F}_q$ через $z_i = S(0,d_{i2})$, таким чином елементи d_{i2} формують F_2 – базис для F_q. Обираємо $\beta = [B_1,...,B_{81}]$, де $B_i = \{1, S(0,d_{i2})\}$, потім генеруємо елементи $e_{i2}, f_{i2} \in \mathrm{F}_q$ випадковим чином та визначаємо $\alpha = [A_1,...,A_{81}]$, де $A_i = \{1, S(e_{i2}, f_{i2})\}$

Нехай $t = S(x,0)$, де $x \in \mathrm{F}_q$ – задано випадковим чином. Будуємо γ, як це описано у визначенні MST_3. Тобто, визначаємо

$$\gamma_{i2} = \beta_{i2} t^{-1} \alpha_{i2} t = S(0,d_{i2}) S(x, x^{\theta} x) S(e_{i2}, f_{i2}) S(x,0) =$$

$$= S(e_{i2}, d_{i2} + f_{i2} + e_{i2} x^{\theta} + e_{i2}^{\theta} x) =: S(e_{i2}, g_{i2})$$

і обираємо $\gamma = [C_1,...,C_{81}]$, де $C_i = \{1, \gamma_{i2}\}$.

Атака реалізується наступним чином. Нехай $t' = S(y,0)$ буде випадкова спроба вгадати t. Формуємо $b = [B_1,...,B_{81}]$, де $B_i = \{1, b_{i2}\}$ та b_{i2} задано як

$$b_{i2} = \gamma_{i2} t'^{-1} \alpha_{i2} t' = S(e_{i2}, g_{i2}) S(y, y^{\theta} y) S(e_{i2}, e_{i2}{}^{\theta} e_{i2} + f_{i2}) S(y,0)$$
$$= S(0, g_{i2} + f_{i2} + e_{i2} y^{\theta} + e_{i2}^{\theta} y)$$

Якщо множина $\{b_{i2}\}_{i=1}^{81}$ є лінійно незалежною, то $\tilde{b}$ є бієкцією, та з [9] випливає, що маємо еквівалентний секретний ключ. Якщо множина лінійно залежна, повторюємо цей процес з другою спробою здогадки t'. В роботі [12] цю атаку було згенеровано для 10 000 випадкових екземплярів MST_3. Результати наведені в табл. 1.

Середня кількість здогадок для t' перед тим, як знайти еквівалентний секретний ключ, склала приблизно 3,47. Таким чином, схема у цьому випадку небезпечна.

Таблиця 1

Експериментальні результати для Прикладу 1

Кількість здогадок t'	1	2	3	4	5	6	7	8	9
Частота	2829	2111	1429	1048	799	490	374	279	181
Кількість здогадок t'	10	11	12	13	14	15	16	17	18
Частота	133	98	66	47	31	26	19	11	5
Кількість здогадок t'	19	20	21	22	23	24	25	26	27
Частота	3	7	7	4	2	1	0	0	0

Розглянемо Приклад 2 для β типу $(8,64,64,...,64)$. Уданому випадку використовувані логарифмічні підписи складаються з одного блоку розміром 8 та тринадцять блоків розміром 64. Побудуємо β наступним чином. Виробляємо випадковий базис $\{z_1,...,z_{81}\}$ для Z.

Розглянемо ланцюжок підгруп $1 = Z_0 < Z_1 < ... < Z_{27} = Z$, де $Z_i = \langle z_1,...,z_{3i} \rangle$ для $1 \le i \le 27$. Формуємо поперечний логарифмічний підпис типу $(8,8,...,8)$ (з 27 блоками), чий i – й блок є поперечним для Z_{i-1} в Z_i, містить тотожність якості першого елементу. Потім випадковим чином поєднуємо 26 блоків розміром 8 по парах, щоб сформувати 13 блоків розміром 64. Шляхом передупорядковування блоків побудували ATLS $\beta = [B_1, B_2, \ldots, B_{14}]$ типу $(8,64,64,...,64)$ для Z. Визначимо елементи $d_{ij} \in F_q$ через $\beta_{ij} = S(0, d_{ij})$.

Генеруємо елемент $t = S(x,0)$, елементи $\alpha_{ij} = S(e_{ij}, f_{ij})$, елементи $\gamma_{ij} = S(e_{ij}, g_{ij})$ та накриття α та γ, як у Прикладі 1. Зокрема має місце рівність $g_{ij} = d_{ij} + f_{ij} + e_{ij}^{\theta} x + e_{ij} x^{\theta}$.

Атака відновлює секретний ключ безпосередньо невеликим вичерпним пошуком замість того, щоб вгадувати еквівалентний секретний ключ. З [12] витікає, що існує i та j таке, що $j \ge 2$ і $B_i \cdot b_{ij} = B_i$. Для i та j існує лише невелика кількість можливостей (з використанням незначного вичерпного пошуку); можемо припустити, що дійсний вибір для i та j відомий. Знаємо, що $d_{ij} = g_{ij} + f_{ij} + e_{ij}^{\theta} x + e_{ij} x^{\theta}$. Більш того, коли $B_i \cdot b_{ij} = B_i$, має місце рівність $d_{ij} + d_{ik} = d_{il}$ щонайменше $|B_i| - 2$ пар індексів k, l, де $2 \le k, l \le |B_i|$ та де j, k та l різні. Записуючи u_{ijkl} для $u_{ij} + u_{ik} + u_{il}$, отримаємо рівняння $g_{ijkl} + f_{ijkl} = e_{ijkl}{}^{\theta} x + e_{ijkl} x^{\theta}$.

Зазначимо, що елементи e_{ijkl}, f_{ijkl} та g_{ijkl} є відомими (формуючи частину відкритого ключа (α,γ)), але χ залишається невідомим. Для заданого $e\in \mathrm{F}_q$ відображення $\phi_e : \mathrm{F}_q \to \mathrm{F}_q$, задане за допомогою $x \mapsto e^o x + e x^o$ є F_2- лінійним відображенням. Більш того, коли $e\neq 0$, маємо, що ϕ_e є ядром розміру 2. Припустимо (у самому найкращому випадку), що e_{ijkl} не дорівнює нулю, отримаємо, що кожне таке рівняння виконується не більше ніж двома можливостями для χ (і ці варіанти легко обчислюються з використанням елементарної лінійної алгебри). Є менше 2^{18} варіантів для i, j, k та l. Як тільки ці вибори фіксовані, існує не більше 2 значень для χ, які задовольняють рівнянню. Таким чином, можемо відновити χ вичерпним пошуком, хоча 2^{20} можливостей (для кожної можливості для χ можемо побудувати b та перевірити, чи є $\tilde{b}$ бієкцією: ця перевірка може бути ефективно виконана для ATLS.). Зазначимо, що у цій атаці значним чином використовується той факт, що $|B_i|>2$, якщо $|B_i|=2$, то припустимих варіантів для j та k немає. Зазначимо також, що коли маємо правильне значення для i та j, той саме елемент χ буде знайдений щонайменше $|B_i|-2$ разів рішення рівняння при j та k, що змінюються за усіма можливими значеннями. Це спостереження можна використовувати для більш ефективного відновлення χ. Нарешті, зазначимо, що коли i правильно вгадується, множина B_i має властивість, що добуток його елементів повинен бути тотожнім (оскільки те саме вірно для будь-якого суміжного класу підгрупи Z порядку 4 або більше). Цю властивість можна використовувати для знаходження χ без необхідності вгадати j,k або l. Реалізуємо атаку з використанням SAGE на стандартному ПК, та в кожному запуску довільно обране секретне значення χ було повернено правильно протягом 30 хвилин. Таким чином, у цьому випадку криптосистема MST_3 також небезпечна.

Розглянемо приклад 3 для β типу $(2,2,...2,16,16,...,16)$. Нарешті, розглянемо випадок, коли β складається з 41 множини розмірів 2 та10 множин розміру 16. У цій ситуації рівняння не обмежує число можливостей для χ достатнім чином та тому об'єднуємо два рівняння для відновлення χ.

Побудуємо β, починаючи з ланцюжка підгруп $1=Z_0<Z_1<...<Z_{61}=Z$, де кожен Z_i має індекс 2 в Z_{i+1} при $0\le i\le 40$ та індекс 4 для $41\le i\le 60$. Формуємо випадковий поперечний логарифмічний підпис для цього ланцюжка (враховуючи тотожність як перший елемент в кожному поперечному): цей логарифмічний підпис буде складатися з 41 множини розмірів 2 та 20 множин розміру 4. Потім поєднуємо 20 множин розміру 4 в пари, щоб сформувати 10 множин розміру 16, де поєднання цих множин обирається випадковим чином. Результатом є ATLS $\beta=[B_1,B_2,...,B_{41},B_{42},...,B_{51}]$ того типу, який шукаємо. Потім обираємо t та α та будуємо, як і раніше, γ.

Таблиця 2

Експериментальні результати для прикладу 2

Номер можливих χ	0	1	2	4	8	16
Розподіл правильних індексів	0	579	386	33	2	0
Розподіл неправильних індексів	276	543	170	10	1	0

У даному випадку атака реалізується наступним чином. Визначимо підгрупу $H=\langle B_1,...,B_{41}\rangle$. Визначимо $\beta_{ij}=S(0,d_{ij})$ та $V=\langle d_{i2}:1\le i\le 41\rangle$. Зауважимо, що V має розмі-

рність 41 та $H=\{S(0,v):v\in V\}$. Зрозуміло, що образ $[B_{42},...,B_{51}]$ в Z/H є ATLS для Z/H та не містить блоків розмірами 2. Таким чином, можемо продовжувати аналогічно Прикладу 2, на цей раз працюючи в частці Z/H, щоб вивести рівняння, що x повинно задовольняти за модулем V. Використовуючи позначення з Прикладу 2, отримаємо рівняння виду $g_{ijkl}+f_{ijkl}+V=\phi_{e_{ijkl}}(x)$, де $\phi_{e_{ijkl}}$ є F_2- лінійним відображенням. У припущенні, що e_{ijkl} відмінний від нуля, рівняння цієї форми обмежує χ лежати в афінному підпросторі з розміром не більше 42, тому зменшили розмір вичерпного пошуку можливостей χ до 2^{42}. Але правильне припущення для i означає, що χ задовольняє хоча б $|B_i|-2\geq 2$ таких рівнянь, як j,k та l змінюються. Якщо правильно вгадуємо дві такі комбінації j,k та l, знаємо, що χ лежить в перетині двох афінних підпросторів розмірності не більше 42 (а саме, множини рішень, що відповідають двом рівнянням), та це зменшує кількість можливостей для χ до незначного числа. Дійсність кожної можливості для χ можна визначити, перевіривши бієкцію $\breve{b}$, як у прикладі 2.

Під час реалізації цієї ідеї створили 1 000 випадкових ATLS для Z/H. Для кожного ATLS обирали випадкову пару рівнянь, де індекси i,j,k та l були правильно вгадані, та обчислили розмір перетинів двох множин рішень. Зробили те саме, коли індекси були вгадані неправильно, щоб перевірити, що кількість можливостей для χ у цьому випадку не дуже велика. Записуємо результати в табл. 2.

Як видно з табл. 2, у будь-якому випадку число можливостей для χ невелике. Для перевірки необхідно менше 2^{20} пар рівнянь, та тому зазвичай очікуємо вичерпний пошук χ, розміром не більше 2^{24} (крім того, у цьому пошуку очікуємо, що знаходження χ буде відбуватися з відносно високою частотою, так як воно з'являється для кожної правильної пари рівнянь).

Висновки

Атаки на криптосистему MST_3 в її базовій конструкції призводять до її компрометації. Базовим елементом криптосистеми MST_3 є логарифмічні підписи – особливий вид факторизації. Методи генерації логарифмічних підписів суттєво впливають на безпеку конструкції. Зауважимо, що доки не буде винайдено метод створення безпечних слабких логарифмічних підписів, MST_3 небезпечна. Багато атак експлуатують проблеми базової конструкції з використанням Сузукі-2 груп. Більшість атак може буде імплементовано з використанням доступних обчислювачів. Водночас саме розуміння архітектури атаки стимулює спроби використання інших підходів до забезпечення потрібного рівня безпеки, на кшталт використання гомоморфного шифрування у якості додаткового елемента посилення конструкції [14], використання посилених логарифмічних підписів [15]. В останні роки, використовуючи обґрунтовані властивості неабелевих груп [16], результати робіт з пошуку кращих за характеристиками логарифмічних підписів [17], дослідникам вдалось запропонувати посилені конструкції криптосистеми MST_3 за рахунок застосування узагальнених груп [18], автоморфізмів груп [19, 20] та груп з посиленими параметрами безпеки [21]. Підсумовуючи, зауважимо, що доки не буде винайдено метод створення безпечних слабких логарифмічних підписів, MST_3 небезпечна.

Список літератури:

1. Kotukh Y., Khalimov G. Hard problems for non-abelian cryptography // 2021: Fifth International Scientific and Technical Conference "COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES", 2021, pp39-40, https://doi.org/10.30837/csitic52021232176

2. Lempken W. A public key cryptosystem based on non-abelian finite groups / W. Lempken, T. van Trung,

S.S. Magliveras, W. Wei // Journal of Cryptology. 2009. Vol. 22 (1). P. 62–74.

3. Gonzáles Vasco M. I. On minimal length factorizations of finite groups / M. I. Gonzáles Vasco, M. Rotteler, R. Steinwandt // Experimental Mathematics. 2003. Vol. 12 (1). P. 1–12.

4. Singhi N. Minimal logarithmic signatures for finite groups of Lie type / N. Singhi, N. Singhi, S. Magliveras // Designs, Codes and Cryptography. 2010. Vol. 55 (2). P. 243–260.

5. Magliveras S. New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups / S. Magliveras, D. Stinson, T. van Trung // Journal of Cryptology. 2002. Vol. 15. P. 285–297.

6. Goldreich O. Foundations of Cryptography: Basic Tools // Cambridge University Press. 2001.

7. Nuss A. On group based public key cryptography [Electronic resource] : Phd thesis. Access mode : http://nbn-resolving.de/urn:nbn:de:bsz:21-opus-63659.

8. Blackburn S. R. Cryptanalysis of the MST 3 public key cryptosystem / S. R. Blackburn, C. Cid, C. Mullan // Journal of Mathematical Cryptology. 2009. Vol. 3 (4). P. 321–338.

9. Bohli J. Weak keys in MST / J. Bohli, M. I. Gonzáles Vasco, C. J. M. Martínez, R. Steinwandt // Designs, Codes and Cryptography. 2005. Vol. 37 (3). P. 509–524.

10.Caranti A. The round functions of cryptosystem PGM generate the symmetric group / A. Caranti, F. D. Volta // Designs, Codes and Cryptography. 2006. Vol. 38 (1). P. 147–155.

11.Magliveras S. Algebraic Properties of Cryptosystem PGM / S. Magliveras, N. D. Memon // Journal of Cryptology. 1992. Vol. 5 (3). P. 167–183.

12.Mullan, Ciaran. Some Results in Group-Based Cryptography. (2011)//Thesis

13.Svaba P. and T. van Trung. Public key cryptosystem MST3 cryptanalysis and realization // Journal of Mathematical Cryptology. Vol.4. No.3. Pp.271–315,2010

14.Cong Y., Hong H., Shao J., Han S., Lin J. and Zhao S. A New Secure Encryption Scheme Based on Group Factorization Problem // IEEExplore, November 20, 2019 Digital Object Identifier 10.1109/ACCESS.2019.2954672 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8907845

15.T. van Trung. Construction of strongly aperiodic logarithmic signatures // J. Math. Cryptol. Vol. 12. No. 1. Pp. 23-35, 2018

16.Kotukh Y., Severinov E., Vlasov O., Tenytska A., Zarudna E. Some results of development of cryptographic transformations schemes using non-abelian groups. Radiotekhnika. 2021. No. 204. P. 66–72. https://doi.org/10.30837/rt.2021.1.204.07

17.Kotukh E., Severinov O., Vlasov A., Kozina L., Tenytska A., Zarudna E. Methods of construction and properties of logariphmic signatures . *Radiotekhnika* 2021. No 205. P. 94–99. https://doi.org/10.30837/rt.2021.2.205.09

18.Khalimov G. MST_3 Cryptosystem Based on a Generalized Suzuki 2-Groups [Electronic resource] / G. Khalimov, Y. Kotukh, S. Khalimova. Access mode : http://ceur-ws.org/Vol-2711/paper1.pdf

19.Khalimov G., Kotukh Y., Khalimova S. MST3 cryptosystem based on the automorphism group of the hermitian function field' // IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 – Proceedings, 2019. Pp. 865 – 868.

20.Khalimov G., Kotukh Y., Khalimova S. Encryption scheme based on the automorphism group of the Ree function field // 2020 7th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2020, 2020, 9340192.

21.Khalimov G., Kotukh Y., Didmanidze I., Sievierinov O., Khalimova S., Vlasov A. Towards three-parameter group encryption scheme for MST3 cryptosystem improvement // 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), 2021, pp. 204-211, doi: 10.1109/WorldS451998.2021.9514009.

Надійшла до редколегії 03.08.2021

Відомості про авторів:

Котух Євген Володимирович – канд. техн. наук, доцент, кафедра комп'ютерних наук, Сумський державний університет, Україна, e-mail: yevgenkotukh@gmail.com

Охріменко Тетяна Олександрівна – канд. техн. наук, докторант, старший науковий співробітник науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі, Національний авіаційний університет, Київ, Україна. e-mail: t.okhrimenko@nau.edu.ua

Дяченко Оксана Федорівна – канд. пед. наук, доцент кафедри системного аналізу та інформаційних технологій, Маріупольський державний університет, Маріуполь, Україна. e-mail: o.dyachenko@mdu.in.ua

Ротаньова Наталія Юріївна – канд. пед. наук, доцент, доцент кафедри системного аналізу та інформаційних технологій, Маріупольський державний університет, Маріуполь, Україна. e-mail: n.rotaneva@mdu.in.ua

Козіна Лідія Сергіївна – здобувач вищої освіти, кафедра інформаційних та комп'ютерних систем, Національний університет "Чернігівська політехніка", Чернігів, Україна, e-mail: lidiia.kozina@gmail.com

Зеленський Данїїл Володимирович – здобувач вищої освіти, факультет комп'ютерних наук, Харківський національний університет радіоелектроніки, Харків, Україна.

РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ

УДК 004.89: 621.396 **DOI:10.30837/rt.2021.3.206.10**

В.В. ЖИРНОВ, канд. техн. наук, С.В. СОЛОНСКАЯ, канд. техн. наук,
В.И. ЗАРИЦКИЙ, канд. техн. наук

МЕТОД БОРЬБЫ С НЕСТАЦИОНАРНЫМИ ЕСТЕСТВЕННЫМИ И ИМИТИРУЮЩИМИ ПОМЕХАМИ В ИНТЕЛЛЕКТУАЛЬНЫХ ОБЗОРНЫХ РЛС

Введение

Рассмотрены актуальные вопросы защиты РЛС от нестационарных естественных и имитирующих искусственных помех на основе интеллектуального анализа сигнальной отметки. Предложены универсальные алгоритмы автоматизации операций обработки информации, обеспечивающие эффективную идентификацию ложных отметок за счет семантических признаков флуктуаций радиолокационной отметки. Показано, как этот подход может использоваться для быстрого автоматического обнаружения и распознавания ложных отметок воздушных и надводных объектов. В разработанную технологию системы входят процедуры формализации и анализа символьной модели изображения наблюдаемых объектов для принятия решений, основанных на прецедентах.

Известно, что обзорные РЛС, использующие как сложные сигналы с внутриимпульсной модуляцией, так и локаторы обычного типа, подвержены воздействию нестационарных естественных, например типа «ангел-эхо», и преднамеренных имитирующих помех. Для создания преднамеренных имитирующих отметок противник использует внесение амплитудной модуляции в ретранслируемый зондирующий сигнал РЛС [1, 2]. В результате анализа удалось выяснить, что в имитирующих помехах, полученных путем размножения амплитудной модуляцией, появляются так называемые «интеллектуальные» флуктуации пачечной структуры ложных отметок, которые отличаются от флуктуаций пачек реальных отметок и могут быть легко обнаружены человеком-оператором [3, 4]. Это объясняется тем, что при переизлучении с различной задержкой образуется пачка многократных помех и различия, вводимых амплитудной модуляцией флуктуаций связаны с различием в форме между отраженными от реальной цели сигналами и имитирующими сигналами.

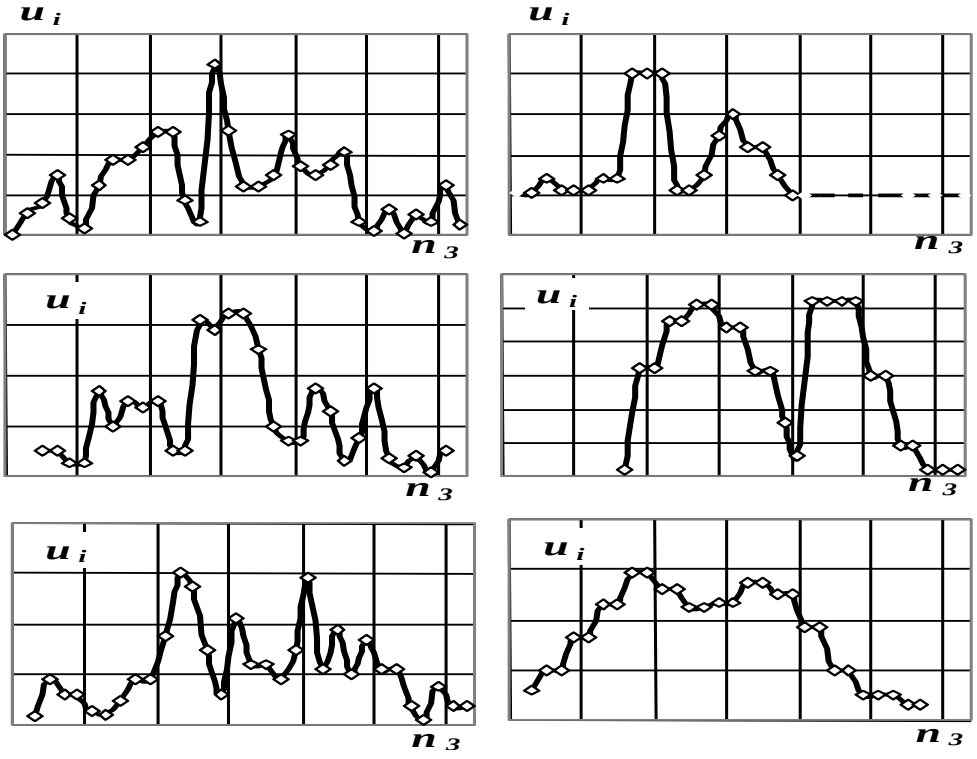
Анализ состояния проблемы показывает, что интеллектуальными считают системы [4, 5], которые могут решать комплекс задач, выполняемых человеком-оператором, или осуществляют поддержку принятия решений. В радиолокационных системах контроля подвижных объектов на воздушном и надводном транспорте используют методы обнаружения и распознавания сигналов [6, 7]. Основной недостаток в известных методах состоит в низкой автоматизации процедур обработки данных, в том числе при обнаружении, распознавании и принятия решений о нестационарных естественных и имитирующих искусственных помехах.

Символьная модель изображений амплитудных флуктуаций пачки сигналов от нестационарных естественных и имитирующих помех и от реальных объектов

Символьная модель процессных знаний формирования и анализа изображений амплитудных флуктуаций пачки импульсных сигналов – это математическое описание процедур и отношений при восприятии и анализе сигналов человеком-оператором в виде различительных признаков (или свойств) для определения типов объектов [8]. Такое математическое описание процессов деятельности эксперта называется идентификацией. Процессы действий эксперта можно идентифицировать прямо и косвенно. При прямой или логической идентификации действий оператора рассматриваем, что для определенного действия оператора поступают сигналы (виды амплитудных флуктуаций пачки), выбираемые из некоторого

множества амплитудных составляющих пачки, и регистрируются ответные сигналы. Всевозможные ответные сигналы деятельности оператора образуют множество.

В ходе исследований типов флуктуаций пачки использовались реальные экспериментальные данные (рис. 1), полученные на обзорной РЛС сантиметрового диапазона (длительность импульса 1 мкс, частота зондирования 365 Гц, период обзора 10 с).



а *б*

Рис.1. Пачка сигналов от ложных (*а*) и от реальных (*б*) объектов

В результате анализа картин флуктуаций радиолокационной пачки в амплитудной области для нестационарных имитирующих искусственных помех и естественных мешающих отражений типа «ангел-эхо» (рис. 1, *а*) и воздушных объектов (рис. 1, *б*) классифицированы на некоторое количество типов.

Семантическая модель процессных знаний для идентификации нестационарных естественных и имитирующих искусственных помех

В разработанную символьную модель входят процедуры формализации и анализа геометрического сигнального образа пачки от наблюдаемых объектов на основе алгебры предикатов [9 – 11] и операций создания предикатной (семантической) модели процессных знаний для получения решений о наблюдаемых объектах локации на основе методов интеллектуального анализа реальных процессов. Пусть $M = \{q_{11}, q_{12}, ..., q_{ij}, ..., q_{mn}\}$ множество, представляющее собой матрицу $\|A\|$ размерностью $M \times N$, состоящее из элементов $k = m \times n$ – значений амплитуд сигналов в элементах обработки зоны или сектора обзора РЛС, а B – некоторое из его подмножеств $B \subseteq M$, амплитуды сигналов которого q_{ij} превышают пороговые значения V_{ij}. Составляем набор логических элементов t_{ij} по следующему принципу: если $q_{ij} \in B$, то $t_{ij} = 1$; если $q_{ij} \notin B$, то $t_{ij} = 0$, $i = \overline{1,m}$, $j = \overline{1,n}$.

Предикат $A(x)$ на множестве M, соответствующий множеству B элементов обработки, превысивших порог, с характеристикой $(t_{11}, t_{12}, \cdots, t_{ij}, \cdots, t_{mn})$, запишется формулой

$$A(x) = t_{11}x^{q_{11}} \vee \ldots \vee t_{mn}x^{q_{mn}} = \bigvee_{i=1,\, j=1}^{mn} t_{ij}x^{q_{ij}} \tag{1}$$

Здесь выражение $x^{q_{ij}}$ – форма узнавания события. Когда $x = q_{ij}$, то $x^{q_{ij}} = 1$.

Семантическая (предикатная) модель процессных знаний формирования и анализа изображений амплитудных флуктуаций пачки импульсных сигналов от наблюдаемых воздушных или наземных объектов в общем виде – это система n унарных и бинарных предикатов Z_j:

$$M = \left\{ Z_j, \;\; j = 1..n \right\}. \tag{2}$$

Такая система предикатов позволяет описать ситуацию вокруг анализируемой в данный момент информационной ячейки и позволяет формализовать процесс формирования символьного изображения отметки $A(x)$ в течение ряда циклов зондирований РЛС. Их еще называют атрибутами или предикатными признаками процесса. Например, для радиолокационных систем обзора пространства это могут быть:

– унарный предикат Z_{pij} присутствия или наличия сигнала в a_{ij} информационной ячейке; i, j – номера элементов зоны обзора РЛС;

– бинарный предикат $Z_{d\,ij}$ ухода сигнала из a_{ij} в соседнюю по дальности информационную ячейку;

– бинарный предикат $Z_{a\,ij}$ перехода сигнала в смежную по азимуту или соседнюю информационную ячейку, прилегающую к рассматриваемой ячейке.

При таких исходных условиях эти предикатные признаки формируются по следующим правилам:

$$Z_{p\,ij} = 1, \text{ при } A_{ij} > 0 \tag{3}$$

$$Z_{d\,ij} = 1, \text{ при } A_{i-1\,j} > 0 \wedge Z_{p\,ij} = 1 \tag{4}$$

$$Z_{a\,ij} = 1, \text{ при } Z_{p\,ij} = 1 \wedge A_{ij-1} > 0, \tag{5}$$

где A_{ij} – предикат события наличия-отсутствия сигнала в соответствующем элементе анализа.

Для радиолокационных станций (РЛС) обзора пространства семантическая модель флуктуаций огибающей пачки описывается двумя составляющими [7]:

1. Предикатным признаком символьной модели пачки сигналов (отметок) воздушных объектов, определяемым как решение уравнения

$$I_{m1} = Z_{mij} = \bigwedge_{l_1}^{l_n} Z_{ai,\,j+l_n} = 1 \cdot \tag{6}$$

2. Предикатной моделью амплитудных флуктуаций радиолокационной пачки, определяемой как совокупность произведений каждого элемента символьной пачки на их амплитудные значения:

$$I_{m2} = \bigvee_{l_1}^{l_n} q_{i,j+l_n} Z_{ai,j+l_n} \quad (7)$$

где l_1, l_n – номера элементов начала и конца пачки.

На рис. 2 приведены реальные, экспериментально полученные картины пачек импульсов от естественных мешающих помех типа «ангел-эхо» и имитирующих летающие объекты помех. В формулах (6) и (7) предусмотрена возможность проверки связей различного типа между информационными единицами. Прежде всего, эти связи характеризуют отношения между информационными единицами. Семантика отношений носит и декларативный, и процедурный характер. С другой стороны процесс, как правило, описывается как функциональными связями, так и отношениями между информационными ячейками. Имея предикатные признаки, мы можем формализовать процессные знания получения символьных моделей нестационарных сигнальных отметок, как для помех типа «ангел-эхо», так и для имитирующих летающие объекты помех [12, 13].

При этом две информационные единицы могут быть связаны отношением "причина – следствие". Это могут быть: отношение появления сигнала в a_{ij} ячейке (предикатный признак $Z^k_{p\,ij}$ присутствия сигнала); отношение ухода сигнала из a_{ij} ячейки (предикатный признак $Z_{d\,ij}$ ухода сигнала); и отношение "соседней ячейки" (предикатный признак $Z_{a\,ij}$ перехода сигнала в смежную по азимуту информационную ячейку). Приведенные отношения характеризуют декларативные знания.

Если между двумя информационными единицами установлено отношение "аргумент – функция", то оно характеризует процессное знание, связанное с вычислением определенных предикатных функций. Исследуем возможные операции.

Для этого составляем предикатные уравнения возможных состояний и путем их решения определяем номера $k = k_1$ и $l = l_1$ рядом расположенных элементов обработки с предикатными признаками $Z_{d\,ij}$ и $Z_{a\,ij}$ соседнего элемента обработки. Определяем также, с какими из этих признаков работать. Для этого при появлении предиката $Z_{p\,ij}$ наличия сигнала в a_{ij} информационной ячейке составляем предикатные уравнения для проверки возможности формирования бинарного предиката $Z_{d\,ij}$ (прихода сигнала из соседней по дальности $a_{i-1\,j}$ ячейки) и бинарного предиката $Z_{a\,ij}$ (перехода сигнала из смежной по азимуту a_{ij-1} ячейки), полученные из условий (4) и (5)

$$(A_{i-1\,j} > 0 \wedge Z_{p\,ij} = 1) = 1; (Z_{p\,ij} = 1 \wedge A_{ij-1} > 0) = 1. \quad (8)$$

Из анализа вариантов решений уравнений (8) можно сделать следующие выводы:

1. Если выполняется 1-е уравнение, то формируется бинарный предикат $Z_{d\,ij}$. Это означает, что сигнал в исследуемую ячейку переходит из соседней по дальности $a_{i-1\,j}$ ячейки и начинает формироваться новая символьная модель сигнальных отметок для протяженных неподвижных объектов типа облака, тучи или атмосферной неоднородности типа «ангел-эхо»;

2. Если выполняется 2-е уравнение, то формируется бинарный предикат $Z_{a\,ij}$. Это означает, что сигнал в исследуемую ячейку переходит из соседней по азимуту a_{ij-1} ячейки и начинает формироваться новая символьная модель (пачка) сигнальных отметок для точечных подвижных и малоподвижных летательных аппаратов типа самолет, вертолет, БПЛА.

Каждый тип амплитудной картины S_j, приведенный на рис. 2, имеет соответствующие нули и единицы согласно предикатной функции $A(x)$. Тип S_1 имеет одиночные группы единиц среди всех остальных нулей. Тип S_2 имеет две группы единиц, а количество нулей между ними меньше или равно двум.

Метод семантической обработки символьного изображения

Для идентификации с амплитудными типами была сформирована система предикатов-признаков $\mathrm{L_i}$, «чувствительных» к количеству и разрывности нулей, единиц и групп сомкнутых единиц (амплитудных пиков) в предикате $A(x)$.

Был введен еще один вид предиката – F(y), построенный на множестве F, элементы $\mathrm{f_1, f_2, ..., f_{k-1}}$ которого определены путем суммирования по модулю два каждого элемента $\mathrm{t_i}$ со смежным элементом. Для определения количества амплитудных пиков использована арифметическая сумма Ф предиката $F(t)$ $\Phi = \sum_{i}^{k-1} f_i = \sum_{i=1}^{k-1} [t_i + t_{i+1}] \big| M_2$, где индекс $\big| M_2$ означает суммирование по модулю два. Анализ возможных значений Φ для различных типов амплитудных картин показывает, что для одиночной группы сомкнутых единиц в множестве F результат суммирования всегда равен двум, независимо от ширины пика, т.е. от количества сомкнутых единиц. Для двух групп сомкнутых единиц результат такой операции равен четырем, для трех пиков – шести и т.д. В признаке $\mathrm{L_1^{j_i}}$, верхний индекс $\mathrm{j_i}$ указывает на наличие в предикате f(x) на количество амплитудных пиков и определяется по следующему правилу: если Ф≥2, то $\mathrm{j_i}$ = Ф/2, иначе $\mathrm{j_i}$ = 0. В модели $\mathrm{j_i = P_i}$.

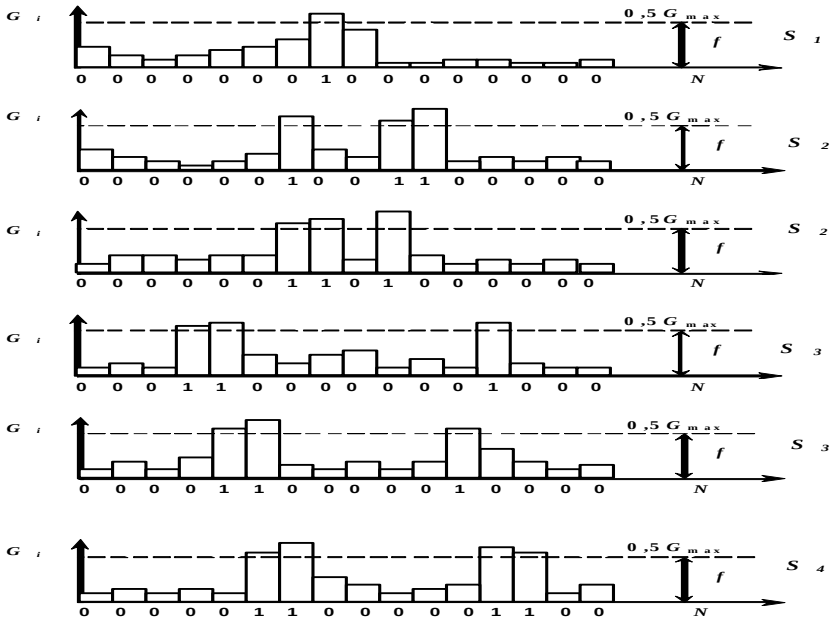


Рис. 2. Типы амплитудных картин флуктуаций пачек сигналов

Введен признак $\mathrm{L_2^{l_i}}$, верхний индекс которого или номер предиката $\mathrm{l_i}$ указывает на количество нулей между группами единиц в предикате A(x). В модели $\mathrm{l_i = L_i}$. Для учета отличий амплитудных картин по энергетике принятого сигнала введен признак $\mathrm{L_3^{s_i}}$, верхний индекс которого указывает на количество единиц в предикате A(x). В модели $\mathrm{s_i = E_i}$.

Алгоритм идентификации типов S_j для амплитудных картин, представленных на рис. 2, описывается следующими уравнениями:

$$
\begin{aligned}
S_1 &= L_1^1 \wedge L_2^0 \wedge (L_3^1 \vee L_3^2);\\
S_2 &= L_1^2 \wedge (L_2^0 \vee L_2^1 \vee L_2^2 \vee L_2^3) \wedge (L_3^2 \vee L_3^3 \vee L_3^4);\\
S_3 &= L_1^2 \wedge (L_2^5 \vee L_2^6 \vee L_2^7 \vee L_2^8) \wedge L_3^3;\\
S_4 &= L_1^2 \wedge (L_2^4 \vee L_2^5 \vee L_2^6) \wedge (L_3^4 \vee L_3^5 \vee L_3^6)\\
S_j &= (L_1^0 \vee L_1^1 \vee \ldots \vee L_1^j) \wedge (L_2^0 \vee L_2^1 \vee \ldots \vee L_2^{l_i}) \wedge (L_3^1 \vee L_3^2 \vee \ldots \vee L_3^{s_i})
\end{aligned}
\qquad (9)
$$

В общем виде (9) можно представить так:

$$
S_j = \left(\bigvee_{j_1}^{j_2} L_1^j \right) \wedge \left(\bigvee_{l_1}^{l_2} L_2^l \right) \wedge \left(\bigvee_{s_1}^{s_2} L_3^s \right). \qquad (10)
$$

На основе полученных уравнений разработана функциональная схема алгоритма определения типов флуктуаций пачки, приведенная на рис. 3.

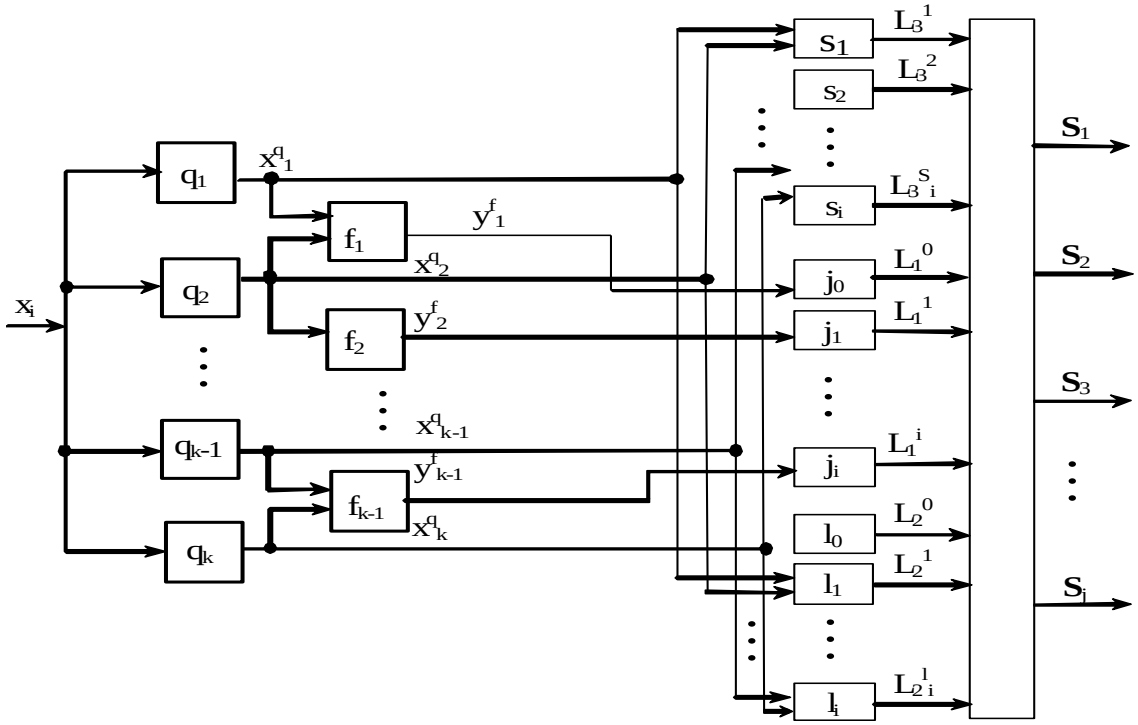


Рис. 3. Схема алгоритма определения типов флуктуаций пачки

По полученной совокупности признаков-предикатов L_i спектральный образ однозначно соотносится с одним из типов спектра S_j. Распознавание воздушных объектов осуществляется по результатам идентификации спектральных типов.

Верификация предложенной модели проводилась на реальных данных (рис. 2), полученных на обзорной РЛС сантиметрового диапазона. На основе этих данных смоделированы типы характерных пачек радиолокационных сигналов. По результатам модельных экспериментов все они были правильно идентифицированы. Таким образом, все операции по классификации и распознаванию воздушных объектов выполняются автоматически и в реальном масштабе времени.

Заключение

1. Разработан метод защиты обзорных РЛС от нестационарных естественных и имитирующих искусственных помех. В основе способа лежит интеллектуальный анализ символьного изображения радарных отметок. Предложены универсальные алгоритмы автоматизации операций обработки информации, обеспечивающие эффективную идентификацию ложных отметок за счет семантических признаков флуктуаций радиолокационной отметки. Показано, как этот подход может использоваться для быстрого автоматического обнаружения и распознавания ложных отметок воздушных и надводных объектов. В разработанную технологию системы входят процедуры формализации и анализа символьной модели изображения наблюдаемых объектов для принятия решений, основанных на прецедентах.

2. Реализован метод семантической обработки символьного изображения для обзорных радиолокационных систем. Для идентификации типов амплитудных флюктуаций вводятся семантические признаки-предикаты, по их сочетанию любая картина однозначно соотносится с одним из типов, согласно разработанным уравнениям предикатных операций. На основании полученных уравнений синтезирована функциональная схема определения типов картин. На основе этих данных смоделированы типы характерных пачек радиолокационных сигналов. По результатам модельных экспериментов все они были правильно идентифицированы.

Список литературы:

1. Карманов Ю.Т., Непомнящий Г.А Способ защиты РЛС со сложным сигналом от имитирующей помехи // Вестник ЮУрГУ. 2009. №26. С. 41–46.
2. Тенденции развития авиационных средств радиоэлектронной борьбы ВВС США / Я.Н. Кожушко [и др.] // Наука і техніка Повітряних Сил Збройних Сил України. 2011. № 2(6). С. 44–48.
3. Миллиметровая радиолокация. Методы обнаружения и наведения в условиях естественных и организованных помех / А.Б. Борзов и [др.]. Москва : Радиотехника, 2010. 376 с.
4. Russel S. Artificial intelligence. A modern approach, Second Edition / S. Russel, P. Norvig. Williams, 2006. 1410 p.
5. Бондаренко М. Ф. Теория интеллекта : учебник / М. Ф. Бондаренко, Ю. П. Шабанов-Кушнаренко. Харьков : изд-во СМИТ, 2007. 576 с.
6. Журавлев Ю. И. Об алгебраическом подходе к решению задач распознавания или классификации / Ю. И. Журавлев // Проблемы кибернетики. 2005. Вып. 33. С. 5–68.
7. Advanced Methods and Deep Learning in Computer Vision.1st Edition / Editors: E. R. Davies, Matthew Turk. Academic Press. 2021. Page Count: 586. ISBN: 9780128221099.
8. Volodymyr Zhyrnov, Svitlana Solonska PROCESS KNOWLEDGE BOUT OBSERVED OBJECTS IN INTELLECTUAL MONITORING SYSTEMS // Telecommunications and Radio Engineering – 2020. Vol. 79, Issue 18, Pages 1599-1607. |Scopus|0.69|. DOI: 10.1615/TelecomRadEng.v79.i18.20.
9. TRENDS IN ARTIFICIAL INTELLIGENCE (Тенденції в штучному інтелекту) // Editorial team Janis Eitner (V.i.S.d.P.), Katrin Berkler, Henning Köhler, Roman Möhlmann. Fraunhofer-Gesellschaft e.V., 2018. p.p. 1-32/ https://www.fraunhofer.de/content/dam/zv/en/Publications/Trends-in-artificial-intelligence.pdf.
10. Solonskaya S.V., Zhirnov V.V. Signal processing in the intelligence systems of detecting low-observable and low-doppler aerial targets/ Telecommunications and Radio Engineering – 2018. Volume 77, Issue 20, Pages 1827-1835.
11. Jianping Ou, Jun Zhang and Ronghui Zhan. Processing Technology Based on Radar Signal Design and Classification // International Journal of Aerospace Engineering. Vol. 2020, pp. 1-19. Article ID 4673763. https://doi.org/10.1155/2020/4673763.
12. Solonska S., Zhyrnov V. Adaptive semantic analysis of radar data using fuzzy transform (Book Chapter). Springer, 2020, Lecture Notes on Data Engineering and Communications Technologies. Vol 48. P. 157-179.
13. Volodymyr Zhyrnov, Svitlana Solonska INTELLIGENT SYSTEM FOR DETECTION OF LOW-VISIBLE AIR OBJECTS IN SURVEILLANCE RADARS // Telecommunications and Radio Engineering – 2020. Vol. 79, Issue 17, Pages 1513-1519. |Scopus|0.69|. DOI: 10.1615/TelecomRadEng.v79.i17.20.

Поступила в редколлегию 23.09.2021

Сведения об авторах:

Жирнов Владимир Витальевич – канд. техн. наук, Харьковский национальный университет радиоэлектроники, в.н.с. НИЦ интегрированных радиоэлектронных систем и технологий, Украина; e-mail: nauka123@ukr.net

Солонская Светлана Владимировна – канд. техн. наук, доцент кафедры естественных и гуманитарных наук, Харьковский национальный автомобильно-дорожный университет, Украина; e-mail: solonskaya@ukr.net, ORCID: https://orcid.org/0000-0002-8841-7825

Зарицкий Валерий Иванович – канд. техн. наук, Харьковский национальный университет радиоэлектроники, начальник научно-исследовательской части (НИЧ), Украина, e-mail: valerii.zarytskyi@nure.ua, ORCID: https://orcid.org/0000-0001-9047-8152

УДК 621.397.48:004.932.2 **DOI:10.30837/rt.2021.3.206.11**

В.М. КАРТАШОВ, д-р техн. наук, О.И. ХАРЧЕНКО, канд. техн. наук,
В.А. ПОСОШЕНКО, канд. техн. наук, В.И. КОЛЕСНИК, А.Б. ЕГОРОВ, канд. техн. наук,
Л.П. ТИМОШЕНКО, канд. техн. наук, А.И. КАПУСТА

ОБНАРУЖЕНИЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ С ИСПОЛЬЗОВАНИЕМ РАССЕЯНИЯ РАДИОВОЛН НА АКУСТИЧЕСКИХ ВОЗМУЩЕНИЯХ СРЕДЫ, СОЗДАВАЕМЫХ ЛЕТАТЕЛЬНЫМ АППАРАТОМ

Введение

Беспилотные летательные аппараты (БПЛА) получили значительное распространение, поскольку способны выполнять широкий спектр полезных для человечества функций. Они используются для контроля различных объектов и обширных территорий, в том числе морских акваторий, получения разнообразной информации о состоянии атмосферы и степени ее загрязнения, доставки грузов, проведения спасательных операций [1, 2] и т.д.

В то же время БПЛА являются источником потенциальных угроз в ряде областей деятельности человека. Грозным оружием БПЛА являются при использовании их организованными преступными группировками, контрабандистами, определенную опасность они могут представлять также при несанкционированном использовании их отдельными злоумышленниками [1, 2].

В последние годы сформировалась актуальная научно-техническая проблема обнаружения и наблюдения БПЛА с целью предотвращения выполнения ими несанкционированных действий. В соответствии с современными представлениями при обнаружении БПЛА используются следующие методы и средства: радиолокационные (как активные, так и пассивные) [3, 4], оптические, инфракрасные [9], акустические [5] методы, а также комплексные системы, в которых осуществляется совместная обработка информации, получаемой с использованием указанных информационных каналов. В данном направлении работают научные и инженерные коллективы во многих странах мира, однако в целом научно-техническая проблема наблюдения БПЛА, особенно малых БПЛА, остается нерешенной: эффективность обнаружения БПЛА с использованием всех указанных методов остается недостаточной, а потребности практики имеющимися средствами удовлетворяются далеко не в полной мере.

Известно, что существующая научно-техническая проблема не может быть решена на том уровне науки и технологий, на котором она порождена. Кроме того, в ряде работ [1, 2] отмечается, что технологии, используемые при проектировании и изготовлении БПЛА, развиваются намного быстрее, чем объективные средства их обнаружения и контроля.

Следовательно, для эффективного решения существующей научно-технической проблемы необходим новый, качественный скачок в развитии методов и средств обнаружения и наблюдения БПЛА.

Основным методом обнаружения БПЛА, обеспечивающим наибольшую дальность обнаружения и наилучшие поисковые возможности, остается активный радиолокационный метод [2 – 4]. Основная трудность радиолокационного наблюдения БПЛА заключается в том, что искомый объект имеет малую эффективную площадь рассеяния (ЭПР) в силу достаточно малых физических размеров, а также вследствие использования специальных технологий при проектировании и изготовлении БПЛА, направленных на уменьшение рассеяния радиоволн.

Процесс обнаружения летательных аппаратов с малым значением ЭПР может быть основан на использовании побочных эффектов, сопровождающих полет летательного аппарата [2, 4]. Это, в частности, инверсный след в атмосфере, акустические возмущения среды, формирование собственного электромагнитного излучения и др.

Определенный интерес представляет исследование возможности обнаружения БПЛА радиолокационным методом при использовании рассеяния радиоволн на акустических возмущениях среды, создаваемых летательным аппаратом. Впервые на принципиальную возможность рассеяния радиоволн на акустических волнах было указано в фундаментальной теоретической монографии [29]. Первый радиолокатор, использующий рассеяние радиоволн на возмущениях атмосферы, создаваемых излучаемой с поверхности земли звуковой волной, был создан в 1961 г. [35]. С тех пор в данной области получено значительное количество разнообразных научных и экспериментальных результатов.

Статья посвящена анализу известных научных и практических результатов для оценки возможности обнаружения БПЛА по радиосигналам, рассеянным на акустических возмущениях среды, создаваемых БПЛА, и формулированию соответствующих научных и технических задач в данной области знаний.

Акустическое излучение БПЛА

Источниками акустического сигнала БПЛА являются двигатель и несущие винты. Исследованию особенностей акустического сигнала, формируемого и излучаемого БПЛА, посвящен ряд теоретических и экспериментальных работ. Показано, что структура и параметры акустического сигнала БПЛА зависят от вида объекта, его формы, количества двигателей, количества несущих винтов и т.д.

Следует заметить, что исследования акустического поля летательных аппаратов были начаты еще в начале XX века и достаточно интенсивно продолжались в 30-40-е годы прошлого столетия [33, 34]. Исследования выполнялись с целью развития акустического метода обнаружения летательных аппаратов, которые обладали к тому времени достаточно серьезными характеристиками: дальностью, скоростью, высотой полета, полезной нагрузкой.

Однако затем акустический метод обнаружения самолетов был вытеснен радиолокацией, позволившей обеспечить значительно лучшие характеристики по обнаружению летательных аппаратов – дальность, всепогодность и т.д., прежде всего вследствие лучшего распространения радиоволн в атмосфере Земли по сравнению с акустическими волнами.

В то же время необходимо отметить, что уже в указанный период были получены серьезные результаты в теоретическом плане по исследованию формирования акустических волн летательными аппаратами и распространению акустических колебаний в атмосфере, которые не утратили своего значения и в настоящее время. Отметим, что монография [32] представляет собой переиздание книги, впервые увидевшей свет в 1940 г. Определенные успехи в указанный период были достигнуты и в области развития акустической техники – акустических антенн и др. И теперь мы возвращаемся к акустическим методам обнаружения летательных аппаратов уже на новом, более совершенном этапе развития технологий.

Экспериментальные исследования структуры и параметров звукового поля БПЛА в виде квадрокоптера показали, что спектры его акустического излучения содержат ярко выраженные гармонические составляющие, имеющие частоты, кратные частоте вращения винта. Основной тон находится в полосе частот 80 – 240 Гц, а количество гармоник может быть от 10 до 40. Спектр сигнала простирается до частот более 10 – 14 КГц [14].

В режиме полета спектральные линии акустического излучения квадрокоптера размываются вследствие различия режимов работы (частоты вращения) имеющихся четырёх двигателей при компенсации автоматикой БПЛА воздействия дестабилизирующих факторов, возникающих в процессе полёта. Это фактор может являться одним из информационных признаков классификации БПЛА среди других объектов. Расширение спектральных линий проявляется сильнее при увеличении номера гармоники. Все указанные особенности акустического сигнала БПЛА наблюдаются на спектрограмме рис. 1.

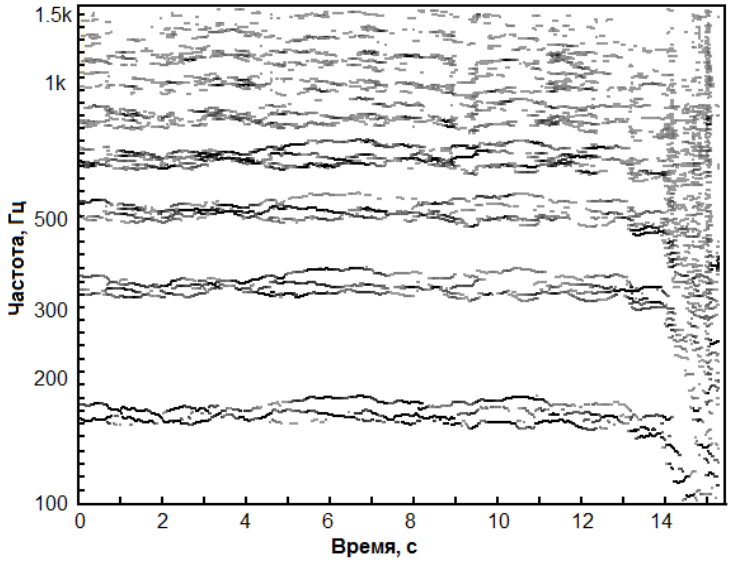


Рис. 1. Спектрограмма акустического сигнала квадрокоптера

Спектральные гармонические составляющие акустического сигнала квадрокоптера шире, чем у моноплана, что объясняется различием режимов работы двигателей в процессе полета или при отработке системой компенсации ветровых возмущений.

По мере увеличения расстояния, прошедшего акустической волной в атмосфере, происходят изменения в спектре акустического излучения (АИ), сопровождающиеся заметным ослаблением высокочастотных составляющих. Изменения формы спектров АИ БПЛА в реальных условиях наблюдения обусловлены дисперсионными свойствами среды, а также изменчивостью характеристик пространственной направленности излучения в полосе частот.

Большое значение для практики имеют диаграммы излучения БПЛА, характеризующие распределение излучаемой акустической энергии по направлениям. В ряде работ рассматривалась пространственная направленность звукового излучения БПЛА, в частности в [10] сделан вывод о том, что в первом приближении БПЛА может считаться изотропным источником излучения.

В то же время эксперименты показывают существенную направленность излучения как отдельных элементов конструкции аппарата – винтомоторной группы, электродвигателей квадрокоптера, так и всей конструкции в целом. Показано, что пространственные распределения как отдельных спектральных (гармонических) составляющих, так и полной энергии (во всем диапазоне частот) являются существенно анизотропными.

Нормализованные характеристики пространственной направленности акустического излучения квадрокоптера DJI Phantom 3 в вертикальной плоскости для первых четырёх гармоник лопастной частоты воздушного винта представлены на рис. 2. Анализ представленных результатов показывает, что с повышением номера гармоники происходит усложнение формы характеристики направленности: она становится более изрезанной, увеличивается глубина провалов, уменьшается ширина лепестков и происходит изменение направления основного излучения.

Как видно из рис. 2, различным ракурсам наблюдения БПЛА соответствуют различные уровни спектральных гармонических составляющих излучения, определяемых характеристиками направленности. Из этого следует, что интенсивность акустического излучения в зависимости от угла наблюдения должна описываться некоторым законом распределения вероятностей, а дальность обнаружения БПЛА с использованием акустического метода является величиной статистической, зависящей от ракурса наблюдения.

Звуковые волны, порождаемые БПЛА, являются также источником информации в акустическом методе обнаружения и наблюдения БПЛА, который в настоящее время интенсивно развивается.

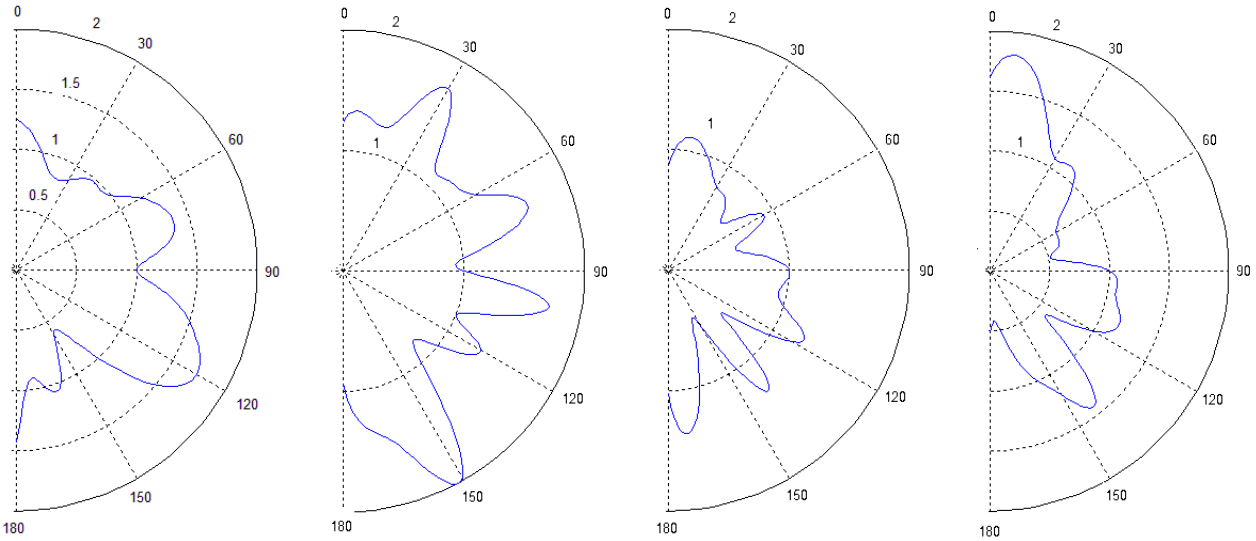


Рис. 2. Нормализованные характеристики направленности акустического излучения квадрокоптера DJI Phantom 3 в вертикальной плоскости на гармониках лопастной частоты винта: 1 – 1-я гармоника, 2 – 2-я гармоника, 3 – 3-я гармоника, 4 – 4-я гармоника

Теоретические и экспериментальные результаты рассеяния радиоволн на звуковых волнах

При радиолокации, распространяющейся в атмосфере звуковой волны, получение отраженного сигнала становится возможным в силу частичного отражения радиоволны от акустических колебаний, которые, распространяясь в атмосфере, модулируют плотность воздуха и, следовательно, создают неоднородности диэлектрической проницаемости.

В борновском приближении – приближении однократного рассеяния, выражение для рассеянного радиосигнала имеет вид

$$\vec{E}_1(\vec{r}) = \frac{k_e^2}{4\pi}\int_V \frac{\exp\{jk_e|\vec{r}-\vec{r}'|\}}{|\vec{r}-\vec{r}'|}\varepsilon_{\approx}(\vec{r}')\left[\vec{n}\left[\vec{E}_0(\vec{r}')\vec{n}\right]\right]d^3\vec{r}', \quad (1)$$

где $\vec{E}_1(\vec{r})$ – рассеянное поле в точке $\vec{r}$; $\varepsilon_{\approx}(\vec{r}')$ – переменная составляющая поля диэлектрической проницаемости; k_e – волновое число падающей электромагнитной волны; $\vec{E}_0(\vec{r}')$ – падающее на рассеивающий объем V электромагнитное излучение; $\vec{n}(\vec{r},\vec{r}')$ – единичный вектор, направленный из переменной точки интегрирования $\vec{r}'$ (точки рассеяния) в точку наблюдения.

Начало координат здесь совмещено с центром рассеивающего объема. Двойное векторное произведение, стоящее в подынтегральном выражении (1), описывает векторное сложение в точке приема волн, приходящих под различными углами.

Поле диэлектрической проницаемости $\varepsilon(\vec{r}',t)$ в задаче рассеяния радиоволн на звуке представляется в виде

$$\varepsilon(\vec{r}',t) = \varepsilon_1(\vec{r}',t) + \varepsilon_s(\vec{r}',t), \quad (2)$$

где $\varepsilon_1(\vec{r}',t)$ – собственная диэлектрическая проницаемость среды; $\varepsilon_S(\vec{r}',t)$ – составляющая диэлектрической проницаемости, порожденная звуком.

В реальной атмосфере обычно всегда выполняется неравенство $\langle|\varepsilon_S|\rangle \ll 1$. Это позволяет получать решение задачи в приближении однократного рассеяния. Регулярный компонент диэлектрической проницаемости $\langle\varepsilon_1\rangle$ с достаточной степенью точности можно считать равным единице, а турбулентные флуктуации много меньше единицы и на несколько порядков меньше величины $|\varepsilon_S|$ [35].

Влиянием турбулентных флуктуаций диэлектрической проницаемости на распространение радиоволн можно пренебречь, поэтому атмосферная турбулентность входит в окончательные формулы только через флуктуации величины ε_S. С учетом изложенного, не конкретизируя вид функции $\varepsilon_S(\vec{r}',t)$, выражение для диэлектрической проницаемости среды запишем в виде

$$\varepsilon(\vec{r}',t) \approx 1 + \varepsilon_S(\vec{r}',t). \tag{3}$$

Достаточный для обработки и регистрации уровень отраженного радиосигнала может быть получен только в случае выполнения некоторых условий. Во-первых, необходимо отражение от «цуга» акустических волн длиной $N_S\lambda_S$, при $N_S >> 1$, во-вторых, требуется выполнение условия Брэгга

$$\lambda_e = 2\lambda_S \sin\theta, \tag{4}$$

где λ_e – длина электромагнитной волны; N_s – количество периодов (длин волн) акустической неоднородности, участвующих в формировании рассеянного радиосигнала; λ_S – длина волны акустических колебаний; θ – угол между фронтом акустической волны и направлением распространения радиоволны.

Выполнение условия Брэгга приводит к тому, что радиоволны, отраженные от различных участков акустического цуга, складываются синфазно и амплитуда суммарного отраженного радиосигнала увеличивается.

Впервые на принципиальную возможность рассеяния радиоволн на акустических волнах было указано в фундаментальной теоретической монографии [29]. Теоретические и экспериментальные основы развития атмосферной акустики были заложены трудами ученых Обухова А.М. [27], Каллистратовой М.А. [28], Татарского В.И. [29, 30].

Длина радиоволны первой экспериментальной радиоакустической системы зондирования атмосферы ЕМАС [35], созданной в 1961 г., составляла $\lambda_e = 3$ см, длина акустической волны – $\lambda_S = 1{,}5$ см, а максимальная дальность действия – 30 м. Полученная дальность разочаровала исследователей и следующая разработка появилась только в 1972 г., когда была выяснена причина малой дальности зондирования – значительное затухание высокочастотных акустических волн в атмосфере. Установка называлась RASS и имела следующие параметры [54, 58]: $\lambda_e = 8{,}15$ м; $\lambda_S = 4{,}075$ м. С помощью этой установки удалось получить отраженный сигнал с высоты 1,5 км, но минимальная высота зондирования составляла 600 м, а пространственная разрешающая способность – 200 м.

В большинстве последующих установок радиоакустического зондирования атмосферы [33, 35] применялись импульсное акустическое излучение и непрерывное монохроматическое радиоизлучение, использовались отдельные, разнесенные на некоторое расстояние приемная и передающая радиоантенны (рис. 3). Передающая акустическая антенна, как правило, располагается посредине между радиоантеннами. Такая схема расположения антенн в сово-

купности с указанной комбинацией зондирующих радио- и акустического сигналов (схема построения системы) получила название «основной».

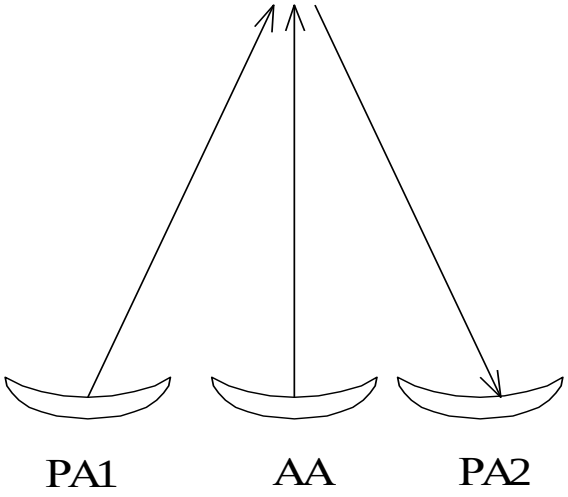


Рис. 3. Схема расположения антенн станции радиоакустического зондирования атмосферы: РА1 – передающая радиоантенна; АА – акустическая антенна; РА2 – приемная радиоантенна

К середине 80-х годов, когда сформировались принцип построения и структура доплеровской радиоакустической системы (РАС), в мире насчитывалось около 10 работающих установок РАЗ, большинство из которых были построены по основной схеме [35].

Все имевшиеся к тому времени системы (кроме ЕМАС и РАЗ-10) были стационарными. В качестве передающих и приемных радиоантенн чаще всего использовались параболические зеркальные антенны, в качестве акустических излучателей – решетки динамиков.

Отметим, что в бывшем Советском Союзе, а ныне в Украине исследования метода и систем радиоакустического зондирования (РАЗ) наиболее интенсивно проводились (и проводятся) именно в Харьковском институте радиоэлектроники (теперь ХНУРЭ). За период с 1965 по 2003 г. здесь созданы пять экспериментальных установок радиоакустического зондирования, в том числе первая в Европе, и выполнен большой объем атмосферных и аппаратурных исследований [33, 37, 38].

Сегодня станции радиоакустического зондирования атмосферы разрабатываются в ряде стран отдельными научными коллективами для выполнения экспериментов по исследованию атмосферы, а также производятся некоторыми научно-производственными фирмами небольшими сериями [37, 38].

Радиоакустический метод обнаружения БПЛА

Радиоакустический метод локации БПЛА заключается в излучении зондирующего радиосигнала в исследуемую область пространства, приеме рассеянных на звуке радиосигналов, их обработке, и обнаружении принимаемых сигналов, свидетельствующих о наличии в сканируемой области пространства беспилотного летательного аппарата. Процесс зондирования пространства, рассеяния радиоволн, излучаемых радиолокационной станцией, на возмущениях среды, создаваемых акустическими волнами летящего БПЛА, представлен на рис. 4.

Излученный БПЛА звуковой сигнал сохраняет значительную интенсивность на расстоянии в несколько сотен метров, поэтому обнаружение некоторой возмущенной этим сигналом области позволит фактически обнаружить сам летательный аппарат, поскольку данное расстояние при достаточно больших удалениях БПЛА не является значительным.

Как показано выше, БПЛА излучает акустические волны в диапазоне частот от сотен герц до 10 – 15 кГц. Диапазон радиоволн, в котором может быть получен рассеянный радиосигнал, соответствующий указанному диапазону акустических волн, простирается от

λ_e=6,8 м (соответствует частоте акустического сигнала f_s=100 Гц (λ_s=3,4 м) до λ_e=5,4 см (что соответствует частоте акустического сигнала f_s=15 кГц (λ_s=2,7 см).

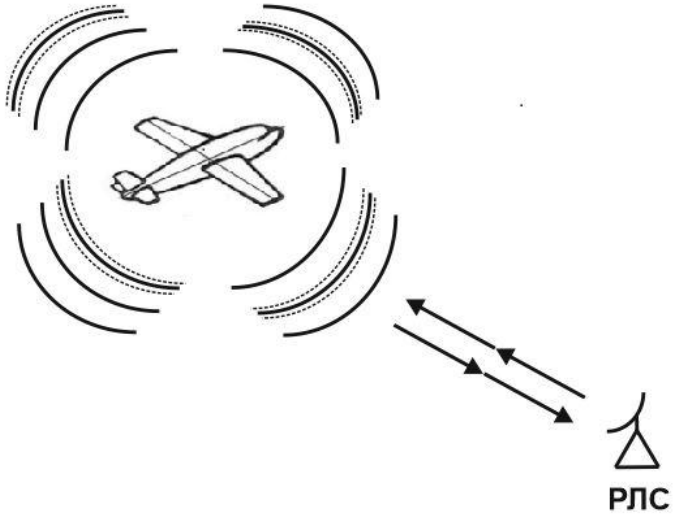


Рис. 4. Рассеяние радиоволн, излучаемых РЛС, на возмущениях среды, создаваемых акустическими волнами БПЛА

Выражение (1), описывающее рассеянный на звуке радиосигнал, является достаточно сложным, что затрудняет его использование на практике [37, 38]. При решении конкретных прикладных задач целесообразно иметь более простую, адекватную математическую модель, которая позволяла бы определять основные свойства и характеристики радиосигнала, рассеянного на звуковых волнах, порождаемых БПЛА.

В соответствии с изложенным при проведении последующих научных исследований в данном направлении необходимо разработать конструктивные математические модели, описывающие процесс рассеяния, и исследовать свойства радиосигналов, рассеянных на акустических волнах БПЛА: их спектральный состав сигналов, структурные особенности, энергетические свойства. Необходимо также разработать методы обработки радиосигналов, рассеянных на звуковых волнах БПЛА, с целью обнаружения принимаемых сигналов.

Выводы

1. Принципиальная возможность обнаружения беспилотных летательных аппаратов по радиосигналам, рассеянным на акустических возмущениях среды, создаваемых летательными аппаратами, вытекает из известных теоретических и экспериментальных результатов. С теоретических позиций вопрос рассеяния радиоволн на акустических волнах обоснован и достаточно детально проанализирован в трудах Татарского В.И., Каллистратовой М.А. и др. [28 – 30; 35].

На практике явление рассеяния радиоволн на звуке используется при построении станций радиоакустического зондирования атмосферы, позволяющих определять ряд важных характеристик атмосферы – температуру, скорость ветра, определяющих ее состояние.

2. Вопрос формирования и излучения акустических волн беспилотными летательными аппаратами, прежде всего их двигателями и несущими винтами, также достаточно обстоятельно исследован с теоретических и экспериментальных позиций. Исследованы их структура, интенсивность, спектральный состав, пространственная направленность. Акустические волны, излучаемые БПЛА, в соответствии со своими характеристиками могут быть источником рассеянных на них электромагнитных волн.

3. При проведении последующих исследований в данном направлении необходимо исследовать свойства радиосигналов, рассеянных на акустических волнах БПЛА: их структурные, частотные, энергетические, пространственные особенности, а также разработать методы

обработки радиосигналов, рассеянных на звуковых волнах БПЛА, с целью обнаружения принимаемых сигналов.

Список литературы:

1. Кошкин Р.П. Беспилотные авиационные системы. Москва : Стратегические приоритеты, 2016. 676 с.
2. Макаренко С. И., Тимошенко А. В., Васильченко А. С. Анализ средств и способов противодействия беспилотным летательным аппаратам. Ч. 1. Беспилотный летательный аппарат как объект обнаружения и поражения // Системы управления, связи и безопасности. 2020. № 1. С. 109-146. DOI: 10.24411/2410-9916-2020-10105.
3. Вишневський С. Д., Бейліс Л. В., Климченко В. Й. Потенційні можливості РЛС РТВ з виявлення оперативно-тактичних та тактичних безпілотних літальних апаратів // Розвиток, бойове застосування та озброєння радіотехнічних військ. 2017. С. 92–98. DOI: 10.30748/nitps.2017.27.18.
4. Карташов В.М., Ситнік О.В. Радіотехнічні системи : навч. посібник. Харків : Сміт, 2009. 448 с.
5. Карташов В.М., Олейников В.Н., Шейко С.А., Бабкин С.И., Корытцев И.В., Зубков О.В. Особенности обнаружения и распознавания малых беспилотных летательных аппаратов // Радиотехника. 2018. Вып. 195. С. 235-243.
6. Kartashov V.M., Oleynikov V.N, Sheyko S.A., Koryttsev I.V., Babkin S.I., Zubkov O.V. Peculiarities of small unmanned aerial vehicles detection and recognition // Telecommunications and Radio Engineering. Vol. 78, Issue 9. P. 771-781.
7. StrelkovaT., KartashovV., Lytyuga A.,Strelkov A. Theoretical Methods of Images Processing in Optoelectronic Systems. Chapter 16. // Biometrics: Concepts, Methodologies, Tools, and Applications; Oleg Sergiyenko and Julio C. Rodriguez-Quiñonez. (341p.), IGI Global, 2017; pp. 361-381.
8. Developing and Applying Optoelectronics in Machine Vision / O. Sergiyenko, J.C. Rodriguez-Quiñonez. IGI Global, 2016. 341p.
9. Koryttsev I., Sheiko S., Kartashov V., Zubkov O., Oleynikov V., Anohin M., Selieznov I. Practical Aspects of Range Determination and Tracking of Small Drones by Their Video Observation // 2020 International Scientific-Practical Conference. Problems of Infocommunications. Science and Technology. Kharkiv, Ukraine. October 6-9, 2020. 5 p.
10. Massey K., Gaeta R. Noise Measurements of Tactical UAVs. // Georgia Inst. of Technology / GTRI / ATAS, Atlanta. 16th AIAA / CEAS Aeroacoustics Conference. American Institute of Aeronautics and Astronautics, 2010, pp. 1–16.
11. Marino L.,Experimental analysis of UAV-propellers noise // 16th AIAA/CEAS Aeroacoustics Conference. University «La Sapienza», Rome, Italy, American Institute of Aeronautics and Astronautics, 2010; pp. 1–14.
12. Sinibaldi G., Marino L. Experimental analysis on the noise of the propellers for small UAV. // Applied Acoustics, 74 (2013); pp. 79–88**.**
13. N. Intaratep W. Alexander N., Devenport W. J., Grace S. M., Dropkin A. Experimental Study of Quadcopter Acoustics and Performance at Static Thrust Conditions // Aeroacoustics Conferences 30 May – 1 June, 2016, Lyon, France, 22nd AIAA/CEAS Aeroacoustics Conference; pp. 1–6.
14. Карташов В.М., Олейников В.Н., Шейко С.А., Бабкин С.И., Корытцев И.В., Зубков О.В., Анохин М.А. Информационные характеристики звукового излучения малых беспилотных летательных аппаратов // Радиотехника. 2017. Вып. 191. С. 181-187.
15. Kartashov V.M., Tikhonov V.A., Voronin V.V. and Tymoshenko L.P. Complex model of random signal in problems of acoustic sounding of atmosphere // Telecommunications and Radio Engineering. 2016. V. 75, Iss. 20. pp.1885–1892. DOI: 10.1615/TelecomRadEng.v75.i20.80.
16. Mezei J., Molnár A. Drone sound detection by correlation // Proceedings of the 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI); Timisoara, Romania. 12–14 May 2016; pp. 509–518. DOI: 10.1109/SACI.2016.7507430.
17. Bernardini A., Mangiatordi F., Pallotti E., Capodiferro L. Drone detection by acoustic signature identification. Electron. Imaging. 2017;2017:60–64. doi: 10.2352/ISSN.2470-1173.2017.10.IMAWM-168. DOI: https://doi.org/10.2352/ISSN.2470-1173.2017.10.IMAWM-168.
18. Liu H., Wei Z., Chen Y., Pan J., Lin L., Ren Y. Drone detection based on an audio-assisted camera array // Proceedings of the 2017 IEEE Third International Conference on Multimedia Big Data (BigMM); Laguna Hills, CA, USA. 19–21 April 2017; pp. 402–406. DOI: 10.1109/BigMM.2017.57.
19. Park S., Shin S., Kim Y., Matson E.T., Lee K., Kolodzy P.J., Slater J.C., Scherreik M., Sam M., Gallagher J.C., et al. Combination of radar and audio sensors for identification of rotor-type unmanned aerial vehicles (uavs) // Proceedings of the 2015 IEEE SENSORS; Busan, Korea. 1–4 November 2015; pp. 1–4. DOI: 10.1109/ICSENS.2015.7370533.
20. Vasilchenko A., Kartashov V.M. Analysis of influence exerted by longitudinal Doppler effect upon output signal of sodar antenna array // Telecommunications and Radio Engineering, Volume 66, Issue 9; pp. 841–847. DOI: 10.1615/TelecomRadEng.v66.i9.50.
21. Zelnio A.M. Detection of small aircraft using an acoustic array // Electrical Engineering, Wright State University, 2007. 55 p.
22. Kozeruk S.A., Korzhyk A.V. Identification of small aircraft by acoustic radiation // Visnyk NTUU KPI. Series Radiotekhnika Radiobuduvannia. 2019. Iss. 76. pp. 15–20. DOI: https://doi.org/10.20535/RADAP.2018.80.30-46.

23. Sadasivan S., Gurubasavaraj M., Sekar S.R. Acoustis siqnature of an unmanned air vehicle – exploitation for aircraft localisation and parameter estimation // Eronautical DEF SCI J. 2001. Vol. 51, №3. pp. 279–283.
24. Тихонов В.А., Карташов В.М., Олейников В.М., Леонидов В.И., Тимошенко Л.П., Селезнев И.С., Рыбников Н.В. Обнаружение-распознавание беспилотных летательных аппаратов с использованием составной модели авторегрессии их акустического излучения // Вісник НТУУ «КПІ». Радіотехніка. Радіоапаратобудування. 2020. Вип. №81, С. 38–46. DOI: https://doi.org/10.20535/RADAP.2020.81.38-46.
25. Oleynikov V., Zubkov O., Kartashov V., Koryttsev I., Sheiko S., Babkin S. Experimental estimation of direction finding to unmanned air vehicles algorithms efficiency by their acoustic emission // 2019 International Scientific-Practical Conference «Problems of Infocommunications – Science and Technology, PIC S and T 2019 – Proceeding», 2019; pp.175–178. DOI: 10.1109/PICST47496.2019.9061337.
26. Kartashov V.M., Oleynikov V.N, Zubkov O.V., Korytsev I.V., Babkin S. I., Sheiko S.A., Kolendovskaya M.M. Spatial-temporal Processing of acoustic Signals of Unmanned Aerial Vehicles // Telecommunications and Radio Engineering, V. 79, №9. 2020, pp.769–780. DOI: 10.1615/TelecomRadEng.v79.i9.40.
27. Обухов А.М. О рассеянии звука в турбулентном потоке // Доклады АН СССР. 1941. Т.30, №7. С.611 – 614.
28. Каллистратова М.А. Экспериментальное исследование рассеяния звуковых волн в атмосфере // Атмосферная турбулентность. Москва : Изд. АН СССР, 1961. С.203 – 258.
29. Татарский В.И. Теория флуктуационных явлений при распространении волн в турбулентной атмосфере. Москва : Изд. АН СССР, 1959. 331 с.
30. Татарский В.И Распространение волн в турбулентной атмосфере. Москва : Наука, 1967. 548 с.
31. Marschall J.M., Peterson A.M., Barnes A.A. Combined radar acoustic sounding system // Appl. Opt. 1972. Vol.2, №1. P. 108 – 112.
32. Блохинцев Д.И. Акустика неоднородной движущейся среды. Москва : Наука, 1981. 207 с.
33. Дистанционные методы и средства исследования процессов в атмосфере Земли ; под ред. Б.Л. Кащеева, Е.Г. Прошкина, М.Ф. Лагутина. Харьков : Бизнес Информ, 2002. 426 с.
34. Красненко Н.П. Акустическое зондирование атмосферы. Новосибирск: Наука, 1986. 167 с.
35. Калистратова М.А., Кон А.И. Радиоакустическое зондирование атмосферы. Москва : Наука, 1985. 200 с.
36. Карташов В.М., Куля Д.Н., Кушнир М.В., Толстых Е.Г. Выбор модели изменения скорости звука для оптимального линейного фильтра систем радиоакустического зондирования атмосферы // Радиотехника. 2013. №173. С. 63–78.
37. Карташов В.М. и др. Обработка сигналов в радиоэлектронных системах дистанционного мониторинга атмосферы. Харьков : ХНУРЭ, 2014. 312 с.
38. Карташов В.М. Модели и методы обработки сигналов систем радиоакустического и акустического зондирования атмосферы. Харьков : ХНУРЭ, 2011. 234 с.

Поступила в редколлегию 21.09.2021

Сведения об авторах:

Карташов Владимир Михайлович – д-р техн. наук, профессор, Харьковский национальный университет радиоэлектроники, заведующий кафедрой медиаинженерии и информационных радиоэлектронных систем; Украина, e-mail: volodymyr.kartashov@nure.ua; ORCID: https://orcid.org/0000-0001-8335-5373

Харченко Оксана Игоревна – канд. техн. наук, Харьковский национальный университет радиоэлектроники, доцент кафедры медиаинженерии и информационных радиоэлектронных систем Украина; e-mail: oksana.kharchenko@nure.ua; ORCID: https://orcid.org/0000-0002-1553-0966

Посошенко Виталий Александрович – канд. техн. наук, Харьковский национальный университет радиоэлектроники, доцент кафедры медиаинженерии и информационных радиоэлектронных систем, Украина; e-mail: vitalii.pososhenko@nure.ua; ORCID: https://orcid.org/0000-0003-0867-9161

Колесник Виктория Ивановна – Харьковский национальный университет радиоэлектроники, ассистент кафедры медиаинженерии и информационных радиоэлектронных систем, Украина; e-mail: viktoriia.kolisnyk@nure.ua; ORCID: https://orcid.org/0000-0002-2382-9124

Егоров Андрей Борисович – канд. техн. наук, Харьковский национальный университет радиоэлектроники, доцент кафедры информационно-измерительных технологий, Украина; e-mail: andriy.yegorov@nure.ua; ORCID: https://orcid.org/0000-0002-8528-6428

Тимошенко Леонид Петрович – канд. техн. наук, Харьковский национальный университет радиоэлектроники, профессор кафедры медиаинженерии и информационных радиоэлектронных систем, Україна; e-mail: leonid.tymoshenko@nure.ua; ORCID: https://orcid.org/0000-0003-1924-5908

Капуста Анастасия Игоревна – Харьковский национальный университет радиоэлектроники, аспирант кафедры медиаинженерии и информационных радиоэлектронных систем, Украина; e-mail: anastasiia.kapusta@nure.ua; ORCID: https://orcid.org/0000-0003-2206-1552

ІНФОРМАЦІЙНІ МЕТОДИ РАДІОТЕХНІКИ

УДК 006.91:004.9 **DOI:10.30837/rt.2021.3.206.12**

І. МОЩЕНКО, канд. техн. наук, О.НІКІТЕНКО, канд. техн. наук,
Ю.КОЗЛОВ, канд. техн. наук, Ю.ЖАРКО, канд. техн. наук

ОСОБЛИВОСТІ СТАТИСТИЧНОЇ ОБРОБКИ ДАНИХ ЗАСОБАМИ СИСТЕМ КОМП'ЮТЕРНОЇ МАТЕМАТИКИ

Вступ

Під час досліджень та оцінювання параметрів фізичних коливальних систем виникають певні питання, які, на перший погляд, не мають явних точок контакту одна з одною:

1. Моделювання поведінки таких систем дозволяє теоретично визначити взаємний вплив одних параметрів системи на інші;
2. Механізми визначення фізичних явищ та параметрів системних конструктивних вузлів, які мають вплив на характеристики цих систем;
3. Визначення параметрів, які впливають на поведінку системи загалом або окремих її вузлів;
4. Визначення частотних характеристик систем зі схрещеними полями;
5. Створення системи оцінювання вибраних параметрів;
6. Вибір методів дослідження частотних параметрів;
7. Вимірювання параметрів частоти (збирання даних);
8. Вибір методів обробки зібраних даних;
9. Обробка зібраних статистичних даних.

З іншого боку, основними розділами теоретичної метрології традиційно є: основа забезпечення єдності вимірювань (включаючи стандартизацію одиниць фізичних величин, відтворення та методи передачі їх розміру); теорія помилок (невизначеностей) та методи оцінювання результатів вимірювань; методи та засоби вимірювальної техніки.

Зараз методи статистичної обробки використовують не тільки у виробництві, але також у плануванні, розробці системи маркетингу, матеріально-технічного постачання тощо. Особливу увагу приділяють якості планування, дизайну, виробництва продукції, але про якість обробки результатів вимірювань майже не згадують. Таким чином, передбачається, що точність обробки результатів є абсолютною.

Будь-яке вимірювання частоти або періоду (часу) закінчується обробкою отриманих результатів. Сьогодні обробку експериментальних даних часто здійснюють за допомогою комп'ютера. Вважається, що комп'ютерні розрахунки мають абсолютну точність, але це не відповідає дійсності. З іншого боку, статистичні розрахунки без застосування комп'ютера є працемісткими і вимагають використання багатьох таблиць стандартних розподілів квартилів. Спеціальні статистичні пакети вимагають від фахівців високого рівня знань в галузі математичної статистики.

Таким чином, мета цієї роботи – порівняння результатів статистичних обчислень, отриманих під час дослідження коливальних станів електровакуумних приладів зі схрещеними полями за допомогою різних математичних пакетів з результатами, що розраховані за теоретичними формулами.

Матеріали і методи

Електровакуумні прилади зі схрещеними полями мають високий рівень шуму. Нелінійна взаємодія електронного пучка та електромагнітних хвиль призводить до збудження хаотичних або комбінованих коливань. Було проведено дослідження спектру низько- і високочастотних режимів для доведення хаотичної поведінки коливань, що збуджуються в електроваку-

умних приладах зі схрещеними полями [1 – 3]. Експериментальні дослідження коливальних станів електровакуумних приладів зі схрещеними полями вимагають проведення великої кількості багаторазових вимірювань частоти. Тому під час комп'ютерної обробки результатів експериментальних досліджень постало питання відповідності статистичних характеристик, отриманих за допомогою математичних пакетів, характеристикам, розрахованим за теоретичними формулами.

За необхідності отримання числових результатів вимірювання аналіз помилок повинен бути невід'ємною частиною будь-якого серйозного розрахунку. Вхідна інформація часто не достатньо точна, оскільки дані, що використовують, найчастіше є експериментальними даними або базуються на наближеній оцінці. Крім того, обчислювальні процеси самі можуть додавати до результатів деякі помилки. Коли вирішують конкретну проблему, ми маємо справу з трьома основними типами помилок: помилки, що містяться у вхідній інформації; помилки, обумовлені обмеженням нескінченного математичного процесу кінцевою кількістю операцій (помилки обмеження); помилки, що виникають внаслідок необхідності подавати число у формі кінцевої послідовності цифр (помилки округлення).

Помилки в початковій інформації виникають в результаті неточності вимірювань або через неможливість подати необхідне значення кінцевим дробом. Помилки, що містяться у вхідній інформації, визначають точність результатів розрахунку, незалежно від методу, за допомогою якого ці розрахунки здійснюють. Два інших типи помилок – помилки обмеження та помилки округлення – визначають числовими методами, що використовують для вирішення проблеми. Навіть якщо ми припустили, що вхідна інформація не містить жодних помилок, а всі обчислювальні процеси є скінченними і не призводять до помилок обмеження, то у цьому випадку існує третій тип помилки – помилки округлення. Під час чисельного аналізу однією з найважливіших проблем є питання про те, як помилка, що виникає в певному місці під час обчислення, розподіляється в майбутньому, незалежно від того, стає її вплив більшим чи меншим під час виконання наступних операцій.

Проаналізуємо процес накопичення похибок при обчисленні найбільш часто обчислюваного параметра – дисперсії

$$D = \frac{1}{n-1}\sum_{i=1}^{n}\left(x_i - \bar{x}\right)^2 . \qquad (1)$$

Наведена формула складається з таких операцій: віднімання $x_i - \bar{x}$; множення (піднесення до ступеня) $\left(x_i - \bar{x}\right)^2$; додавання $\sum_{i=1}^{n}\left(x_i - \bar{x}\right)^2$; кінцеве ділення. Добре відомо, якщо потрібно додавати або віднімати послідовності довгих чисел (підсумовування) з метою зменшення похибки обчислення, спочатку необхідно знайти суму найменших чисел і потім переходити до більших. Це вимагає додаткових операцій під час написання коду програми. Ці операції призначенні для того, щоб попередньо відсортувати значення перед отриманням суми. У таких випадках відносна похибка підрахунку суми не перевищуватиме $5\cdot 10^{-t}$, де t – кількість значущих цифр. Якщо це можливо, слід уникати двох майже однакових чисел (обчислення віднімання). Формули, що містять таке віднімання, дуже часто можуть бути перетворені таким чином, щоб уникнути такої операції. Ця вимога, як і попередня, вимагає додаткових операцій при написанні програмного коду. У будь-якому випадку, щоб зменшити накопичення помилок під час обчислень, бажано зменшити кількість необхідних арифметичних операцій. Таким чином, під час обробки експериментальних результатів за допомогою комп'ютерних програм необхідно враховувати вищезазначені аспекти, якщо створюють оригінальну обчислювальну програму. Якщо використовують спеціальне програмне забезпечення, варто ознайомитися з алгоритмами обчислення необхідних характеристик, щоб зменшити накопичення похибок розрахунку [4].

Авторами розглянуто обробку даних за допомогою найпопулярніших пакетів: електронних таблиць Excel та систем комп'ютерної математики (СКМ) Maple, MatLab та MathCad.

Дві останні системи базуються на ядрі Maple. Більшість існуючих математичних пакетів дозволяють користувачам працювати з випадковими величинами, включаючи популярні пакети. У цих пакетах розділ статистики має власну розроблену систему команд для обслуговування прикладних завдань. Статистичні команди призначені для тих категорій користувачів, яким потрібне середовище, що дозволяє легко переходити від однієї математичної спеціалізації до іншої.

Порівняння результатів

Особливості обробки статистичних даних, отриманих під час дослідження коливальних станів електровакуумних приладів зі схрещеними полями, досліджено шляхом обробки вибірки з 80 значень частоти генерації магнетрону (табл. 1) за допомогою популярних математичних пакетів Excel, Maple, Matlab та MathCad та порівняння отриманих результатів з розрахунками за теоретичними формулами.

Таблиця 1

Sample (частота GHz)

13,39	13,46	13,26	13,59	13,54	13,42
13,42	13,53	13,33	13,36	13,37	13,45
13,38	13,55	13,43	13,44	13,31	13,32
13,53	13,29	13,50	13,34	13,37	13,44
13,51	13,24	13,44	13,33	13,33	13,58
13,30	13,34	13,53	13,25	13,54	13,50
13,40	13,54	13,48	13,28	13,32	13,36
13,28	13,55	13,48	13,49	13,26	13,40
13,53	13,43	13,34	13,33	13,26	13,36
13,57	13,50	13,52	13,58	13,30	13,62
13,43	13,37	13,39	13,66	13,50	13,40
13,42	13,40	13,23	13,38	13,31	13,47
13,57	13,28	13,45	13,34	13,64	13,56
13,40	13,31				

Результати статистичної обробки наведено в табл. 2.

Таблиця 2

Результати обробки

Математичний пакет	Математичне сподівання, ГГц	Дисперсія, $ГГц^2$	Стандартне відхилення, ГГц	Коефіцієнт асиметрії	Коефіцієнт ексцесу
Теоретичний	13,42	0,01136203	0,10659280	0,194202	2,0440198
Excel	13,42	0,0113620	0,1065928	0,201703	0,884131
Maple	13,42	0,011362	0,106593	0,196660	2,069893
Matlab	13,42	0,0114	0,1066	0,1979	2,0961
MathCad	13,42	0,011	0,107	0,202	0,884

Результати розрахунків за допомогою усіх пакетів дають однакові результати для математичного сподівання, дисперсії та стандартного відхилення. Щодо коефіцієнтів асиметрії та ексцесу, то більшість результатів не збігаються.

Результати побудови гістограми для зразкових значень наведено на рис. 1 – 5.

На рисунках видно, що гістограми, які побудовані вручну та за допомогою СКМ Maple, Matlab та MathCad, однакові. А гістограма, яка побудована за допомогою пакету Excel, має багато відмінностей.

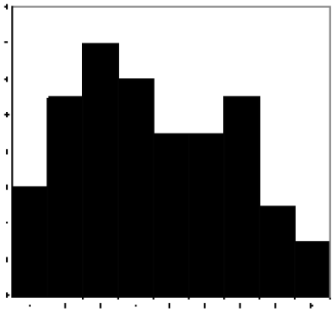


Рис. 1. Теоретична гістограма

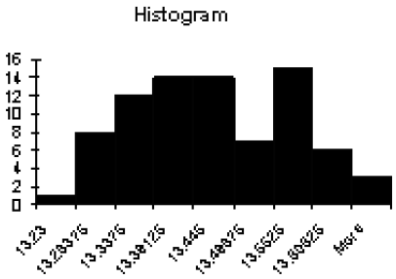


Рис. 2. Гістограма Excel

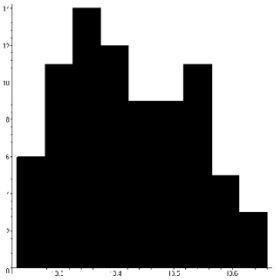


Рис. 3. Гістограма Maple

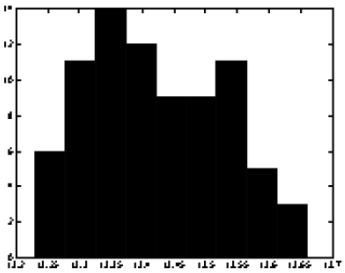


Рис. 4. Гістограма Matlab

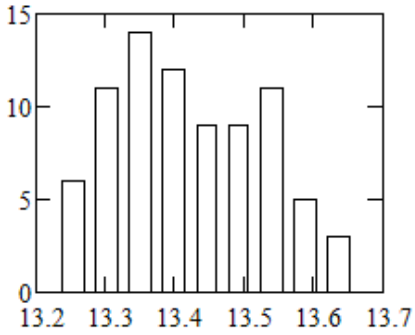


Рис. 5. Гістограма MathCad

.

Обговорення

Аналіз результатів розрахунків показав, що відмінність отриманих значень коефіцієнтів асиметрії та ексцесу обумовлений різними визначеннями цих показників вищезазначеними пакетами.

А. Коефіцієнт асиметрії

В теорії коефіцієнт асиметрії, який характеризує асиметричність функції розподілу, визначають як

$$\frac{m_3}{\sigma^3}; \qquad (2)$$

де m_3 _ центральний момент третього порядку, що визначають як $m_3 = \frac{1}{n}\sum_{i=1}^{n}\left(x_i - \bar{x}\right)^3$, де n – розмір вибірки; x_i – виміряне значення; $\bar{x}$ – математичне сподівання (середнє арифметичне) $\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$; σ – стандартне відхилення.

В пакетах Excel і MathCad коефіцієнт асиметрії розраховуються таким чином [5, 8]:

$$\frac{n}{(n-1)(n-2)}\frac{m_3}{\sigma^3}. \tag{3}$$

В СКМ Maple коефіцієнт асиметрії розраховують таким чином [6]:

$$\frac{n}{(n-1)}\frac{m_3}{\sigma^3}. \tag{4}$$

В СКМ Matlab коефіцієнт асиметрії розраховують за теоретичною формулою [7].

Б. Коефіцієнт ексцесу

В теорії коефіцієнт ексцесу, який характеризує площинність функції розподілу, розраховують як

$$\frac{m_4}{\sigma^4}-3; \tag{5}$$

де m_4 – центральний момент четвертого порядку, який визначають за формулою $m_4=\frac{1}{n}\sum_{i=1}^{n}\left(x_i-\bar{x}\right)^4$; 3 – враховує той факт, що коефіцієнт ексцесу нормального закону розподілу дорівнює 3.

В пакетах Excel і MathCad коефіцієнт ексцесу розраховують за формулою [5, 8]

$$\frac{n^2(n+1)}{(n-1)(n-2)(n-3)}\frac{m_4}{\sigma^4}-\frac{3(n-1)^2}{(n-2)(n-3)}. \tag{6}$$

В СКМ Maple коефіцієнт ексцесу розраховуються як [6]

$$\frac{n}{(n-1)}\frac{m_4}{\sigma^4}. \tag{7}$$

В СКМ Matlab коефіцієнт ексцесу розраховують за теоретичною формулою без приведення до нормального закону розподілу [7].

В. Гістограма.

Для з'ясування причин невідповідності гістограми було проаналізовано межі інтервалів варіаційного ряду вибірки, яку досліджували. Результати визначення меж інтервалів, розраховані за допомогою Excel, Maple, Matlab і MathCad, наведено в табл. 3.

Таблиця 3

Межі інтервалів

Excel									
Bin	13,23	13,28375	13,3375	13,39125	13,445	13,49875	13,5525	13,60625	More
Frequency	1	8	12	14	14	7	15	6	3
Maple and Matlab									
Bin	13,23000 …13,277 78	13,27778 …13,325 56	13,32556 …13,373 33	13,37333 …13,421 11	13,42111 1…13,46 889	13,46889 …13,516 67	13,51667 …13,564 44	13,56444 …13,612 222	13,61222 …13,66
Frequency	6	11	14	12	9	9	11	5	3
MathCad									
Average	13,254	13,302	13,349	13,397	13,445	13,493	13,541	13,588	13,636
Frequency	6	11	14	12	9	9	11	5	3

Порівняння меж інтервалів з табл. 2 показало, що в Excel межі інтервалів обчислюються з помилками. Це призводить до неправильного визначення кількості елементів у цих інтервалах.

Для того щоб правильно побудувати гістограму за допомогою пакету Excel, необхідно заздалегідь розрахувати межі інтервалів.

Висновки

Таким чином, коли обчислюють статистичні характеристики за допомогою комп'ютерних пакетів, необхідно:

- здійснити попереднє порівняння результатів теоретичних розрахунків та розрахунків за допомогою визначеного комп'ютерного математичного пакету;
- за наявності відмінностей з'ясувати, за якими формулами розраховані необхідні параметри, та вжити відповідних заходів для усунення можливих розбіжностей.

Список літератури:

1. Nikitenko O.M., Volovenko M.V. Chaotic behavior of oscillations in crossed-field electron vacuum devices // 2008 IEEE International Vacuum Electronics Conference, IVEC with 9th IEEE International Vacuum Electron Sources Conference, IVESC. 2008. P. 257-258.
2. Moshchenko I., Nikitenko O., Chen Xin. Research of low frequency components of a magnetron oscillator spectrum // Ukrainian Metrological Journal. 2019. No 4. P. 29 – 32.
3. Chen Xin, Ruzhentsev I. V., Nikitenko O.M. Pokaznyky yakosti elektrovakuumnykh system zi skhreshchenymy poliamy [Quality indicators of crossed-field electron vacuum systems] // Information Processing Systems. 2011. No 6 (96). P. 72 – 77. (in Ukrainian).
4. Korchakova A.S., Nikitenko O.M Osoblyvosti statystychnoi obrobky danykh za dopomohoiu kompiutera [Features of statistical data processing using a computer] // Metrology and Instruments. 2014. No 1. P. 138 – 142. (in Ukrainian).
5. Microsoft Official Academic Course MICROSOFT EXCEL 2016
https://www.dit.ie/media/ittraining/msoffice/MOAC Excel 2016 Core.pdf
6. Maple User Manual, Maplesoft, a division of Waterloo Maple Inc., 2014 https://www.maplesoft.com/documentation center/maple18/UserManual.pdf
7. MATLAB The Language of Technical Computing, https://web.stanford.edu/class/ee254/software/using ml.pdf
8. MathCAD Tutorial, Colorado State University Student, www.engr.colostate.edu/ECE562/mathcad.pdf

Надійшла до редколегії 28.08.2021

Відомості про авторів:

Мощенко Інна Олексіївна – канд. техн. наук, Харьковский национальный университет радиоэлектроники, старший викладач кафедри метрології та технічної експертизи; Україна; e-mail: inna.moshchenko@nure.ua; ORCID: https://orcid.org/0000-0002-2738-0037

Нікітенко Олександр Миколайович – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, доцент кафедри метрології та технічної експертизи; Україна; e-mail: nikonxipe@gmail.com; ORCID: https://orcid.org/0000-0002-1082-5247

Козлов Юрій Валентинович – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, доцент кафедри метрології та технічної експертизи; Украина; e-mail: yurii.kozlov@nure.ua; ORCID: https://orcid.org/0000-0002-6165-4978

Жарко Юрій Григорович – канд. техн. наук, Державне підприємство "Харківський регіональний науково-виробничий центр стандартизації, метрології та сертифікації", провідний інженер із стандартизації відділу оцінки відповідності продукції машинобудування; Украина; e-mail: 090sert@gmail.com; ORCID: https://orcid.org/0000-0002-1328-567X

УДК 621.372; 616.12-073.7 **DOI:10.30837/rt.2021.3.206.13**

Н.О. ТУЛЯКОВА, канд. техн. наук, О.М. ТРОФИМЧУК, д-р техн. наук

МОДИФИЦИРОВАННЫЕ АЛГОРИТМЫ ВЫДЕЛЕНИЯ НЕЛИНЕЙНОГО ТРЕНДА СИГНАЛОВ

Введение

Во многих практических приложениях цифровой обработки сигналов существует задача выделения нелинейного (скачкообразного) тренда сигналов. В частности, в области биомедицинских сигналов актуальной проблемой является устранение таких искажений относительно большой амплитуды и длительности, вызванных движением пациента. Для обработки такого рода сигналов, содержащих скачки и другие точки разрыва производной, не подходит разложение в гармонический ряд Фурье [1, 2] или аппроксимация суммой косинусных функций [3]. Соответственно, применение традиционных линейных фильтров высоких и низких частот (ФВЧ и ФНЧ) на основе данных ортогональных преобразований приводит к значительному сглаживанию сигнала. Адаптивные алгоритмы с динамически изменяемым размером окна [4 – 11], использующие аппроксимацию по методу наименьших квадратов [12], также сглаживают точки резких изменений сигнала. Для фильтрации сигналов, содержащих изменения, подобные резкому и наклонному перепадам (“*step*”, “*ramp*” *edges*), изломы, участки соединения прямых и плавных кривых, успешно применяются алгоритмы медианного типа, относящиеся к нелинейным устойчивым фильтрам [13 – 16]. В частности, высокую эффективность подавления флуктуаций в окрестности перепада при сохранении самой точки разрыва производной обеспечивают алгоритмы класса гибридных медианных фильтров с конечной импульсной характеристикой (КИХ). Выходные сигналы данных нелинейных фильтров определяются как медиана данных в скользящем окне, включающем отсчет входного сигнала, соответствующий центральному индексу окна, и выходные значения линейных КИХ-субапертур [13, 17 – 22]. Применение КИХ-субапертур обеспечивает подавление шума, описываемого гауссовой плотностью распределения вероятностей (ПРВ), а нелинейная медианная операция позволяет сохранять точки перепадов и устранять выбросы.

Ранее полагалось, что медианный фильтр, являющийся оптимальной робастной оценкой по критерию максимума правдоподобия для экспоненциальной функции ПРВ, имеет самую высокую нелинейность свойств и обеспечивает наилучшее сохранение скачка [13 – 16]. Однако предложенный позднее мириадный фильтр, оптимальный для ПРВ Коши, при близких к нулю значениях параметра линейности обладает более высокой робастностью (устойчивостью к выбросам) и нелинейностью свойств [23 – 27]. В частности, анализ свойств алгоритма мириадной фильтрации на основе численного метода Ньютона для поиска минимума мириадной функции потерь [28] для различных типов элементарных сигналов продемонстрировал практически оптимальное качество обработки скачка [29]. Исследования мириадных локально-адаптивных фильтров для комплексной модели одномерного сигнала, содержащей различные типы элементарных сигналов: скачок, излом, пик, точку соединения участка постоянного уровня и гладкой кривой, параболу, также показали улучшение локальных и интегральных показателей эффективности в сравнении с алгоритмами, использующими медианную фильтрацию [30 – 36]. Для обработки биомедицинских сигналов предложенные адаптивные мириадные фильтры [37 – 45] эффективнее подавляют шум, описываемый ПРВ с более “тяжелыми”, чем гауссовы, хвостами, а также имеют высокие динамические свойства (вносят малые искажения) в области резких изменений сигнала. В связи с этим, есть основания предположить, что и в алгоритмах выделения нелинейного тренда [21, 22, 46, 47] замена медианной операции на мириадную может привести к повышению качества обработки.

В сравнении с простым нахождением медианы вычисление мириады более трудоемкое. Однако в рассматриваемых алгоритмах выделения нелинейного тренда мириадную операцию предлагается применять к окнам малого размера, что не сопряжено с большими вычислительными затратами. Помимо использования мириады для получения оценки выходного сигнала по данным окна, предлагается увеличить вес отдельным его элементам, продублировав центральный отсчет и выходные значения КИХ-субфильтров, что может привести к лучшему сохранению "синусоидальных" сигналов [48, 49] и повысить эффективность подавления флуктуаций в окрестности перепадов [17 – 22].

Таким образом, целью статьи является исследование эффективности алгоритмов, используемых для выделения нелинейного тренда сигналов, и предлагаемых модификаций, заключающихся в замене медианной операции над данными в скользящем окне на мириадную и в добавлении веса определенным элементам окна.

Исследуемые алгоритмы выделения нелинейного тренда сигналов

Среди нелинейных фильтров медианного типа высоким качеством обработки окрестностей резкого и наклонного перепадов характеризуются взвешенные КИХ-гибридные медианные фильтры с добавлением веса (количества дублирований) выходным сигналам усредняющих КИХ-субапертур, являющихся экстраполяторами текущего значения сигнала в i-м отсчете 0-го порядка (экстраполяторы сигнала постоянного уровня) [19, 22, 47]. Выходной сигнал данного нелинейного фильтра описывается простым выражением:

$$y^{SWFMH}(i) = med\{\hat{x}^1_{fw}(i),\ 2\Diamond\hat{x}^0_{fw}(i),\ x(i),\ 2\Diamond\hat{x}^0_{bw}(i),\ \hat{x}^1_{fw}(i)\}, \qquad (1)$$

где $y^{SWFMH}(i)$ – выходной сигнал фильтра (*SWFMH – Subfilter Weighted FIR-median Hybrid Filter*); i – индекс, соответствующий центральному положению скользящего окна; $x(i)$ – текущий отсчет входного сигнала и центральный элемент окна; $\hat{x}^0_{fw}(i) = \frac{1}{k}\sum_{j=1}^{k} x(i-j)$, $\hat{x}^0_{bw}(i) = \frac{1}{k}\sum_{j=1}^{k} x(i+j)$ – выходные значения КИХ-субапертур, экстраполирующих ("предсказывающих") текущее значение сигнала, описываемого полиномом 0-го порядка; $\hat{x}^1_{fw}(i) = \sum_{j=1}^{k} h_j\, x(i-j)$, $\hat{x}^1_{bw}(i) = \sum_{j=1}^{k} h_j\, x(i+j)$ – выходные сигналы КИХ-экстраполяторов 1-го порядка, предсказывающих текущее значение сигнала, описываемого полиномом 1-го порядка (*the zeroth and the first order FIR predictors*). Данные КИХ-субфильтры экстраполируют сигнал в i-й точке по k предыдущим (*fw – forward prediction*) и k последующим (*bw – backward prediction*) i-му отсчетам входного сигнала в окне фильтра размером N=2k+1; $h_j = (4k - 6j + 2)/(k(k-1))$ – коэффициенты экстраполяции 1-го порядка, j=1, …, k [20, 50]; $\Diamond$ – нелинейная операция добавления веса – дублирования элемента заданное количество раз.

В данном случае медианная операция применяется к окну из семи элементов – иными словами, используется экстраполяция текущего значения сигнала в i-м отсчете по семи точкам (1). В сравнении со стандартным КИХ-гибридным медианным фильтром введением КИХ-экстраполяторов 1-го порядка достигают улучшения динамических свойств в области треугольных сигналов [19, 20, 29, 51 – 53]. Добавление веса КИХ-экстраполяторам 0-го порядка повышает эффективность подавления шума в окрестности перепада [19, 22, 47]. Одним из практических применений взвешенных КИХ-гибридных медианных фильтров является устранение артефактов движения головой в электроэнцефалограммах [19, 47, 54].

Для задач выделения нелинейного тренда сигналов предложен "Растущий на месте" КИХ-гибридный медианный фильтр (*IPGFMH – In-Place Growing FIR Median Hybrid Filter*) [13, 21, 46, 55]. Его идея заключается в эмуляции каскадной КИХ-гибридной медианной

фильтрации с увеличивающимися с каждым следующим этапом обработки окнами посредством многоуровневой повторной фильтрации в одном окне, размер которого растет относительно центрального положения. Рассмотрим алгоритм *IPGFMH* [21] с использованием экстраполяции по пяти точкам [46]: окно фильтра состоит из центрального *i*-го отсчета и выходных значений КИХ-экстраполяторов 0-го и 1-го порядков, содержащих предшествующие и последующие *i*-му отсчеты сигнала. Данный нелинейный фильтр описывается выражением

$$y_0^{IPGFMH}(i) = x(i);$$
$$y_l^{IPGFMH}(i) = med\{\frac{1}{k_l}\sum_{j=1}^{k_l} x(i-j), \frac{1}{k_l}\sum_{j=1}^{k_l} h_j x(i-j)\ ,\ y_{l-1}(i), \frac{1}{k_l}\sum_{j=1}^{k_l} h_j x(i+j), \frac{1}{k_l}\sum_{j=1}^{k_l} x(i+j)\}; \quad (2)$$
$$y^{IPGFMH}(i) = y_L(i);$$

где $k_l > k_{l-1}$ – размер КИХ-субапертур, возрастающий с каждым следующим уровнем повторной фильтрации; $l = 1 \ldots L$ – уровень фильтрации сигнала; k_L – размер максимальной субапертуры, $N = 2k_L + 1$ – размер скользящего окна фильтра.

Алгоритм *IPGFMH* [21] имеет улучшенные в сравнении с каскадным КИХ-гибридным медианным фильтром [13, 18] свойства при обработке резких перепадов. Предположим, окно фильтра достигло области перепада: его центральный элемент соответствует точке скачка, КИХ-субапертуры охватывают расположенные слева и справа отсчеты. Непосредственно вблизи точки перепада шум подавляется КИХ-субапертурами малого размера на начальных уровнях фильтрации, а КИХ-субапертуры большого размера, применяющиеся на последних уровнях, не оказывают влияния на выходной сигнал, так как различие их выходных значений велико; соответственно, в результате медианной операции на выход поступает центральный элемент окна. Применение КИХ-субапертур большого размера обеспечивает лучшее подавление шума при обработке однородных участков. Общий размер скользящего окна фильтра соответствует последнему *L*-му уровню и определяется исходя из априорной информации о длительности перепада, который необходимо сохранить при обработке [13, 18, 21].

Предлагаемые модификации алгоритмов

Предлагаются следующие модификации описанных выше алгоритмов (1) – (2).

Взвешенный КИХ-гибридный фильтр с заменой медианной операции на мириадную:

$$y^{myrSWFMH}(i) = myriad\{\hat{x}_{fw}^1(i),\ 2\Diamond\hat{x}_{fw}^0(i),\ x(i),\ 2\Diamond\hat{x}_{bw}^0(i),\ \hat{x}_{fw}^1(i),\ K_{myr}\}, \quad (3)$$

где $y^{myrSWFMH}(i)$ – выходной сигнал модифицированного *SWFMH* фильтра (1), использующего операцию нахождения мириады выборки (*myriad*); K_{myr}=0,1 – параметр нелинейности, имеющий малое значение, задающее высокую нелинейность свойств мириадному фильтру.

Мириадный алгоритм *IPGFMH* (2) с добавлением веса выходным значениям КИХ-экстраполяторов 0-го порядка и центральному элементу окна, описываемый как

$$y_0^{myrIPGFMH9P}(i) = x(i);$$
$$y_l^{myrIPGFMH9P}(i) = myriad\{2\Diamond\hat{x}_{fw_l}^0(i),\ \hat{x}_{fw_l}^1(i)\ ,\ 3\Diamond y_{l-1}(i),\ \hat{x}_{bw_l}^1(i),\ 2\Diamond\hat{x}_{bw_l}^0(i),\ K_{myr}\}; \quad (4)$$
$$y^{myrIPGFMH9P}(i) = y_L(i);$$

где $y^{myrIPGFMH9P}(i)$ – выходной сигнал модифицированного мириадного *IPGFMH* фильтра (2), экстраполирующего на каждом уровне фильтрации выходной сигнал по девяти точкам;

$$\hat{x}_{fw_l}^0(i) = \frac{1}{k_l}\sum_{j=1}^{k_l} x(i-j),\ \ \hat{x}_{fw_l}^1 = \frac{1}{k_l}\sum_{j=1}^{k_l} h_j x(i-j),\ \ \hat{x}_{bw_l}^0(i) = \frac{1}{k_l}\sum_{j=1}^{k_l} x(i+j),\ \ \hat{x}_{bw_l}^1 = \frac{1}{k_l}\sum_{j=1}^{k_l} h_j x(i+j)$$

– КИХ-субапертуры, экстраполирующие текущее *i*-е значение выходного сигнала $y(i)$ на *l*-м

уровне фильтрации по k_l предыдущим (*fw*) и k_l последующим (*bw*) отсчетам в окне данных, $k_l > k_{l-1}$; $h_j = (4k_l - 6j + 2)/(k_l(k_l - 1))$ – коэффициенты экстраполяции 1-го порядка, j=1, …, k_l; l =1…L – уровень фильтрации сигнала; K_{myr}=0,1 – параметр нелинейности; ◊ – операция добавления веса (количества повторений) определенным элементам окна.

Анализ результатов исследования

Анализ эффективности рассмотренных алгоритмов выделения нелинейного тренда проводился с помощью численного моделирования. Использовались тестовые сигналы вида "ступенькообразного" и "наклонного" перепадов ("*step edge*" и "*ramp edge*"), имитирующие нелинейный тренд, треугольный пик ("*triangular peak*") и парабола ("*parabola*").

Модель тестового воздействия описывается как

$$x(i)=s(i)+n(i), \tag{5}$$

где i – индекс отсчетов дискретного сигнала; $x(i)$ – входной сигнал; $s(i)$ – чистый сигнал; $n(i)$ – аддитивный гауссов шум с нулевым математическим ожиданием и дисперсией σ_a^2.

Для количественной оценки качества фильтрации вычислялись значения среднеквадратической ошибки (СКО), усредненные для большого количества реализаций тестового сигнала с шумом, по формуле

$$MSE = \sum_{j=1}^{N_R} \left(\sum_{i=1}^{I} (y^f(i) - s(i)^2 / I) / N_R \right), \tag{6}$$

где *MSE* (*mean squire error*) – критерий СКО; I – длительность тестового сигнала; $y^f(i)$ – выходной сигнал фильтра; $s(i)$ – тестовый сигнал без шума; N_R – количество реализаций тестового сигнала со сгенерированным с помощью датчика случайных чисел шумом.

Критерий минимума СКО [13] интегрально характеризует уменьшение дисперсии шума на выходе фильтра и динамические ошибки, вносимые им при обработке. Для получения устойчивых результатов оценок эффективности статистическое усреднение проводилось для большого количества реализаций N_R=200.

Исследовались следующие нелинейные фильтры: *SWFMH* – взвешенный КИХ-гибридный медианный фильтр (1); *IPGFMH* – "Растущий на месте" КИХ-гибридный медианный фильтр (2), экстраполирующий выходной сигнал по пяти точкам; модифицированные фильтры: *IPGFMH9P* – алгоритм *IPGFMH* с экстраполяцией сигнала по девяти точкам, *myrSWFMH, myrIPGFMH, myrIPGFMH9P* – соответствующие мириадные алгоритмы (префикс "*myr*" – *myriad*); двухпроходные фильтры *TPSWFMH, TPmyrSWFMH, TPmyrIPGFMH, TPmyrIPGFMH9P* ("*TP*" – *two-pass*). Для сравнения исследовались медианный (*Med*) и мириадный (*Myr*) фильтры и их двухпроходные варианты (*TPMed, TPMyr*).

Рассмотрим тестовый сигнал вида "резкий перепад" ("*step edge*") при воздействии аддитивного гауссова шума среднего уровня (дисперсия σ_a^2=0,01). Выходные сигналы исследуемых нелинейных фильтров приведены на рис. 1, графики, характеризующие подавление шума фильтрами по критерию СКО (6) в зависимости от размера окна *N*, – на рис. 2.

Как видим (рис. 1, *б, в*, рис. 2, *а*), ошибки *Myr* фильтра в сравнении с *Med* меньше. Для данных фильтров целесообразен выбор меньших окон, и имеется явный минимум кривой СКО, свидетельствующий о наличии оптимального размера окна (рис. 2, *а*). В сравнении с *Med* фильтром алгоритмы *SWFMH, IPGFMH* и их модификации (рис. 1, *г – и*) заметно улучшают качество обработки перепада: значения СКО более чем в 3,5 и 5 раз меньше (рис. 2, *б – г*). Замена медианной операции на мириадную [29] в алгоритмах *SWFMH* и *IPGFMH* заметно уменьшает значения СКО при обработке скачка. В отличие от *Med, Myr* и *SWFMH* фильтров для алгоритмов *myrSWFMH, IPGFMH, myrIPGFMH, IPGFMH9P, myrIPGFMH9* минимальные значения СКО "размыты" в широком диапазоне изменения размера окна *N* (рис. 2). На практике данное свойство может оказаться полезным, так как априорная информация о длительности перепада (тренда), в соответствии с которой выбирается размер окна, не всегда

доступна. Повторная фильтрация уменьшает значения СКО для моделируемой ситуации среднего уровня гауссова шума, однако при больших окнах становится нецелесообразной вследствие увеличения динамических ошибок фильтров.

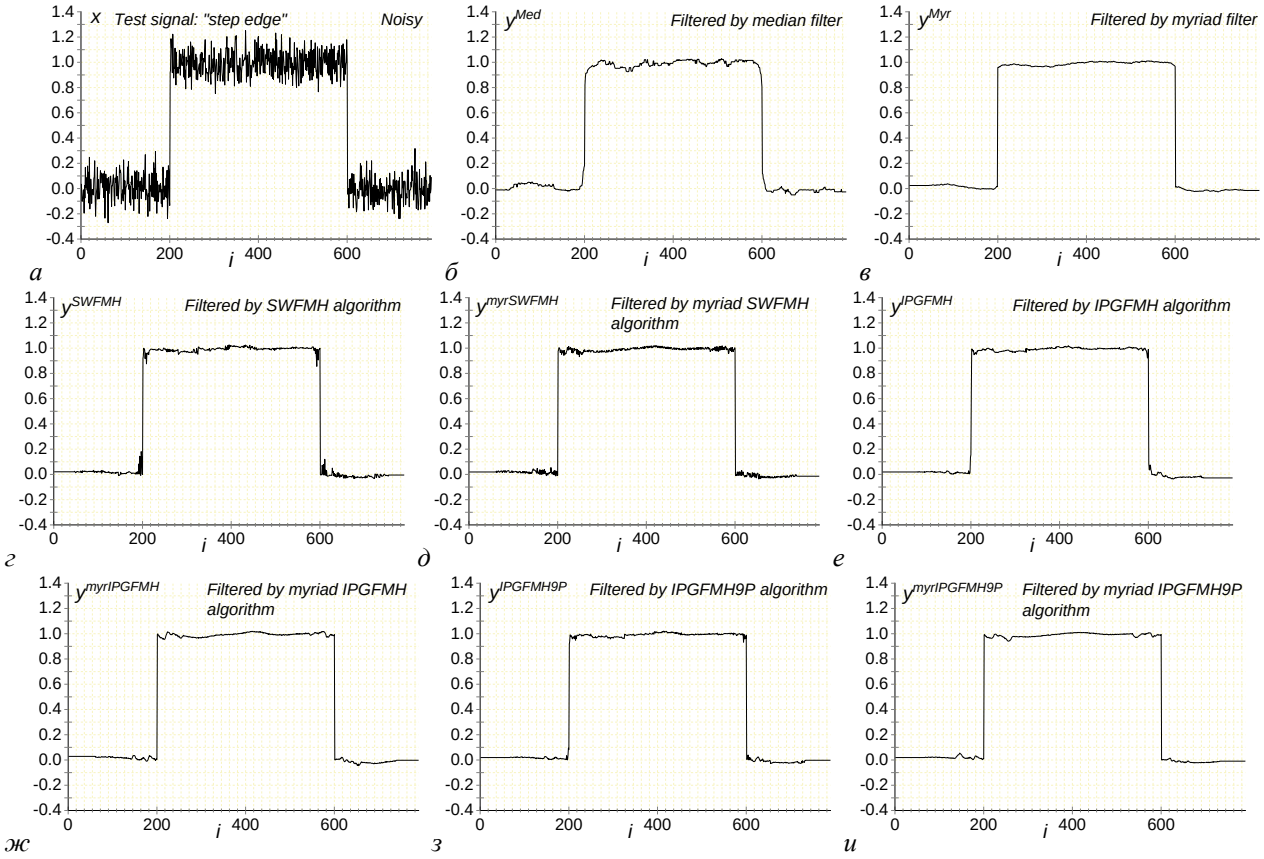


Рис. 1. Применение нелинейной фильтрации для сигнала вида “резкий перепад”: *а* – входной сигнал с аддитивным гауссовым шумом; *б*, *в* – выходные сигналы *Med* и *Myr* фильтров; *г*, *д* – выходные сигналы *SWFMH* фильтра и его мириадного варианта *myrSWFMH*; *е*, *ж* – выходные сигналы *IPGFMH* фильтра и его мириадного варианта *myrIPGFMH* с экстраполяцией сигнала по пяти точкам; *з*, *и* – выходные сигналы *IPGFMH9P* фильтра и его мириадного варианта *myrIPGFMH9P* с экстраполяцией сигнала по девяти точкам

Рассмотрим тестовый сигнал вида “наклонный перепад” (“*ramp edge*”) при воздействии аддитивного гауссова шума среднего уровня (σ_a^2=0,01). Выходные сигналы фильтров приведены на рис. 3, а усредненные кривые, иллюстрирующие уменьшение СКО (6), – на рис. 4.

Для данного тестового сигнала ошибки рассмотренных фильтров немного увеличились: примерно в 1,4 и 1,1 раза для *Med* и *Myr* фильтров (рис. 3, *б*, *в*), в 1,1 раз для *SWFMH* (рис. 3, *г*) и в 1,2 – 1,3 раза – для *IPGFMH* (рис. 3, *е*) и *IPGFMH9P* (рис. 3, *з*). Преимущество замены медианной операции на мириадную менее наглядно: *myrSWFMH* (рис. 3, *д*) улучшает эффективность *SWFMH* (рис. 3, *г*) примерно в 1,3 раза (рис. 4, *б*), а для *myrIPGFMH* (рис. 3, *ж*) и *myrIPGFMH9P* (рис. 3, *и*) значения СКО в сравнении с *IPGFMH* (рис. 3, *е*) и *IPGFMH9P* (рис. 3, *з*) уменьшились в 1,1 и 1,4 раза (рис. 4, *в*, *г*). Минимум СКО для *SWFMH* и *IPGFMH* и их модификаций (рис. 4, *б* – *г*) “размыт” в менее широком диапазоне изменения размера окна. Использование мириадной операции улучшает эффективность подавления шума на линейно изменяющемся участке: сравним выходные сигналы *IPGFMH* (рис. 3, *е*) и *IPGFMH9P* (рис. 3, *з*) с их мириадными вариантами *myrIPGFMH* (рис. 3, *ж*) и *myrIPGFMH9P* (рис. 3, *и*). Наиболее эффективным также является алгоритм *myrIPGFMH9P*, обеспечивающий уменьшение СКО в сравнении с *myrSWFMH* примерно в 1,3 раза, а с исходным вариантом *IPGFMH* – в 1,6 раза.

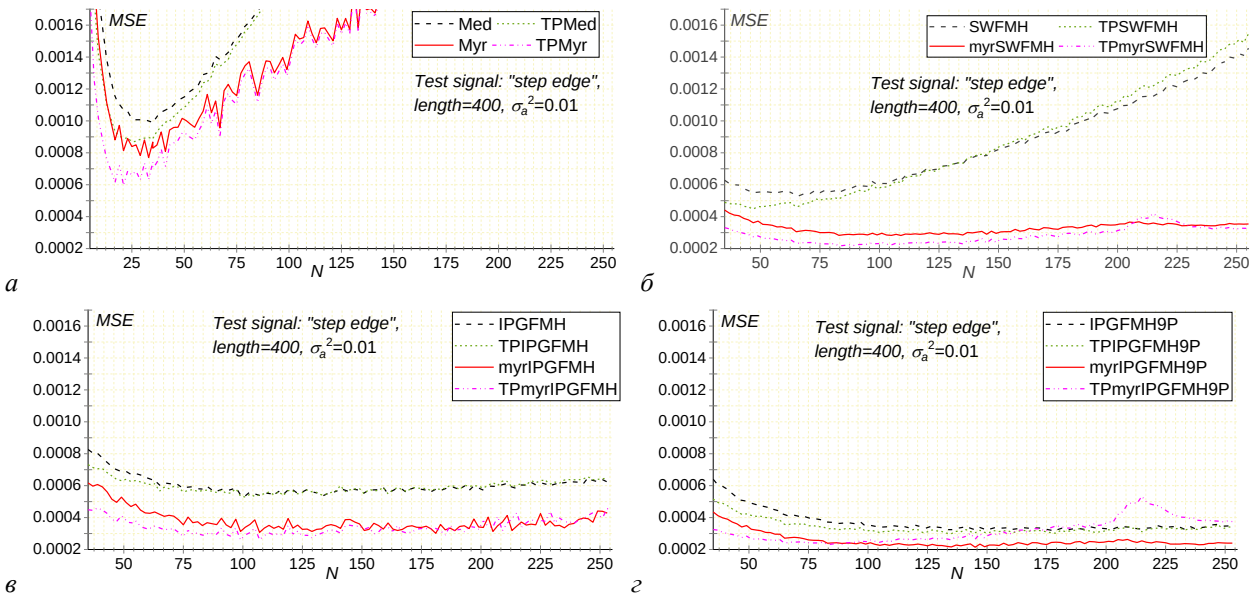


Рис. 2. Статистические оценки эффективности фильтров по критерию СКО для тестового сигнала вида “резкий перепад” с аддитивным гауссовым шумом: *а* – ошибки *Med* и *Myr* фильтров и их двухпроходных реализаций: *TPMed*, *TPMyr*; *б* – ошибки *SWFMH* и его мириадного *myrSWFMH* и двухпроходных *TPSWFMH*, *TPmyrSWFMH* вариантов; *в* – ошибки *IPGFMH* с экстраполяцией сигнала по пяти точкам и перечисленных модификаций фильтра: *myrIPGFMH*, *TPIPGFMH*, *TPmyrIPGFMH*; *г* – ошибки *IPGFMH9P* с экстраполяцией сигнала по девяти точкам и его мириадного *myrIPGFMH9P* и двухпроходных *TPIPGFMH9P*, *TPmyrIPGFMH9P* вариантов

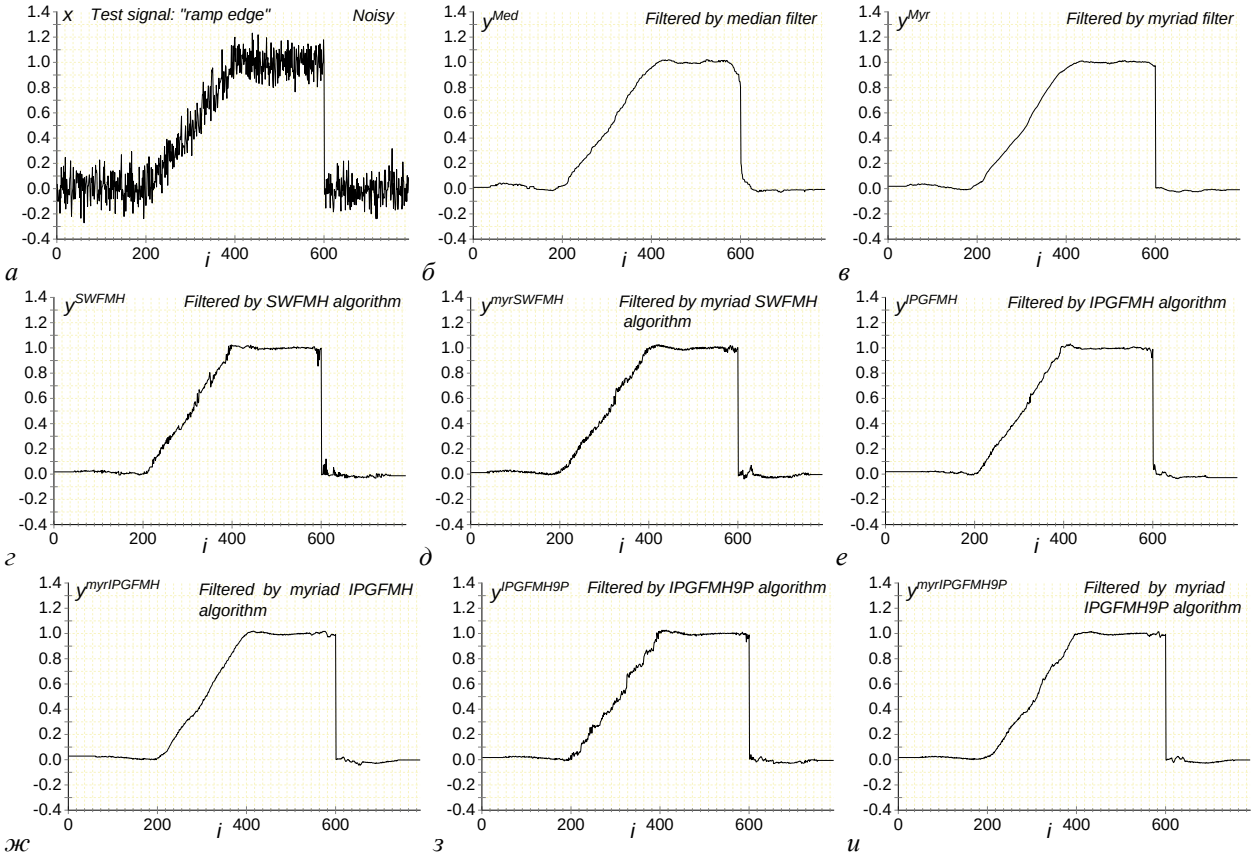


Рис. 3. Применение нелинейной фильтрации для сигнала вида “наклонный перепад”: *а* – входной сигнал с аддитивным гауссовым шумом; *б*, *в* – выходные сигналы *Med* и *Myr* фильтров; *г*, *д* – выходные сигналы *SWFMH* фильтра и его мириадного варианта *myrSWFMH*; *е*, *ж* – выходные сигналы *IPGFMH* фильтра и его мириадного варианта *myrIPGFMH* с экстраполяцией сигнала по пяти точкам; *з*, *и* – выходные сигналы *IPGFMH9P* фильтра и его мириадного варианта *myrIPGFMH9P* с экстраполяцией сигнала по девяти точкам

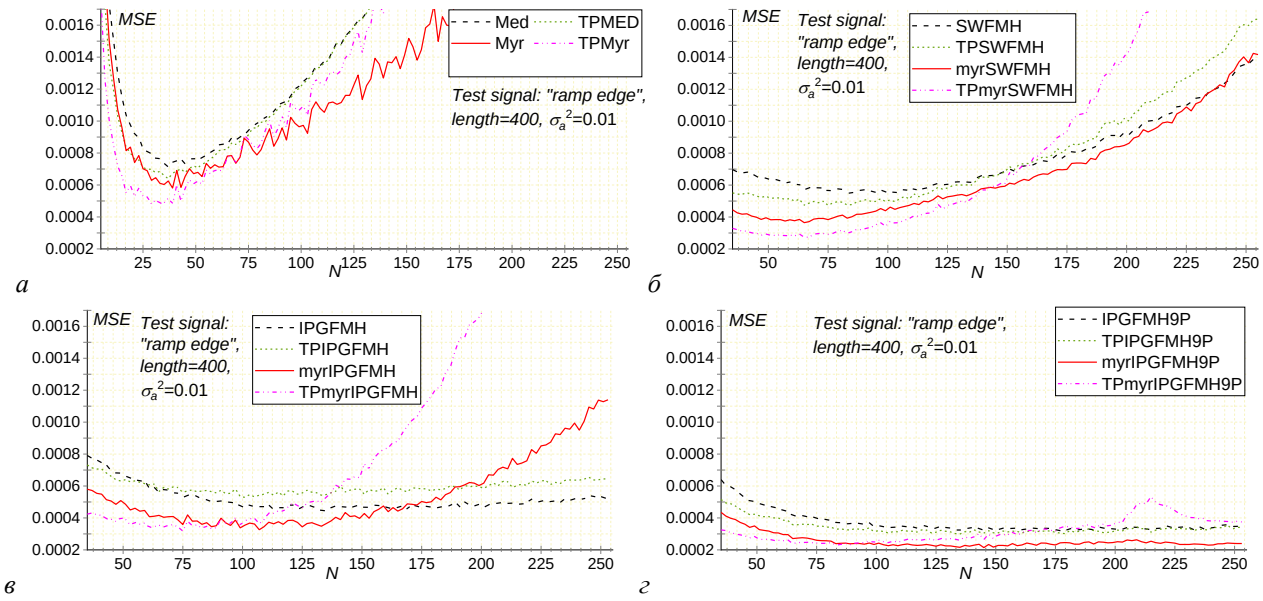


Рис. 4. Статистические оценки эффективности фильтров по критерию СКО для тестового сигнала “наклонный перепад” с аддитивным гауссовым шумом: *а* – ошибки *Med* и *Myr* фильтров и их двухпроходных реализаций: *TPMed*, *TPMyr*; *б* – ошибки *SWFMH* и его мириадного *myrSWFMH* и двухпроходных *TPSWFMH*, *TPmyrSWFMH* вариантов; *в* – ошибки *IPGFMH* с экстраполяцией сигнала по пяти точкам и перечисленных модификаций фильтра: *myrIPGFMH*, *TPIPGFMH*, *TPmyrIPGFMH*; *г* – ошибки *IPGFMH9P* с экстраполяцией сигнала по девяти точкам и его мириадного *myrIPGFMH9P* и двухпроходных *TPIPGFMH9P*, *TPmyrIPGFMH9P* вариантов

Рассмотрим тестовый сигнал вида треугольного экстремума (“*triangular peak*”) при воздействии аддитивного гауссова шума среднего уровня (σ_a^2=0,01). Сигналы на выходах фильтров приведены на рис. 5, графики СКО (6) в зависимости от размера окна – на рис. 6.

Треугольный сигнал, наряду с “резким” и “наклонным” перепадами, является стабильной точкой фильтров (1) – (4), использующих КИХ-экстраполяцию 1-го порядка. К стабильным точкам (*root signals*) нелинейного фильтра относятся сигналы, которые в отсутствие помех полностью сохраняются на его выходе [13]. Стабильными точками медианного фильтра являются “резкий” и “наклонный” перепады. Введением КИХ-экстраполяторов 1-го порядка расширяют набор стабильных точек включением в него наряду с перепадами треугольного сигнала [13, 17 – 20]. Как видим (рис. 5), изломы сохранены достаточно хорошо, “провала” в области экстремума, свойственного стандартному КИХ-гибридному медианному фильтру [51, 53], не наблюдается. Алгоритмы, использующие мириадную фильтрацию, лучше подавляют шум: сравним выходные сигналы *SWFMH* (рис. 5, *г*) и *myrSWFMH* (рис. 5, *д*), *IPGFMH9P* (рис. 5, *з*) и *myrIPGFMH9P* (рис. 5, *и*).

Для треугольного сигнала эффективность *Med* и *Myr* фильтров практически одинакова (СКО для *Myr* в 1,1 раз меньше). Минимум СКО для алгоритмов *SWFMH* и *myrSWFMH* (рис. 6, *б*), *IPGFMH* и *myrIPGFMH* (рис. 6, *в*), *IPGFMH9P* и *myrIPGFMH9P* (рис. 6, *г*) менее “размыт” в сравнении с обработкой “резкого” (рис. 2, *б* – *г*) и “наклонного” (рис. 4, *б* – *г*) перепадов. При меньших окнах (N≤100) эффективней мириадные алгоритмы (рис. 6, *б* – *г*), а при больших окнах – меньшие СКО имеют медианные фильтры, причем кривая минимальных значений СКО для *IPGFMH* (рис. 6, *в*) и *IPGFMH9P* (рис. 6, *г*) имеет протяженный характер. Для больших окон (N>100) применение *IPGFMH* наиболее эффективно (рис. 6, *в*). Для меньших окон (N≤75) для *Med*, *Myr*, *myrSWFMH*, *myrIPGFMH9P* фильтров минимум СКО более явный, а наименьшие СКО обеспечивают *Myr* и *myrIPGFMH9P*. Преимущество *myrIPGFMH9P* над *IPGFMH9P* составляет 1,4 раза, а над *IPGFMH* – 1,6 раза.

Рассмотрим тестовый сигнал вида параболы (“*parabola*”) при воздействии аддитивного гауссова шума среднего уровня (σ_a^2=0,01). Сигналы на выходах фильтров приведены на рис. 7, а графики значений СКО (6) в зависимости от размера окна – на рис. 8.

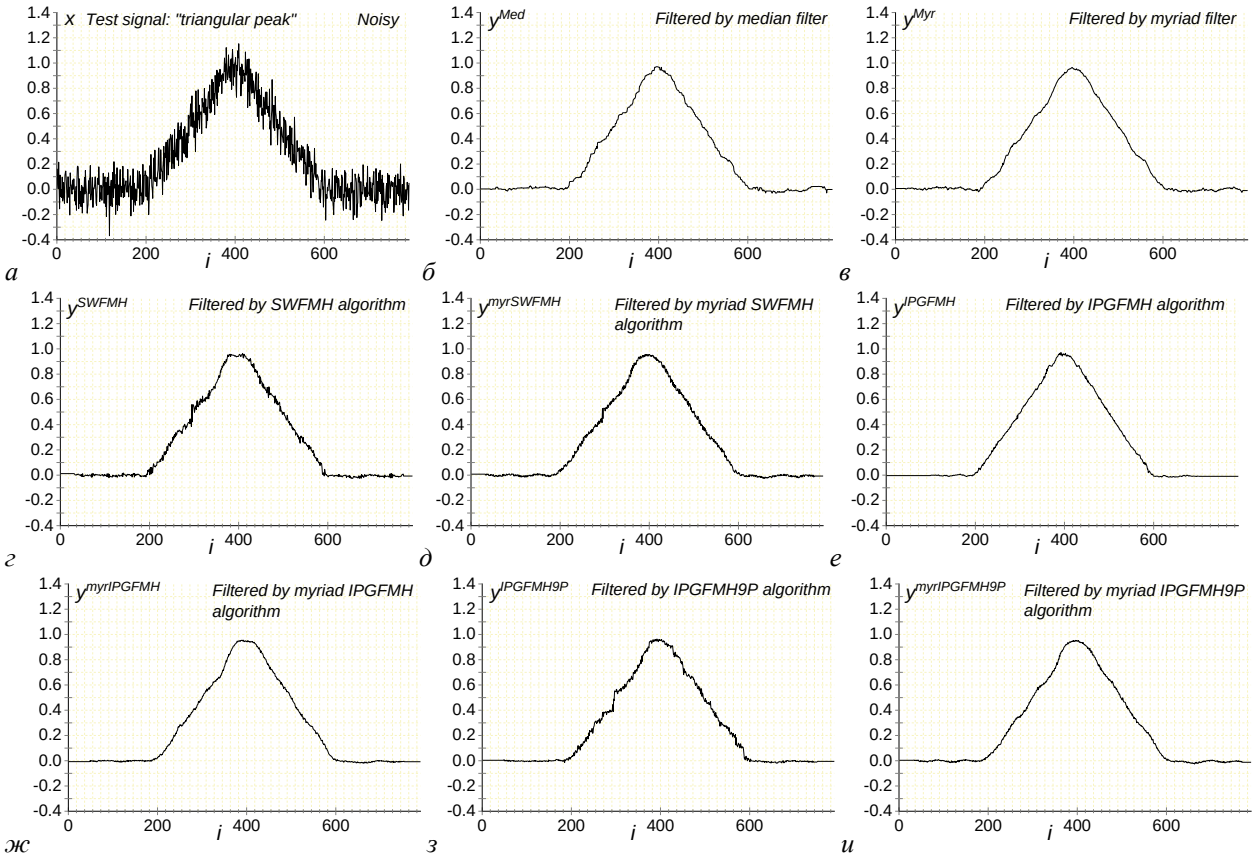


Рис. 5. Применение нелинейной фильтрации для сигнала вида “треугольный экстремум”: *а* – входной сигнал с аддитивным гауссовым шумом; *б*, *в* – выходные сигналы *Med* и *Myr* фильтров; *г*, *д* – выходные сигналы *SWFMH* фильтра и его мириадного варианта *myrSWFMH*; *е*, *ж* – выходные сигналы *IPGFMH* фильтра и его мириадного варианта *myrIPGFMH* с экстраполяцией сигнала по пяти точкам; *з*, *и* – выходные сигналы *IPGFMH9P* фильтра и его мириадного варианта *myrIPGFMH9P* с экстраполяцией сигнала по девяти точкам

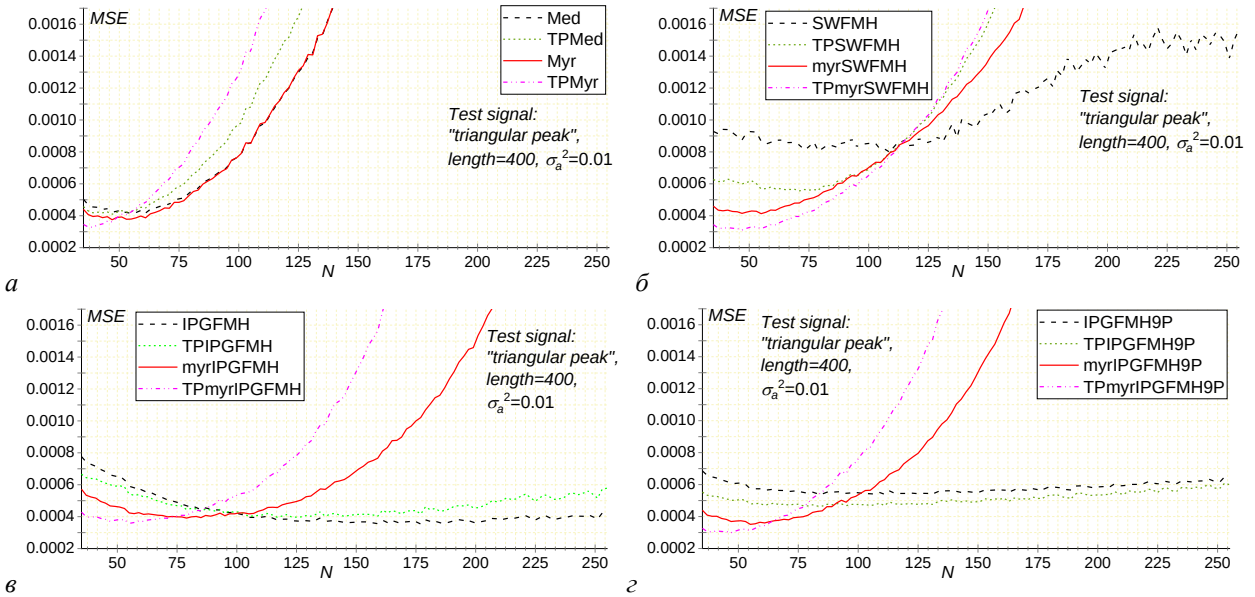


Рис. 6. Статистические оценки эффективности фильтров по критерию СКО для тестового сигнала “треугольный экстремум” с аддитивным гауссовым шумом: *а* – ошибки *Med* и *Myr* фильтров и их двухпроходных реализаций: *TPMed*, *TPMyr*; *б* – ошибки *SWFMH* и его мириадного *myrSWFMH* и двухпроходных *TPSWFMH*, *TPmyrSWFMH* вариантов; *в* – ошибки *IPGFMH* с экстраполяцией сигнала по пяти точкам и перечисленных модификаций фильтра: *myrIPGFMH*, *TPIPGFMH*, *TPmyrIPGFMH*; *г* – ошибки *IPGFMH9P* с экстраполяцией сигнала по девяти точкам и его мириадного *myrIPGFMH9P* и двухпроходных *TPIPGFMH9P*, *TPmyrIPGFMH9P* вариантов

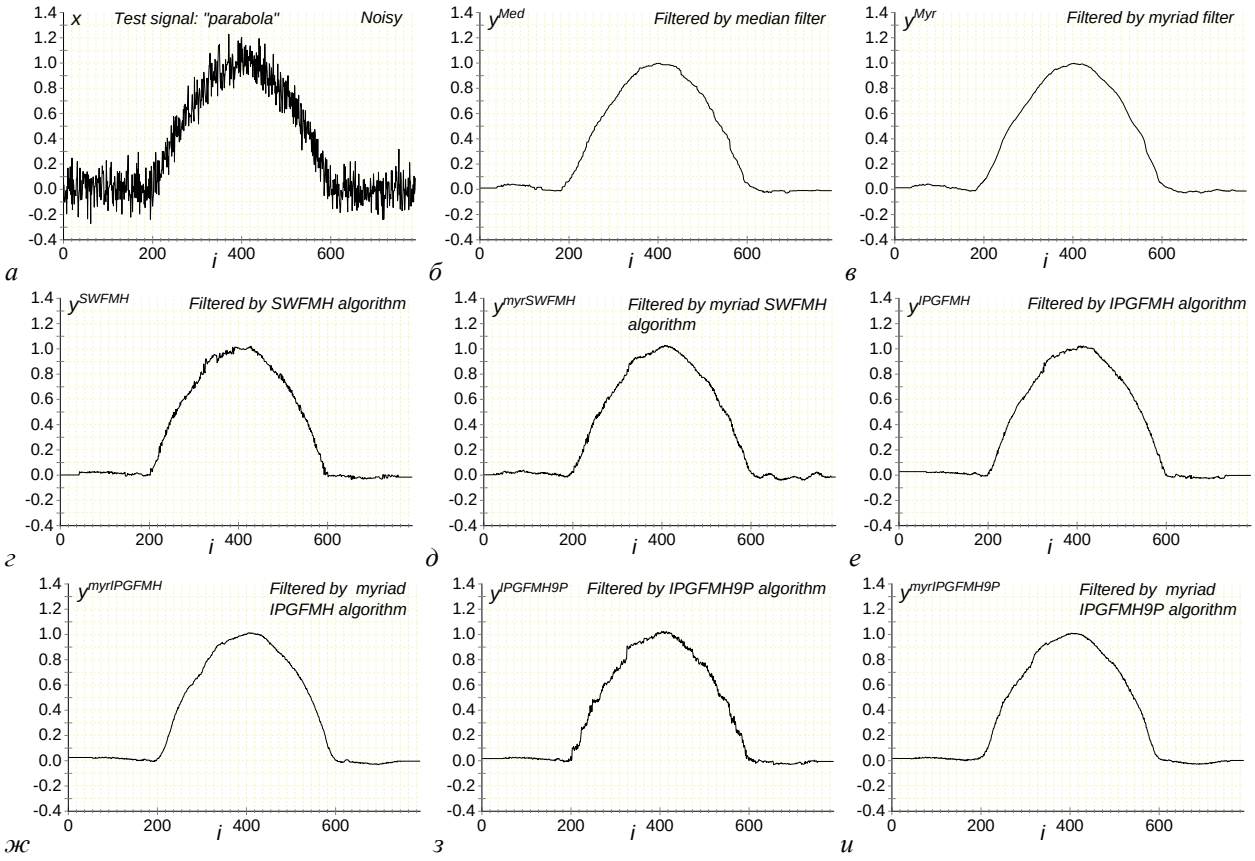


Рис. 7. Применение нелинейной фильтрации для сигнала вида “парабола”: *а* – входной сигнал с гауссовым шумом; *б*, *в* – выходные сигналы *Med* и *Myr* фильтров; *г*, *д* – выходные сигналы *SWFMH* фильтра и его мириадного варианта *myrSWFMH*; *е*, *ж* – выходные сигналы *IPGFMH* фильтра и его мириадного варианта *myrIPGFMH* с экстраполяцией сигнала по пяти точкам; *з*, *и* – выходные сигналы *IPGFMH9P* фильтра и его мириадного варианта *myrIPGFMH9P* с экстраполяцией сигнала по девяти точкам

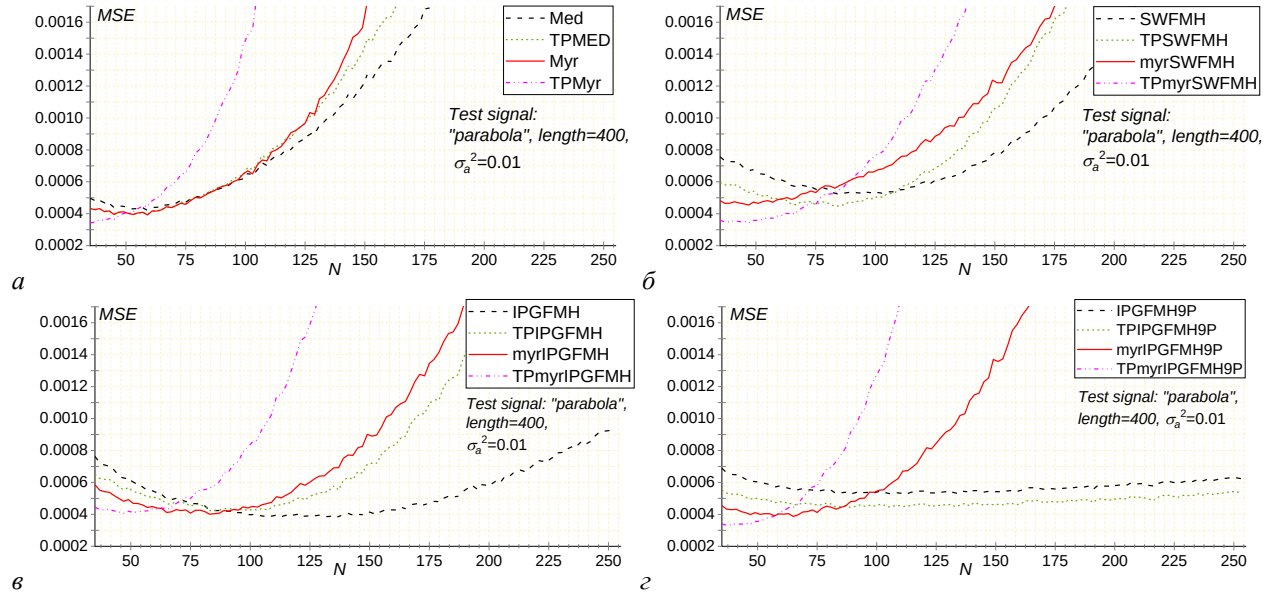


Рис. 8. Статистические оценки эффективности фильтров по критерию СКО для тестового сигнала “парабола” с аддитивным гауссовым шумом: *а* – ошибки *Med* и *Myr* фильтров и их двухпроходных реализаций: *TPMed*, *TPMyr*; *б* – ошибки *SWFMH* и его мириадного *myrSWFMH* и двухпроходных *TPSWFMH*, *TPmyrSWFMH* вариантов; *в* – ошибки *IPGFMH* с экстраполяцией сигнала по пяти точкам и перечисленных модификаций фильтра: *myrIPGFMH*, *TPIPGFMH*, *TPmyrIPGFMH*; *г* – ошибки *IPGFMH9P* с экстраполяцией сигнала по девяти точкам и его мириадного *myrIPGFMH9* и двухпроходных *TPIPGFMH9P*, *TPmyrIPGFMH9P* вариантов

Как видим (рис. 7), качество обработки параболы достаточно высокое. Мириадные фильтры улучшают подавление шума на восходящей и нисходящей ветвях кривой: сравним выходные сигналы *SWFMH* (рис. 7, *г*) и *myrSWFMH* (рис. 7, *д*), алгоритмов *IPGFMH* (рис. 7, *е*) и *myrIPGFMH* (рис. 7, *ж*), *IPGFMH9P* (рис. 7, *з*) и *myrIPGFMH9P* (рис. 7, *и*). Точки соединения участков постоянного уровня и ветвей параболы не сглажены. Благодаря использованию КИХ-экстраполяторов 1-го порядка “провала” в области экстремума параболы, характерного для стандартного КИХ-гибридного медианного фильтра, не наблюдается.

В данном случае до определенного размера окна (N<100) эффективность *Med* и *Myr* фильтров практически одинаковая, а при больших окнах СКО для *Med* меньше (рис. 8, *а*). Для алгоритмов *IPGFMH* и *IPGFMH9P* применение мириадной операции (при N<100) уменьшает значения СКО примерно в 1,2 – 1,3 раза по сравнению с *Med* фильтром (рис. 8, *б* – *г*). Наименьшие СКО в широком диапазоне изменения окна (N≤105) имеет *myrIPGFMH9P*, однако его преимущество над *Med*, *Myr* и *myrSWFMH* незначительно (в 1,1 – 1,3 раза).

Применение *IPGFMH9P* и *myrIPGFMH9P* для фильтрации сигналов электронейрограмм (ЭНГ) глаз и электроэнцефалограммы (ЭЭГ) показано на рис. 9 – 11.

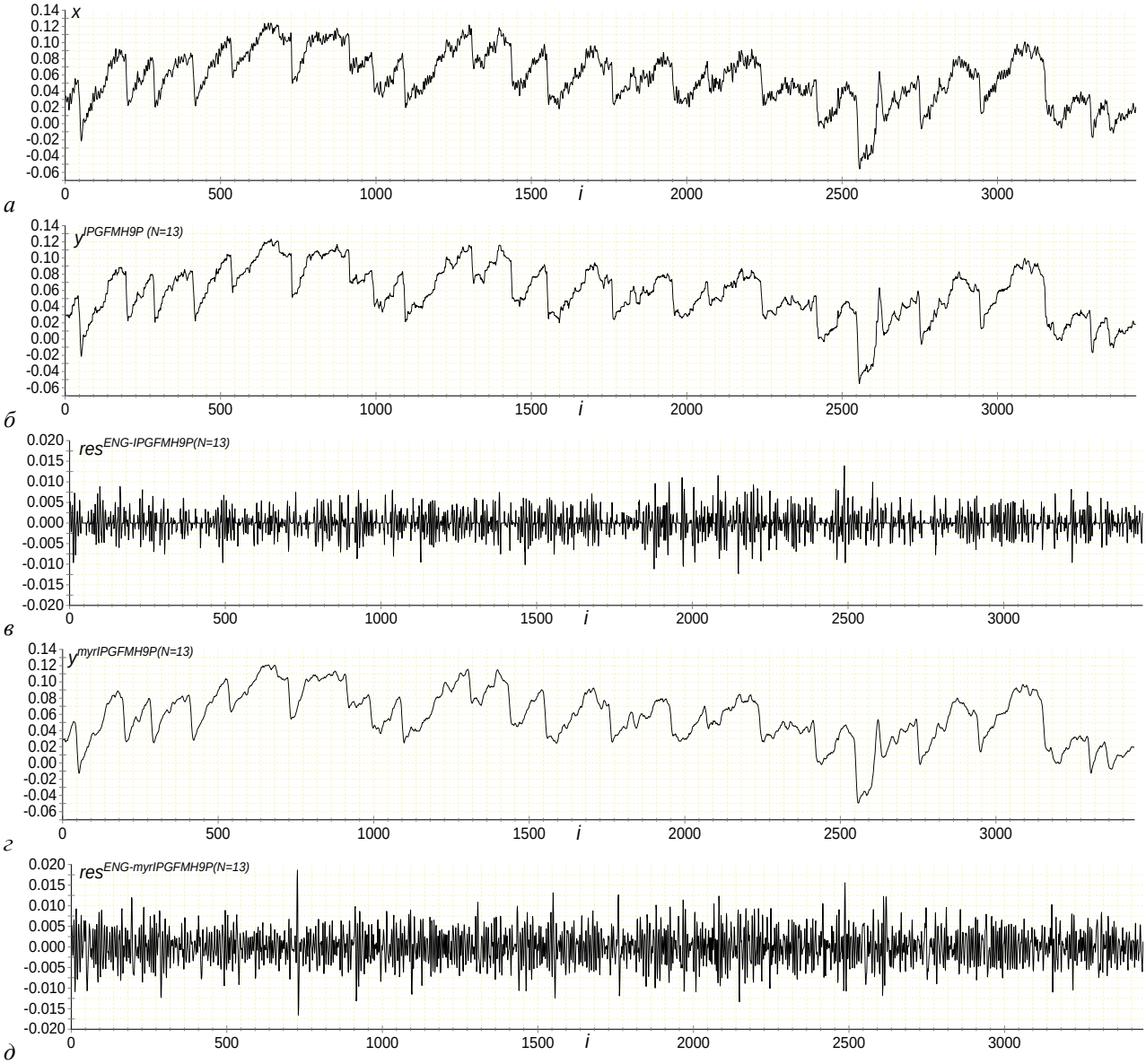


Рис. 9. Обработка ЭНГ левого глаза: *а* – входной сигнал; *б* – сигнал на выходе *IPGFMH9P* (размер окна N=13); *в* – разность между входным сигналом и сигналом на выходе *IPGFMH9P*; *г* – выходной сигнал мириадного фильтра *myrIPGFMH9P* (N=13); *д* – разность между входным сигналом и сигналом на выходе *myrIPGFMH9P*

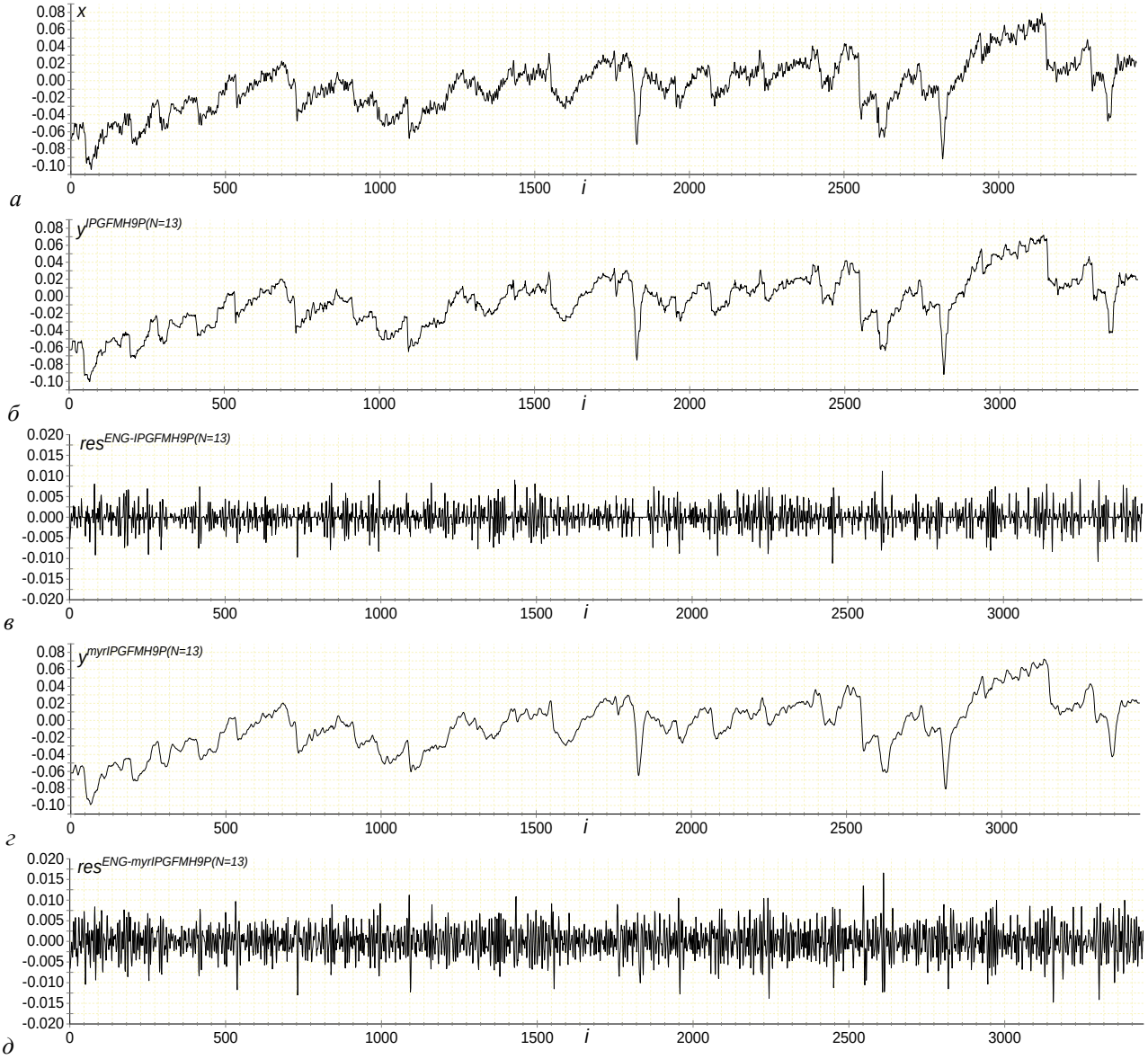


Рис. 10. Обработка ЭНГ правого глаза: *а* – входной сигнал; *б* – сигнал на выходе алгоритма *IPGFMH9P* (*N*=13); *в* – разность между входным сигналом и сигналом на выходе *IPGFMH9P*; *г* – выходной сигнал мириадного фильтра *myrIPGFMH9P* (*N*=13); *д* – разность между входным сигналом и сигналом на выходе *myrIPGFMH9P*

Как видим (рис. 9 – 10), использование мириадной операции улучшает подавление высокочастотных флуктуаций при хорошем сохранении скачков и других резких изменений сигнала. При небольших размерах окна указанные нелинейные фильтры, подобно линейным ФНЧ, хорошо подавляют шум, а при больших окнах ведут себя как нелинейные аналоги ФВЧ, хорошо сохраняя изменения в сигнале относительно большой длительности вида резкого и наклонного перепадов, по форме подобные низкочастотным сигналам, описываемым аналитическими функциями. Так, для ЭНГ глаз (рис. 9 – 10) хорошо подавляется флуктуационная составляющая, и, в отличие от линейных фильтров, незначительно сглаживаются резкие изменения сигнала. Для устранения двигательных артефактов (рис. 11) фильтруется шумоподобный сигнал ЭЭГ, а выделяется нелинейный тренд, содержащий артефакты (моргания глаз), который затем вычитаются из исходного сигнала. При этом высокочастотный спектр информационного сигнала хорошо сохраняется.

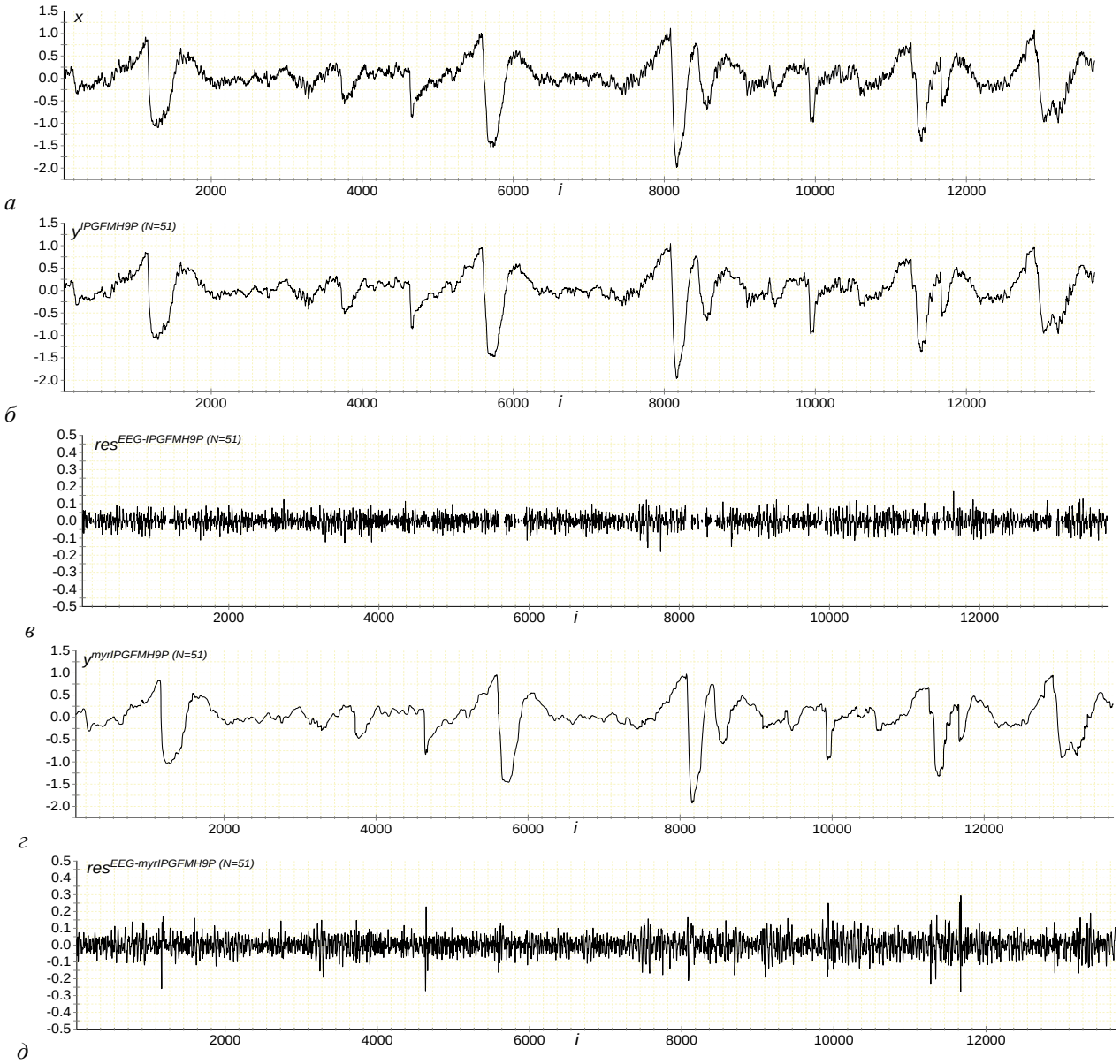


Рис. 11. Устранение артефактов в ЭЭГ: *а* – входной сигнал; *б* – сигнал на выходе *IPGFMH9P* (*N*=51); *в* – разность исходного сигнала и выходного сигнала *IPGFMH9P*; *г* – сигнал на выходе мириадного фильтра *myrIPGFMH9P* (*N*=51); *д* – разность исходного сигнала и выходного сигнала *myrIPGFMH9P*

Таким образом, основываясь на анализе выходных сигналов исследуемых алгоритмов нелинейной фильтрации и эффективности их применения для тестовых сигналов вида резкого и наклонного перепадов, треугольного пика и параболы, можно сделать выводы:

- рассмотренные алгоритмы, применяющиеся в задачах выделения нелинейного тренда, обеспечивают высокое качество обработки указанных типов сигналов, значительно улучшая эффективность медианного фильтра в области перепадов;
- модификация алгоритмов путем замены медианной операции на мириадную улучшает качество выходных сигналов в области скачка и эффективность подавления высокочастотных флуктуаций;
- применение мириадной фильтрации повышает степень подавления шума на линейно изменяющихся участках наклонного перепада и треугольного сигнала и на ветвях параболы;
- добавление веса центральному элементу окна и выходным значениям КИХ-экстраполяторов 0-го порядка повышает качество обработки окрестностей перепадов;

- использование КИХ-экстраполяторов 1-го порядка позволяет избежать недостатка, присущего стандартному КИХ-гибридному медианному фильтру, заключающегося в искажениях вида провала в области параболического и треугольного экстремумов;

- повторная обработка сигнала повышает степень подавления шума, однако целесообразна при небольших размерах окон;

- среди рассмотренных алгоритмов наилучшую эффективность обеспечивает “Растущий на месте” КИХ-гибридный алгоритм с заменой медианной операции на мириадную, причем, преимущество наиболее наглядно при обработке скачков сигнала;

- при небольших размерах окон рассмотренные нелинейные фильтры могут применяться для подавления высокочастотного шума (подобно ФНЧ), при этом, ими хорошо сохраняются резкие изменения сигнала, а при больших окнах – для выделения нелинейного тренда (как нелинейные аналоги ФВЧ), что может использоваться для задач устранения двигательных артефактов в биомедицинских сигналах, в частности в ЭЭГ;

- рассмотренные алгоритмы нелинейной фильтрации имеют простую реализацию и могут выполнять обработку сигнала в режиме квазиреального времени.

Заключение

Рассмотрены алгоритмы нелинейной устойчивой фильтрации класса КИХ-гибридных медианных фильтров, применяемые в задачах выделения нелинейного тренда сигналов. В данных алгоритмах, имеющих простую реализацию, используется операция нахождения медианы данных в скользящем окне, включающем текущее *i*-е значение входного сигнала, соответствующее центральному элементу окна, и выходные значения КИХ-субапертур, являющихся экстраполяторами 0-го и 1-го порядков. КИХ-субапертуры содержат отсчеты сигнала, предшествующие и следующие за текущим *i*-м отсчетом. Предложено модифицировать данные алгоритмы путем замены операции определения медианы данных в окне на вычисление их мириады, а также добавления веса центральному элементу окна и выходным значениях КИХ-экстраполяторов 0-го порядка.

С помощью численного моделирования получены статистические оценки эффективности по критерию СКО для тестовых сигналов вида “резкий” и “наклонный” перепады, треугольный экстремум и парабола. Построены графики статистически усредненных значений СКО в зависимости от размера окна фильтра, интегрально характеризующие ослабление шума и динамические ошибки, вносимые в результате фильтрации. На основе анализа выходных сигналов фильтров и статистических оценок их качества показаны высокая эффективность применения исследованных нелинейных фильтров для перечисленных типов сигналов и улучшения, достигнутые в результате предложенных модификаций фильтров. Приведены примеры обработки биомедицинских сигналов ЭНГ и ЭЭГ, иллюстрирующие хорошее качество подавления высокочастотных флуктуаций и, одновременно, сохранения резких изменений сигнала, и удаление двигательных артефактов (моргания глаз) без значительных искажений сигнала.

Список литературы:

1. Oppenheim A. V., Schafer R. W. Discrete time Signal Processing. Englewood Cliffs, NJ: Prentice Hall, 1989.
2. Lathi B. P. Signal Processing and Linear Systems. Carmichael, CA: Berkeley-Cambridge, 1998.
3. Rao A., Yip P. Discrete Cosine Transform. Academic Press, 1990.
4. Christov I. I., Daskalov I. K. Filtering of electromyogram artifacts from the electrocardiogram // Med. Eng. Phys. 1999. Vol. 21. P. 731–736. https://doi.org/10.1016/S1350-4533(99)00098-3
5. Dotsinsky I., Mihov G. Simple approach for tremor suppression in electrocardiograms // Int. J. Bioaotomation. 2010. Vol. 14, No. 2. P. 129–138.
6. Bortolan G., Christov I. Dynamic filtration of high-frequency noise in ECG signal // Comput. Cardiol. 2014. Vol. 41. P. 1089–1092. http://www.cinc.org/archives/2014/pdf/ 1089.pdf
7. Bortolan G., Christov I., Simova I., Dotsinsky I. Noise processing in exercise ECG stress test for the analysis and the clinical characterization of QRS and T wave alternans // Biomedical Signal Processing and Control. 2015. Vol. 18. P. 378–385. https://doi.org/10.1016/j.bspc.2015.02.003

8. Christov I., Neycheva T., Schmid R., Stoyanov T., Abächerli R. Pseudo real-time low-pass filter in ECG, self-adjustable to the frequency spectra of the waves // Med. Biol. Eng. Comput. 2017. Vol. 55. P. 1579–1588. https://doi.org/10.1007/s11517-017-1625-y

9. Christov I., Neycheva T., Schmid R. Fine tuning of the dynamic low-pass filter for electromyographic noise suppression in electrocardiograms // Comput. Cardiol. 2017. Vol. 44. P. 1–4. http://www.cinc.org/archives/2017/pdf/088-007.pdf, https://doi.org/10.22489/CinC.2017.088-007

10. Christov I., Gotchev A., Bortolan G., Neycheva T., Raikova R., Schmid R. Separation of the electromyographic from the electrocardiographic signals and vice versa. A topical review of the Dynamic procedure // Int. J. Bioaotomation. 2020. Vol. 24, No. 3. P. 289–317. https://doi.org/10.7546/ijba.2020.24.3.000744

11. Tulyakova N., Trofymchuk O. Real-time filtering adaptive algorithms for non-stationary noise in electrocardiograms // Biomedical Signal Processing and Control. 2022. Vol. 72. https://doi.org/10.1016/j.bspc.2021.103308

12. Savitzky A., Golay M. Smoothing and differentiation of data by simplified least squares procedures // Anal. Chem. 1964. Vol. 36. P. 1627–1639. https://doi.org/10.1021/ac60214a047

13. Astola J., Kuosmanen P. Fundamentals of Nonlinear Digital Filtering. USA: CRC Press LLC, 1997. 276 p.

14. Pitas I., Venetsanopoulos A. N. Nonlinear Digital Filters: Principles and Application. USA: Kluwer Academic Publisher, 1990. 324 p.

15. Хьюбер Дж. П. Робастность в статистике : пер. с англ. Москва : Мир, 1984. 304 с.

16. Быстрые алгоритмы в цифровой обработке изображений / Т. С. Хуанг, Дж.-О. Эклунд, Г. Дж. Нуссбаумер и др. ; под ред. Т. С. Хуанга : пер. с англ. Москва : Радио и связь, 1984. 224 с.

17. Astola J., Heinonen P., Neuvo Y. Liner Median Hybrid Filters // ISCAS'86: Proc. of the IEEE Int. Symp. Circuits and Systems, May 5-7, 1986. San Jose, California (USA), 1986. P. 357–360.

18. Heinonen P., Neuvo Y. FIR Median Hybrid Filter // Proc. of the IEEE Trans. Acoust. Speech and Signal Processing. 1987. Vol. ASSP–35, No. 6. P. 832–838.

19. Nieminen A., Heinonen P., Neuvo Y. A New Class of Detail-Preserving Filters for Image Processing // Proc. of the IEEE Trans Pattern Analysis and Machine Intelligens. 1987. Vol. PAMI-9. P. 74–90.

20. Heinonen P., Neuvo Y. Median type filters with predictive FIR substructures // Proc. of the IEEE Trans. Acoust. Speech and Signal Process. 1988. Vol. 36, No. 6. P. 892–899.

21. Wichman R., Astola J., Heinonen P., Neuvo Y. FIR-Median Hybrid Filter with Excellent Transient Response in Noisy Conditions // Proc. of the IEEE Transactions on Acoustics, Speech and Signal Processing. 1990. Vol. 38, No. 12. P. 2108–2116.

22. Neejarvi J., Varri A., Fotopouls S., Neuvo Y. Weighted FMH filters // Signal Processing. 1993. Vol. 31. P. 181–190.

23. Gonzalez J. G., Paredes J. L., Arce G. R. Zero-Order Statistics: A Mathematical Framework for the Processing and Characterization of Very Impulsive Signals // IEEE Transactions on Signal Processing. 2006. Vol. 54, No. 10. P. 3839–3851. https://doi.org/10.1109/TSP.2006.880306

24. Carrillo R. E., Aysal T. C., Barner K. E. A Generalized Cauchy Distribution Framework for Problems Requiring Robust Behavior // EURASIP Journal on Advances in Signal Processing. 2010. Vol. 2010. 19 p. https://doi.org/10.1155/2010/312989

25. Kalluri S., Arce G. R. Adaptive weighted myriad filter algorithms for robust signal processing in α-stable noise environments // IEEE Trans. Signal Process. 1998. Vol. 46. P. 322–334. https://doi.org/10.1109/78.655418

26. Gonzalez J. G., Arce G. R. Optimality of the myriad filter in practical impulsive-noise environments // IEEE Transactions on Signal Processing. 2001. Vol. 49, No. 2. P. 438–441. https://doi.org/10.1109/78.902126

27. Gonzalez J. G., Arce G. R. Statistically-efficient filtering in impulsive environments: weighted myriad filters // EURASIP J. Adv. Signal Process. 2002. No. 363195 P. 4–20. https://doi.org/10.1155/S1110865702000483

28. Абрамов С. К. Алгоритм реализации мириадной фильтрации // Авиационно-космическая техника и технология. 2000. № 21. С. 143–147.

29. Тулякова Н. О., Трофимчук А. Н., Стрижак А. Е. Алгоритмы мириадной фильтрации // Радиоэлектронные и компьютерные системы. 2014. № 4 (68). С. 76–83.

30. Abramov S. K., Lukin V. V., Astola J. Adaptive myriad filter // CD-ROM Proc. of NSIP'2001. Baltimore (USA), 2001. 5 p.

31. Тулякова Н. О. Локально-адаптивные мириадные фильтры // Радиотехника. 2014. № 179. С. 50–59.

32. Тулякова Н. О., Трофимчук А. Н., Будник Н. Н., Стрижак А. Е. Сравнительный анализ локально-адаптивных нелинейных фильтров для комплексной модели одномерного сигнала // Радиоэлектронные и компьютерные системы. 2015. № 2 (72). С. 97–111.

33. Тулякова Н. О., Лопаткин Р. Ю., Трофимчук А. Н., Стрижак А. Е. Применение локально-адаптивной мириадной фильтрации для комплексной модели одномерного сигнала // Радиоэлектронные и компьютерные системы. 2017. № 3 (83). С. 14–25.

34. Tulyakova N., Neycheva T., Trofymchuk O., Stryzhak O. Locally-adaptive myriad filtration of one-dimensional complex signal // International Journal Bioaotomation. 2018. Vol 22 (3). P. 273–294. https://doi.org/10.7546/ijba.2018.22.3.275-296

35. Тулякова Н. О., Трофимчук А. Н., Стрижак А. Е. Модифицированные локально-адаптивные мириадные фильтры // Радиотехника. 2019. № 196. С. 77–88.

36. Тулякова Н. О., Трофимчук А. Н., Будник Н. Н., Стрижак А. Е. Применение локально-адаптивной устойчивой фильтрации для повышения точности оценок экстремумов различного типа // Радиотехника. 2015. № 183. С. 59–67.

37. Pander T. An application of weighted myriad filter to suppression an impulsive type of noise in biomedical signals // TASK Quartarly. 2004. Vol. 2, No. 8. P. 199–216.

38. Pander T. Impulsive noise filtering in biomedical signals with application of new myriad filter // BIOSIGNAL' 2010: Proc. of the Int. Conf. 2010. Vol. 20. P. 94–101.

39. Pander T. The class of M-filters in the application of ECG signal processing // Biocybernetics and Biomedical Engineering. 2006. Vol. 26, No. 4. P. 3 – 13.

40. Тулякова Н. О. Локально-адаптивная мириадная фильтрация сигнала электрокардиограммы // Радиотехника. 2015. Вып. 180. С. 152–162.

41. Тулякова Н. О., Трофимчук А. Н., Стрижак А. Е. Алгоритмы фильтрации электрокардиограммы с динамически изменяемым размером окна // Радиоэлектронные и компьютерные системы. 2016. № 2 (76). С. 4–14.

42. Тулякова Н. О., Трофимчук А. Н., Стрижак А. Е. Адаптивные мириадные фильтры для обработки сигналов электрокардиограммы, регистрируемых с высокой частотой дискретизации // Радиоэлектронные и компьютерные системы. 2016. № 4 (78). С. 97–107.

43. Tulyakova N., Trofimchuk A., Strizhak A. Adaptive algorithms for elimination of electromyographic noise in the electrocardiogram signal // Telecommunications and Radio Engineering. 2018. Vol. 77, No. 6. P. 549–561. https://doi.org/10.1615/TelecomRadEng.v77.i6.70

44. Tulyakova N. Locally-Adaptive Myriad Filters for Processing ECG Signals in Real Time // International Journal Bioautomation. 2017. Vol. 21 (1). P. 5–18.

45. Тулякова Н. О., Трофимчук А. Н., Стрижак А. Е. Адаптивный метод с шумо- и сигнально-зависимым переключением фильтров для подавления нестационарного шума в сигнале электрокардиограммы в реальном времени // Радиотехника. 2018. № 194. С. 79–96.

46. Neejarvi J., Neuvo Y., Varri A., Mitra U. Algorithms for real-time trend detection // Signal Processing. 1989. Vol. 18. P. 1–15.

47. Varri A., Neejarvi J., Neuvo Y. A new class of filters to remove artifacts from physiologicals signals // EUSIPCO'92: Proc. of the 6th European Signal Processing Conf. Bruxelles (Belgium), 1992. P. 1741–1744.

48. Neejarvi J., Fotopoulos S., Neuvo Y. A new class of sinusoidal-preserving FMH filters // IEEE International Sympoisum on Circuits and Systems. Singapore, 1991. Vol. 1. P. 220–223. https://doi.org/10.1109/ISCAS.1991.176313

49. Yang R., Yin L., Gabbouj M., Astola J., Neuvo Y. Optimal Weighted Median Filtering Under Structural Constraints // Proc. of the IEEE Trans. on Signal Processing. 1995. Vol. 43, No. 3. P. 591–604.

50. Yuriy S. S., Yrjö N., Sanowar K. Review of Unbiased FIR Filters, Smoothers, and Predictors for Polynomial Signals // Frontiers in Signal Processing, 2018. Vol. 2, No. 1. https://dx.doi.org/10.22606/fsp.2018.21001

51. Лукин В. В., Тулякова Н. О., Дорощук М. О. Анализ свойств алгоритмов нелинейной фильтрации одномерных информационных сигналов // Авиационно-космическая техника и технология. 1999. №. 12. С. 109–113.

52. Тулякова Н. О. Применение нелинейной фильтрации для повышения точности измерения координат экстремумов // Радиоэлектронные и компьютерные системы. 2007. № 2 (21). С. 82–89.

53. Бых А. И., Тулякова Н. О. Методы локально-адаптивной устойчивой фильтрации с линейными субапертурами с конечной импульсной характеристикой // Радиоэлектронные и компьютерные системы. 2012. № 2 (54). С. 25–34.

54. Колодяжный В. М., Тулякова Н. О. Применение взвешенного гибридного медианного фильтра с линейными субапертурами с конечной импульсной характеристикой для удаления артефактов в энцефалограммах // Радиоэлектронные и компьютерные системы. 2010. № 3. С. 87–91.

55. Тулякова Н. О. Применение "Растущего на месте" КИХ-гибридного медианного фильтра для удаления нелинейного тренда ЭКГ // Радиоэлектронные и компьютерные системы. 2009. № 3. С. 73–77.

Поступила в редколлегию 27.08.2021

Сведения об авторах:

Тулякова Наталия Олеговна – канд.техн. наук, Институт прикладной физики НАНУ, научный сотрудник, Украина; e-mail: natashatu@ukr.net; nataliyatulyakova@gmail.com; ORCID: https://orcid.org/0000-0002-9158-8967

Трофимчук Александр Николаевич – д-р техн. наук, проф., член-кор. НАНУ, Институт телекоммуникаций и глобального информационного пространства НАНУ, директор, Украина; e-mail: itgis@nas.gov.ua; ORCID: https://orcid.org/0000-0003-3358-6274

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТЕХНОЛОГІЇ

УДК 004.45:004.057.02 **DOI:10.30837/rt.2021.3.206.14**

О.В. ЗАПОРОЖЕЦ, канд. техн. наук, Н.В. ШТЕФАН, канд. техн. наук

ИЗМЕРЕНИЕ КАЧЕСТВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ МЕЖДУНАРОДНЫХ СТАНДАРТОВ

Введение

Компьютерные системы стали неотъемлемой частью жизнеобеспечения современного человека. Последствия от использования некачественного программного обеспечения могут быть катастрофическими, начиная от техногенных аварий, материальных потерь и опасности для человека и заканчивая имидж-потерями компании-разработчика.

Под качеством программного обеспечения понимается способность программного продукта удовлетворять установленным или предполагаемым потребностям [1]. Поэтому важным является обеспечение взаимопонимания между разработчиками и пользователями. Инженеры должны четко понимать смысл, вкладываемый в концепцию качества, характеристики и значение качества в отношении разрабатываемого или сопровождаемого программного обеспечения. Формулирование четких и понятных требований к качеству программного обеспечения, а затем его количественное оценивание – одна из приоритетных задач обеспечения качества программного обеспечения.

Основой обеспечения качества являются измерения. Они – основной инструмент управления жизненным циклом программных продуктов, оценки выполнения планов и мониторинга. Для количественного определения качества необходимо измерить характеристики программного обеспечения.

Стандартизация обеспечивает унификацию требований к качеству, его измерению и оценке. Использование стандартов дает множество потенциальных преимуществ для любой организации, особенно в таких ключевых областях, как измерение качества программных продуктов, информационных и измерительных систем.

Таким образом, уместно проанализировать требования и рекомендации международных стандартов как основу для формирования требований к качеству программного обеспечения и измерения качества программного обеспечения, что снизит риски при разработке, внедрении и сопровождении программного обеспечения. Актуальность этого вопроса подтверждается еще и тем, что данные стандарты приняты в Украине как национальные.

Первые международные стандарты в этой области были приняты еще в 1991 г. и с тех пор несколько раз пересматривались. Сегодня существует серия стандартов ISO 25000 SQuaRE – Systems and software Quality Requirements and Evaluation – логически организованная и унифицированная серия, охватывающая два основных процесса: спецификация требований к качеству программного обеспечения и оценка качества программного обеспечения, поддерживаемая процессом измерения качества [2].

Модель качества SQuaRE

Стандарты SQuaRE включают пять основных разделов [1]: требования к качеству 2503n, модель качества 2501n, измерение качества 2502n, оценка качества 2504n и управление качеством 2500n, а также раздел расширения 25050 – 25099.

По содержанию стандарты ISO/IEC/IEEE 25000 SQuaRE гармонизированы с ISO/IEC/IEEE 15939 [3], который определяет общий процесс и основу для измерения систем и программного обеспечения, а также соответствующую терминологию с инженерной точки зрения. Следуя современным тенденциям ISO по гармонизации терминологии, стандарт ISO/IEC/IEEE 15939 принимает и адаптирует метрологическую терминологию, установленную VIM [4] для стандартов, связанных с программной и системной инженерией. Следующие понятия из ISO/IEC/IEEE 15939 полностью соответствуют, адаптированы или основаны на определениях из VIM: базовая мера – основана на определении «базового значения»; про-

изводная мера – адаптирована из определения «производного значения»; измерение – адаптировано; метод измерения – на основе определения «метода измерения»; процедура измерения – полностью соответствует; шкала – исходя из определения «шкалы»; единица измерения – полностью соответствует.

Стандарты SQuaRE определяют модели качества программного обеспечения и систем, используемые для определения требований, разработки показателей и измерения качества. Модель качества – это совокупность классов характеристик. Характеристики можно разделить на подхарактеристики и, в некоторых случаях, на подподхарактеристики. Измеряемые свойства, связанные с качеством, называются свойствами качества. Свойства качества связаны с соответствующими показателями качества.

Качество в стандартах SQuaRE описывается четырьмя моделями: модель качества при использовании и модель качества продукта, определенная ISO/IEC 25010, модель качества IT-сервисов ISO/IEC 25011, а также модель качества данных, определенная ISO/IEC 25012.

Модель качества продукта сводит качественные характеристики к восьми характеристикам, каждая характеристика, в свою очередь, состоит из ряда соответствующих подхарактеристик (рис. 1) [5].

Эта модель качества продукта дополняется моделью качества при использовании, которая характеризует влияние продукта (системы или программного продукта) на заинтересованные стороны. Качество при использовании определяется качеством программного обеспечения, оборудования, операционной среды, а также характеристиками пользователей, задач и социальной среды. Модель качества при использовании определяется через пять характеристик, связанных с результатами взаимодействия с системой (рис. 2) [5].

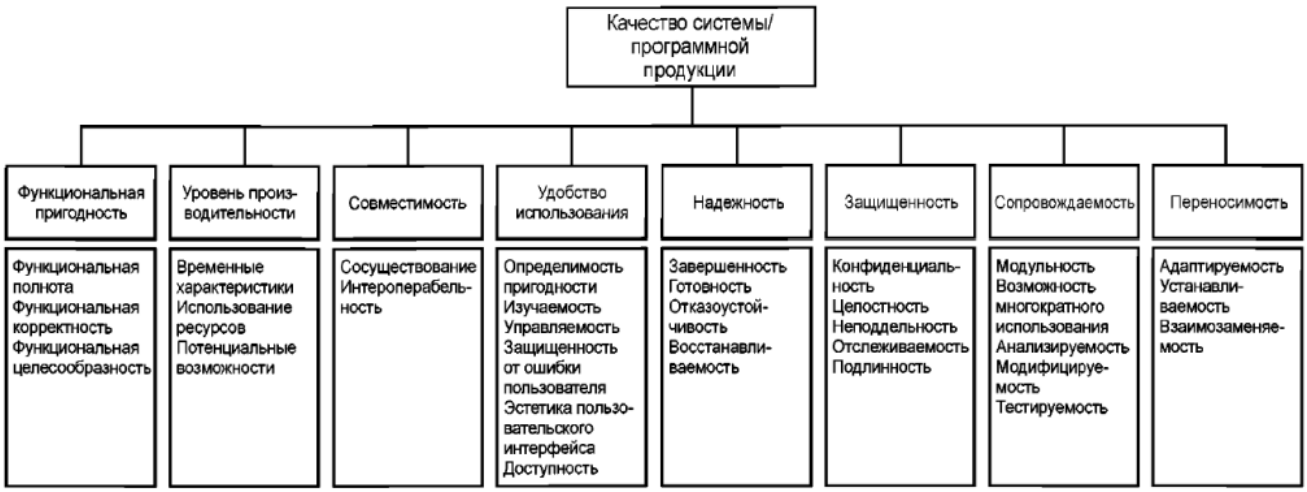


Рис. 1. Модель качества продукта

Рис. 2. Модель качества при использовании

Модели качества продукции и качества при использовании могут быть использованы для определения требований, выработки показателей и выполнения оценки качества. Определенные характеристики качества могут использоваться в качестве контрольного списка для обеспечения детального исследования требований к качеству, обеспечивая таким образом основу для оценки необходимых в процессе разработки систем последующих трудозатрат и действий.

Раздел измерения качества SQuaRE

Раздел измерения качества (2502n) включает стандарты:

– ДСТУ ISO/IEC 25020 – Структура измерения качества: обеспечивает основу для проведения измерения качества;

– ДСТУ ISO/IEC 25021 – Элементы показателя качества: предоставляет формат для определения ЭПК (элементов показателя качества) и несколько примеров ЭПК, которые можно использовать для построения показателей качества программного обеспечения.;

– ISO/IEC 25022 – Измерение качества при использовании: предоставляет показатели, включая связанные функции измерения характеристик качества в модели качества при использовании;

– ДСТУ ISO/IEC 25023 – Измерение качества систем и программных продуктов: предоставляет показатели, включая связанные функции измерения и ЭПК для характеристик качества в модели качества продукта;

– ДСТУ ISO/IEC 25024 – Измерение качества данных: предоставляет показатели, включая связанные функции измерения и ЭПК для характеристик качества в модели качества данных;

– ДСТУ ISO/IEC 25025 – Измерение качества IT-сервисов: предоставляет показатели для модели качества IT-сервисов.

Практическое использование модели измерения качества SQuaRE

Основу для разработки показателей качества обеспечивает стандарт ISO/IEC 25020 [6]. Эталонная модель измерения качества описывает взаимосвязь между моделью качества и построением показателей качества на основе элементов показателей качества (рис. 3).

Свойства качества измеряются с помощью метода измерения. Метод измерения – это логическая последовательность операций, используемая для количественной оценки свойств относительно определенной шкалы. Результатом применения метода измерения являются элементы показателя качества. Характеристики и подхарактеристики качества можно количественно оценить с помощью функции измерения. Функция измерения – это алгоритм, используемый для объединения элементов показателя качества. Показатели качества создаются путем применения функции измерения к набору элементов показателя качества. Результат использования функции измерения называется показателем качества программного обеспечения. Таким образом, показатели качества программного обеспечения становятся количественными индикаторами характеристик и подхарактеристик качества. Для измерения характеристики или подхарактеристики качества можно использовать несколько показателей качества программного обеспечения.

ISO/IEC 25022 [7], ISO/IEC 25023 [8], ISO/IEC 25024 [9] предоставляют набор показателей качества для характеристик систем/программных продуктов в моделях качества при использовании и качества продукта, определенных ISO/IEC 25010, и в модели качества данных, определенной ISO/IEC 25012. Эти показатели качества могут использоваться для определения требований, измерения и оценки качества системы/программного продукта. Исходя из задачи измерения показатели качества выбираются из стандартов ISO/IEC 25022, ISO/IEC 25023, ISO/IEC 25024 для удовлетворения потребностей разработчиков, приобретателей, менеджеров, прямых и косвенных пользователей и других заинтересованных сторон. Кроме того, включаются функции измерения для каждого предлагаемого показателя качества, краткое

рассмотрение использования показателей качества и элементов показателя качества. Элементы показателя качества представлены в ISO/IEC 25021 [10].

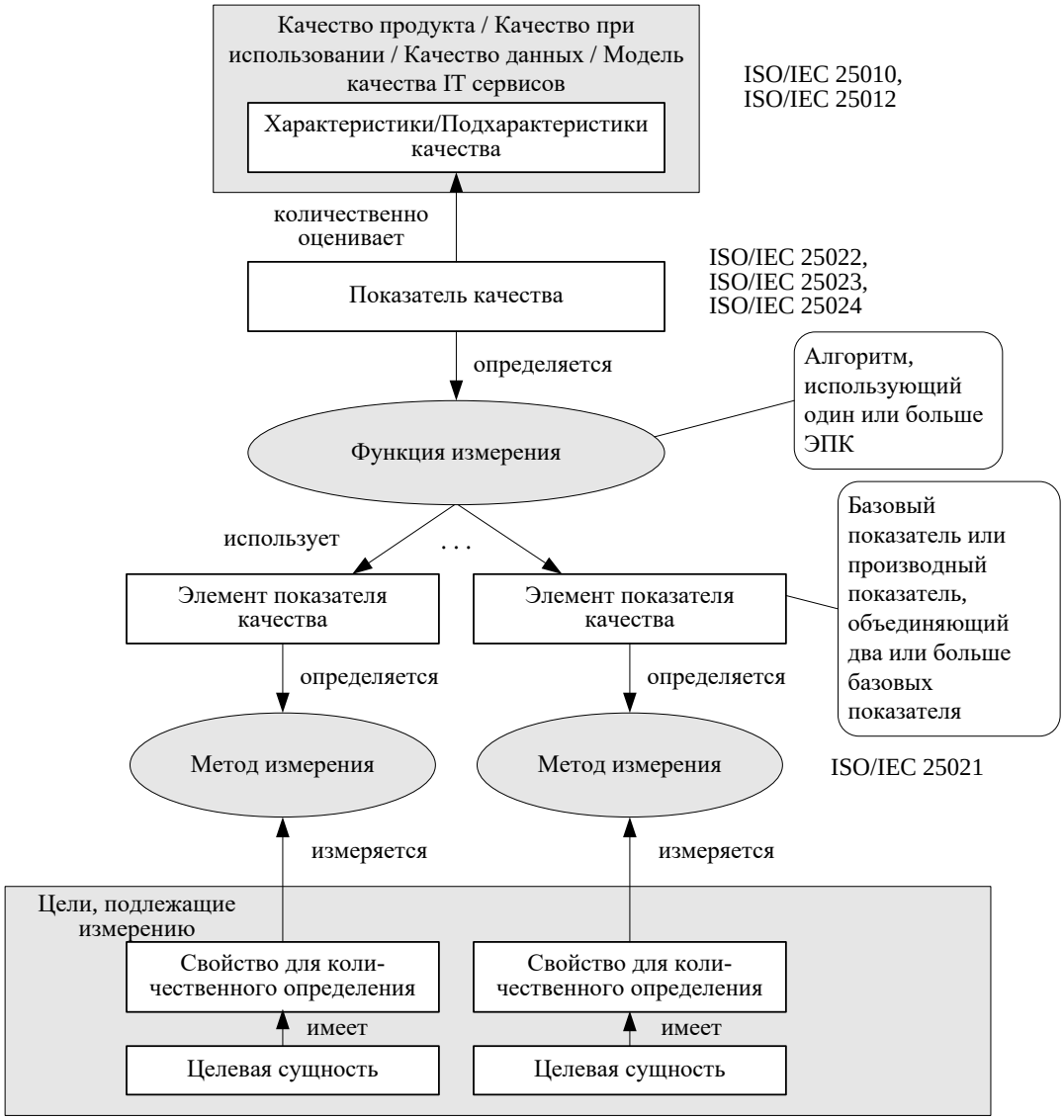


Рис. 3. Взаимосвязь между моделью качества, показателями качества, элементами показателей качества, свойствами для количественного определения, целевыми сущностями

На основе анализа разделов модели качества и измерения качества SQuaRE предлагается алгоритм измерения качества программного обеспечения:

1) определить модели качества по ISO/IEC 25010, ISO/IEC 25012 для идентификации соответствующих характеристик качества программного обеспечения;

2) выбрать показатели качества для каждой характеристики качества, используя ISO/IEC 25022, ISO/IEC 25023, ISO/IEC 25024.

3) используя методы измерения из ISO/IEC 25021 измерить элементы показателя качества;

4) выбранные показатели качества определяются путем применения функции измерения к элементам показателя качества.

В таблице показаны примеры применения стандартов SQuaRE для измерения качества программного обеспечения.

Примеры применения стандартов SQuaRE для измерения качества программного обеспечения

Характеристики/ подхарактеристики качества	Показатель качества. Описание	Функция измерения	Элемент показателя качества	Метод измерения
Функциональная полнота	Функциональное покрытие. Какая часть указанных функций реализована?	$X = 1 - A/B$, A – количество отсутствующих функций, B – количество предусмотренных функций	Количество доступных функций	Просмотр и анализ отдельных функций системы / программного обеспечения, доступных пользователю с ограниченными возможностями для вызова и выполнения, и подсчет количества функций, которые не удалось успешно использовать
Временные характеристики	Среднее время ответа. Сколько в среднем времени требуется системе, чтобы ответить на пользовательскую задачу или системную задачу?	$X = \sum_{i=1}^{n} A_i \Big/ n$, A_i – время, затраченное системой на ответ на конкретную задачу пользователя или системную задачу при i-м измерении, n – количество измеренных ответов	Продолжительность	Продолжительность зависит от общего количества времени и привязана к Международной системе единиц (VIM)

Выводы

1. Раздел «Модели качества» 2501n стандартов SQuaRE описывает модели качества программного обеспечения, которые поддерживают четкое определение требований к качеству программного обеспечения. Характеристики в модели качества при использовании и модели качества продукта предназначены для использования в качестве набора при спецификации или оценке качества программного продукта или компьютерной системы.

2. Измерение качества программного обеспечения основано на двух понятиях: показатель качества и элемент показателя качества. Эталонную модель измерения качества описывает стандарт ISO/IEC 25020.

3. Стандарты ISO/IEC 25022, ISO/IEC 25023, ISO/IEC 25024 для каждой характеристики качества модели определяют показатели качества и функцию измерения.

4. Функция измерения связывает показатели качества с элементами показателя качества, который непосредственно измеряется. Широкий перечень элементов показателей качества содержит стандарт ISO/IEC 25021.

5. Основные преимущества серии стандартов SQuaRE заключаются в том, что они предоставляют методики координации для измерения и оценки качества программных продуктов, руководство по спецификациям требований к качеству программного обеспечения продукта и гармонизацию со стандартом ISO/IEC 15939 в форме эталонной модели измерения качества.

Список литературы:

1. ДСТУ ISO/IEC 25000:2016 Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE). Настанова до SQuaRE (ISO/IEC 25000:2014, IDT).

2. Kazuhiro Esaki. Introduction of Quality Requirement and Evaluation Based on ISO/IEC SQuaRE Series of Standard. // Global Perspectives on Engineering Management. May 2013, Vol. 2 Iss. 2, pp. 52-59.

3. ДСТУ ISO/IEC/IEEE 15939:2018 Інженерія систем і програмних засобів. Процес вимірювання (ISO/IEC/IEEE 15939:2017, IDT).

4. JCGM 200:2012. International vocabulary of metrology – Basic and general concepts and associated terms (VIM).

5. ДСТУ ISO/IEC 25010:2016 Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE). Моделі якості системи та програмних засобів (ISO/IEC 25010:2011, IDT).

6. ДСТУ ISO/IEC 25020:2016 Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE). Рамкова модель і настанова щодо вимірювання (ISO/IEC 25020:2007, IDT).

7. ДСТУ ISO/IEC 25022:2019 Інженерія систем і програмних засобів. Вимоги до якості систем програмних засобів та їхнього оцінювання (SQuaRE). Вимірювання якості під час застосування (ISO/IEC 25022:2016, IDT).

8. ДСТУ ISO/IEC 25023:2019 Інженерія систем і програмних засобів. Вимоги до якості систем програмних засобів та їхнього оцінювання (SQuaRE). Вимірювання якості систем та програмних продуктів (ISO/IEC 25023:2016, IDT).

9. ISO/IEC 25024:2015 Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of data quality.

10. ДСТУ ISO/IEC 25021:2016 ДСТУ ISO/IEC 25021:2016 Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE). Елементи показника якості (ISO/IEC 25021:2012, IDT).

17.09.2021

Сведения об авторах:

Запорожец Олег Васильевич – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, доцент кафедры информационно-измерительных технологий, Украина; e-mail: oleg.zaporozhets@nure.ua; ORCID: https://orcid.org/0000-0002-7831-8479

Штефан Наталья Владимировна – канд. техн. наук, доцент, Харьковский национальный университет радиоэлектроники, доцент кафедры информационно-измерительных технологий, Украина; e-mail: natalya.shtefan@nure.ua; ORCID: https://orcid.org/0000-0001-7926-8437

РЕФЕРАТИ РЕФЕРАТЫ ABSTRACTS

МОДЕЛІ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

МОДЕЛИ, МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ

MODELS, METHODS AND MEANS OF PROTECTING INFORMATION IN INFORMATION AND COMMUNICATION SYSTEMS

УДК 681.3.06

Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки / *О.В. Потій, Ю.І. Горбенко, О.А. Замула, К.В. Ісірова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 206. С. 5 – 24.

Світові тенденції до посилення загроз інформаційної та кібербезпеки, підвищення рівня вразливості інформаційно-телекомунікаційних систем (ІТС) обумовлюють необхідність розробки та впровадження нових стандартів та нормативних документів з інформаційної безпеки, що впроваджують нові технології та передовий практичний досвід із захисту інформації. Основним підходом до забезпечення кібер- і інформаційної безпеки в ІТС є стратегія захисту на основі ризику (Risk-Based Protection Strategy). Основне завдання управління інформаційними ризиками (ІР) – об'єктивно ідентифікувати і оцінити найбільш значущі для бізнесу компанії риски, а також необхідність використання засобів контролю ризиків для збільшення ефективності і рентабельності економічної діяльності компанії. Вважається, що якісне управління ризиками дозволяє використовувати оптимальні за ефективністю і витратам засоби контролю ризиків і заходи захисту інформації, що адекватні поточним цілям і завданням бізнесу компанії. У роботі наведено результати вирішення актуальної проблеми пошуку оптимальних методів оцінки ризиків інформаційної та кібербезпеки. Запропоновано критерії відбору найкращих методів оцінки ризиків. Проведено аналіз відомих методів оцінки ризиків на відповідність даним критеріям. Сформульовано пропозиції щодо створення перспективних методів оцінки ризиків, застосування яких у сучасних системах управління інформаційною безпекою, особливо тих, які створені для об’єктів критичної інфраструктури, дозволить найбільш ефективно вирішувати задачі забезпечення інформаційної і кібербезпеки, а також приватності.

Ключові слова: ризик; кібер- і інформаційна безпека; оцінка ризику; управління ризиками; система управління інформаційною безпекою; обробка ризиків; заходи безпеки; методи оцінки ризику.

Табл. 4. Іл. 6. Бібліогр.: 13 назв.

УДК 681.3.06

Анализ методов оценки и управления рисками кибер- и информационной безопасности / *А.В. Потий, Ю.И. Горбенко, А.А. Замула, Е.В. Исирова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 206. С. 5 – 24.

Мировые тенденции к усилению угроз информационной и кибербезопасности, повышение уровня уязвимости информационно-телекоммуникационных систем (ИТС) обусловливают необходимость разработки и внедрения новых стандартов и нормативных документов по информационной безопасности, внедрения новых технологий и передового практического опыта по защите информации. Основным подходом к обеспечению информационной и кибербезопасности в ИТС является стратегия защиты на основе риска (Risk-Based Protection Strategy). Основная задача управления информационными рисками (ИР) – объективно идентифицировать и оценить наиболее значимые для бизнеса компании риски, а также необходимость использования средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности компании. Считается, что качественное управление рисками позволяет использовать оптимальные по эффективности и затратам средства контроля рисков и меры по защите информации, адекватные текущим целям и задачам бизнеса компании. В работе приводены результаты решения актуальной проблемы поиска оптимальных методов оценки рисков информационной и кибербезопасности. Предложены критерии отбора лучших методов оценки рисков. Проведен анализ известных методов оценки рисков на соответствие данным критериям. Сформулированы предложения по созданию перспективных методов оценки рисков, применение которых в современных системах управления информационной безопасностью, особенно тех, которые предназначены для объектов критической инфраструктуры, позволит наиболее эффективно решать задачи обеспечения информационной и кибербезопасности, а также приватности.

Ключевые слова: риск; кибер- и информационная безопасность; оценка риска; управление рисками; система управления информационной безопасностью; обработка рисков; меры безопасности; методы оценки риска.

Табл. 4. Ил. 6. Библиогр.: 13 назв.

UDC 681.3.06

Analysis of methods for assessing and managing cyber risks and information security / *O. Potii, Y. Gorbenko, O. Zamula, K. Isirova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №206. P. 5 – 24.

Global trends to increase the threats to information and cybersecurity, increasing the level of vulnerability of information and telecommunications systems (ITS) necessitate the development and implementation of new standards and regulations on information security, the introduction of new technologies and best practices in information security. The main approach to information and cybersecurity in ITS is the Risk-Based Protection Strategy. The main task of information risk management (IR) is to identify and assess objectively the most significant risks for the company's business, as well as the need to use risk controls to increase the efficiency and profitability of the company's economic activities. It is believed that quality risk management allows you to use the optimal efficiency and cost of risk control and information protection measures, adequate to the current goals and objectives of the company's business. The paper presents results of solving the current problem of finding optimal methods for assessing the risks of information and cybersecurity. Criteria for selecting the best methods of risk assessment are proposed. The analysis of known methods of risk assessment for compliance with these criteria is performed. Proposals have been formulated to create promising methods for risk assessment, their application to modern information security management systems, especially those designed for critical infrastructure, will most effectively address the problems of information and cybersecurity, as well as privacy.

Key words: risk; cyber and information security; risk assessment; risk management; information security management system; risk processing; security measures; risk assessment methods.

4 tab. 6 fig. Ref: 13 items.

УДК 621.391

Теоретичні підходи до синтезу дискретних сигналів з необхідними властивостями / *І.Д. Горбенко, О.А. Замула* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 206. С. 25 – 32.

Використовувані в інформаційно-комунікаційних системах (ІКС) методи обміну інформацією, формування і обробки даних, а також класи широкосмугових сигналів, що застосовуються в якості фізичного носія даних, не дозволяють забезпечити необхідні (для окремих додатків ІКС) показники кібер- і інформаційної безпеки, завадостійкості прийому сигналів і скритності функціонування ІКС. Більшість існуючих систем використовують сигнали, побудова яких заснована на лінійних законах, що дозволяє зловмисникові на основі встановлення параметрів сигналів, які використовуються в системі, здійснити (з мінімальними витратами енергії) навмисне втручання в роботу ІКС. У статті представлено концептуальні підходи до побудови захищених ІКС, що визначають необхідність охоплення всього спектра перетворень інформації в комплексі і засновані на синтезі систем сигналів з поліпшеними ансамблевими, кореляційними, структурними властивостями. Запропоновано метод синтезу дискретних похідних сигналів на основі нелінійних дискретних складних криптографічних сигналів (КС) і ортогональних сигналів, які утворені на основі рядків матриці Адамара (вихідні сигнали). На основі комп'ютерного моделювання та проведених розрахунків показано, що похідні сигнали, утворені на основі криптографічних послідовностей і рядків матриці Адамара, мають поліпшені, в порівнянні з ортогональними і лінійними класами сигналів, властивості. Викладено підходи до побудови і дано загальну характеристику програмно-апаратного комплексу для синтезу, аналізу, дослідження властивостей, генерації, обробки ряду досліджуваних класів сигналів. Показано, що застосування таких сигналів дозволить поліпшити такі показники функціонування системи, як інформаційна безпека, завадостійкість прийому сигналів і скритності функціонування.

Ключові слова: завадостійкість прийому; скритність; інформаційна безпека; дискретні послідовності; складні сигнали; синтез сигналів; кореляційна функція; похідні системи сигналів; ортогональні сигнали.

Табл. 8. Бібліогр.: 11 назв.

УДК 621.391

Теоретические подходы к синтезу дискретных сигналов с необходимыми свойствами / *И.Д. Горбенко, А.А. Замула* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 206. С. 25 – 32.

Используемые в информационно-коммуникационных системах (ИКС) методы обмена информацией, формирования и обработки данных, а также классы широкополосных сигналов, применяемые в качестве физического носителя данных, не позволяют обеспечить необходимые (для отдельных приложений ИКС) показатели кибер – и информационной безопасности, помехоустойчивости приема сигналов и скрытности функционирования ИКС. Большинство существующих систем используют сигналы, построение которых основано на линейных законах, что позволяет злоумышленнику на основе установления параметров сигналов, используемых в системе, осуществить (с минимальными затратами энергии) преднамеренное вмешательство в работу ИКС. В статье представлены концептуальные подходы к построению защищенных ИКС, определяющие необходимость охвата всего спектра преобразований информации в комплексе и основанные на синтезе систем сигналов с улучшенными ансамблевыми, корреляционными, структурными свойствами. Предложен метод синтеза дискретных производных сигналов на основе нелинейных дискретных сложных криптографических сигналов (КС), и ортогональных сигналов, которые образованы на основе строк матрицы Адамара (исходные сигналы). На основе компьютерного моделирования и проведенных расчетов показано, что производные сигналы, образованные на основе криптографических последовательностей и строк матрицы Адамара обладают улучшенными, по

сравнению с ортогональными и линейными классами сигналов, свойствами. Изложены подходы к построению и дана общая характеристика программно-аппаратного комплекса для синтеза, анализа, исследования свойств, генерации, обработки ряда исследуемых классов сигналов. Показано, что применение таких сигналов позволит улучшить такие показатели функционирования системы, как информационная безопасность, помехоустойчивость приема сигналов и скрытности функционирования.

Ключевые слова: помехоустойчивость приема; скрытность; информационная безопасность; дискретные последовательности; сложные сигналы; синтез сигналов; корреляционная функция; производные сигналы; ортогональные сигналы.

Табл. 8. Библиогр.: 11 назв.

UDC 621.391

Theoretical approaches to the synthesis of discrete signals with necessary properties / *I.D. Gorbenko, A.A. Zamula* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. № 206. P. 25 – 32.

Methods for information exchange, formation and processing of data used in information and communication systems (ICS), as well as classes of broadband signals used as a physical data carrier, do not provide the necessary (for individual ICS applications) indicators of cyber and information security, noise immunity of reception signals and secrecy of IKS functioning. Most of the existing systems use signals, the construction of which is based on linear laws, which allows an attacker, based on the establishment of the parameters of the signals used in the system, to carry out deliberate interference in the operation of the ICS with minimal energy consumption. The article presents conceptual approaches to the construction of secure ICS, which determine the need to cover the entire spectrum of information transformations in the complex, and based on the synthesis of signal systems with improved ensemble, correlation, structural properties. A method is proposed for synthesizing discrete derivatives of signals based on nonlinear discrete complex cryptographic signals (CS) and orthogonal signals formed on the basis of the rows of the Hadamard matrix (initial signals),. Based on computer modeling and the performed calculations, it is shown that the derivative signals formed on the basis of cryptographic sequences and rows of the Hadamard matrix have improved properties compared to orthogonal and linear classes of signals. Approaches to the construction are stated and a general characteristic of the hardware-software complex for synthesis, analysis, study of properties, generation, processing of a number of studied signal classes is given. It is shown that the use of such signals will improve such indicators of the system functioning as information security, noise immunity of signal reception and secrecy of functioning.

Key words: reception noise immunity; secrecy; Information Security; discrete sequences; complex signals; synthesis of signals; correlation function; derived signals; orthogonal signals.

8 tab. Ref: 11 items.

УДК 621.317.76.089.68+681.3.07 (3.06)

Постановка задачі оцінки нестабільності пасивних квантових стандартів частоти при наявності похибки від взаємодії / *О.П. Нарєжній, Т.О. Гріненко, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 206. С. 33 – 44.

Побудова сучасних вимірювальних комплексів системи координатно-часового забезпечення України неможлива без вдосконалення математичних моделей квантових стандартів частоти (КСЧ), що використовуються в групових стандартах. Дана робота присвячена аналізу методів сталого рішення прямих і обернених задач (методів розв'язання некоректних задач) в моделях взаємодії пасивних КСЧ в процесі їх звірень. Пріоритетним завданням є використання цих методів для чисельного рішення задач при проектуванні групових КСЧ і паралельних квантових генераторів випадкових чисел. Методи вирішення подібних завдань затребувані, оскільки дозволяють створювати математичні моделі взаємодії групових КСЧ. Ці моделі дозволять проектувати ефективні паралельні квантові пристрої генерації випадкових чисел для високотехнологічних галузей кібербезпеки.

При оцінці метрологічних параметрів КСЧ, як правило, використовують різновидності методів типу методу найменших квадратів або методу псевдообернеої матриці Мура-Пенроуза. В алгоритмах групових еталонів через нестійкість рішення використовують робасні методи регуляризації або фільтрації, наприклад, метод фільтра Калмана або Вінера. Однак ці методи не працюють при наявності похибки від взаємодії КСЧ в процесі їх функціонування в груповому ідеалі або звіреннях.

Метою роботи є аналіз і обґрунтування постановки задачі оцінки потенційних точністних характеристик пасивних КСЧ при наявності похибки від взаємодії. Параметри регуляризації при визначенні вектора стану групового еталона знаходяться за допомогою сигналів, які передаються глобальними навігаційними супутниковими системами типу GPS\GLONASS в режимі локальної диференціальної корекції.

Ключові слова: атомний годинник; похибка від взаємодії; груповий еталон; квантовий стандарт частоти; шкала часу.

Бібліогр.: 35 назв.

УДК 621.317.76.089.68+681.3.07 (3.06)

Постановка задачи оценки нестабильности пассивных квантовых стандартов частоты при наличии погрешности от взаимодействия / *А.П. Нарежний, Т.А. Гриненко, И.Д. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 206. С. 33 – 44.

Построение современных измерительных комплексов системы координатно-временного обеспечения Украины невозможно без совершенствования математических моделей квантовых стандартов частоты (КСЧ), используемых в групповых эталонах. Данная работа посвящена анализу методов устойчивого решения прямых и обратных задач (методов решения некорректных задач) в моделях взаимодействия пассивных КСЧ в процессе их сличений. Приоритетной задачей является использование этих методов для численного решения задач при проектировании групповых КСЧ и параллельных квантовых генераторов случайных чисел. Методы решения подобных задач востребованы, поскольку позволяют создавать математические модели взаимодействия групповых КСЧ. Эти модели позволят проектировать эффективные параллельные квантовые устройства генерации случайных чисел для высокотехнологичных областей кибербезопасности.

При оценке метрологических параметров КСЧ, как правило, используют разновидности методов типа метода наименьших квадратов или метода псевдообратной матрицы Мура-Пенроуза. В алгоритмах групповых эталонов из-за неустойчивости решения используют робастные методы регуляризации или фильтрации, например, метод фильтра Калмана или Винера. Однако данные методы не работают при наличии погрешности от взаимодействия КСЧ в процессе их функционирования в групповом эталоне или сличениях.

Целью работы является анализ и обоснование постановки задачи оценки потенциальных точностных характеристик пассивных КСЧ при наличии погрешности от взаимодействия. Параметры регуляризации при определении вектора состояния группового эталона находятся с помощью сигналов, передаваемых глобальными навигационными спутниковыми системами типа GPS\GLONASS в режиме локальной дифференциальной коррекции.

Ключевые слова: атомные часы; погрешность от взаимодействия; групповой эталон; квантовый стандарт частоты; шкала времени.

Библиогр.: 35 назв.

UDC 621.317.76.089.68+681.3.07 (3.06)

Statement of the problem of assessing instability of passive quantum frequency standards in the presence of an error from the interaction / *O. P. Nariezhnii, T. O. Grinenko, I. D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №206. P. 33 – 44.

Construction of modern measuring complexes of the coordinate-time support system of Ukraine is impossible without improving mathematical models of quantum standards of frequency (QSF) used in group standards. This work is devoted to the analysis of methods for the stable solution of direct and inverse problems (methods for solving ill-posed problems) in models of the interaction of passive QSF in the process of their comparisons. The priority task is to use these methods for the numerical solution of problems in the design of group QSF and parallel quantum generators of random numbers. Methods for solving such problems are in demand, since they make it possible to create mathematical models of group QSF interaction. These models will enable the design of efficient parallel quantum random number generation devices for high-tech areas of cybersecurity.

Varieties of methods such as the method of least squares or the method of the Moore-Penrose pseudo-inverse matrix are used, as a rule when evaluating the metrological parameters of QSF. Robust methods of regularization or filtering, for example, the Kalman or Wiener filter method, are used in the algorithms of group standards, due to the instability of the solution. However, these methods do not work in the presence of an error from the interaction of QSF in the process of their functioning in a group standard or in comparisons.

The aim of this work is to analyze and substantiate the formulation of the problem of assessing the potential accuracy characteristics of passive QSF in the presence of an error from the interaction. Regularization parameters when determining the state vector of the group standard are found using signals transmitted by global navigation satellite systems such as GPS\GLONASS in the local differential correction mode.

Key words: atomic clocks; error from interaction; group standard; quantum frequency standard; time scale.

Ref: 35 items.

УДК 004.056.5

Дослідження доцільності застосування AVX512 для реалізації сучасних алгоритмів електронних підписів / *І.Д. Горбенко, О.Г. Качко, С.О. Кандій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 206. С. 45 – 52.

Розробка та дослідження електронних підписів на алгебраїчних решітках є одним з перспективних напрямів у постквантовій криптографії. У відкритому конкурсі NIST PQC серед фіналістів представниками криптографії на решітках у категорії електронних підписів є криптосистеми CRYSTALS-Dilithium та Falcon. Більшість операцій у цих криптосистемах зводяться до складання та множення поліномів у скінченному полі з твірним циклотомічним поліномом x^N+1. Використання такого поля дозволяє використовувати теоретико-числове перетворення (NTT) для створення швидких та надійних програмних реалізацій. На практиці для того щоб досягти гарної швидкодії використовуються набори векторизованих (SIMD) інструкцій. Серед існуючих реалізацій найчастіше використовуються AVX2 інструкції. У той же час можливість використання AVX512 інструкцій залишається малодослідженою. Мета роботи – дослідження доцільності використання AVX512 інструкцій для оптимізації NTT, що використовуються у сучасних ЕП на алгебраїчних решітках. Зокрема, наведений метод реалізації теоретико-числового перетворення з використанням AVX512 для ЕП CRYSTALS-

Dilithium та Falcon. Показано збільшення швидкодії порівняно з еталонними оптимізованими авторськими реалізаціями.

Ключові слова: постквантова криптографія; алгебраїчні решітки; CRYSTALS-Dilithium; Falcon, NTT; AVX512.

Табл. 1. Іл. 2. Бібліогр.: 8 назв.

УДК 004.056.5

Исследование целесообразности использования AVX512 для реализации современных алгоритмов электронных подписей / *И.Д. Горбенко, Е.Г. Качко, С.О. Кандий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 206. С. 45 – 52.

Разработка и исследование электронных подписей на алгебраических решетках является одним из перспективных направлений в постквантовой криптографии. В открытом конкурсе NIST PQC среди финалистов представителями криптографии на решетках в категории электронных подписей являются криптосистемы CRYSTALS-Dilithium и Falcon. Большинство операций в этих криптосистемах сводятся к сложению и умножению полиномов в конечном поле с образующим циклотомичним полиномом $x^N + 1$. Использование такого поля позволяет использовать теоретико-числовое преобразование (NTT) для создания быстрых и надежных программных реализаций. На практике для того, чтобы достичь хорошей производительности, используются наборы векторизованных (SIMD) инструкций. Чаще всего используются AVX2 инструкции. В то же время возможность использования AVX512 инструкций остается малоисследованной. Цель работы – исследование целесообразности использования AVX512 инструкций для оптимизации NTT, используемых в современных ЭП на алгебраических решетках. В частности, приведен метод реализации теоретико-числового преобразования с использованием AVX512 для ЭП CRYSTALS-Dilithium и Falcon. Показано увеличение быстродействия по сравнению с эталонными оптимизированными авторскими реализациями.

Ключевые слова: постквантовая криптография; алгебраические решетки; CRYSTALS-Dilithium; Falcon, NTT; AVX512.

Табл. 1. Ил. 2. Библиогр.: 8 назв.

UDC 004.056.5

Investigation of the expediency of using AVX512 for the implementation of modern algorithms for electronic signatures / *I.D. Gorbenko, E.G. Kachko, S.O. Kandii* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №206. P. 45 – 52.

Development and investigation of electronic signatures on algebraic lattices is one of the promising directions in post-quantum cryptography. Cryptosystems CRYSTALS-Dilithium and Falcon represent lattice cryptography in the category of electronic signatures in the NIST PQC open competition among the finalists. Most operations in these cryptosystems are reduced to addition and multiplication of polynomials in a finite field with a generating cyclotomic polynomial $x^N + 1$. Using such a field allows the use of a number-theoretic transformation (NTT) to create fast and reliable software implementations. In practice, vectorized set (SIMD) instructions are used to achieve good performance. AVX2 instructions are most often used among existing implementations. At the same time, the possibility of using AVX512 instructions remains little explored. The purpose of this work is to investigate the feasibility of applying AVX512 instructions to optimization of the NTT, used in modern EPs on algebraic lattices. In particular, the paper presents a method for implementing a number-theoretic transformation using AVX512 for CRYSTALS-Dilithium and Falcon. An increase in performance is shown in comparison with the reference optimized author's implementations.

Key words: postquantum cryptography; algebraic lattice; CRYSTALS-Dilithium; Falcon, NTT; AVX512.

1 tab. 2 fig. Ref: 8 items.

УДК 004.056.5

Дослідження евристичних функцій пошуку нелінійних підстановок для симетричної криптографії / *О.О. Кузнецов, М.О. Полуяненко, В.О.Катрич, С.О. Кандій, Ю.О. Заиченко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 206. С. 53 – 63.

Нелінійні підстановки (S-блоки) застосовуються у більшості сучасних симетричних криптоалгоритмів. Вони призначені для перемішування вхідних даних та відіграють суттєву роль в забезпеченні стійкості проти відомих криптоаналітичних атак (диференційного, лінійного, алгебраїчного та інших методів криптоаналізу). Однак випадкове формування нелінійних підстановок з потрібними показниками є надзвичайно складною математичною задачею. В статті досліджуються евристичні техніки інформованого пошуку S-блоків, зокрема, розглядаються різні функції вартості, що застосовуються в більшості відомих алгоритмах (наприклад, локального пошуку, градієнтного підйому, імітації відпалу, генетичного пошуку, тощо). Метою дослідження є визначення конкретних параметрів евристичних функцій, які з одного боку не знижують ступінь інформованості стосовно вузлів пошуку, а з іншого – не вимагають значних обчислювальних витрат. Досліджується вплив окремих параметрів на значення функції вартості та на складність її обчислення. Також надаються конкретні рекомендації з формування параметрів для евристичного пошуку S-блоків, які суттєво впливають на ефективність генерації нелілійних підстановок для симетричної криптографії.

Ключові слова: евристичні техніки; інформований пошук; нелінійні підстановки; симетрична криптографія.

Табл. 1. Іл. 9. Бібліогр.: 44 назв.

УДК 004.056.5

Исследование эвристических функций поиска нелинейных подстановок для симметричной криптографии / *А.А. Кузнецов, Н.А. Полуяненко, В.А. Катрич, С.О. Кандий, Ю.А. Заиченко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 206. С. 53 – 63.

Нелинейные подстановки (S-блоки) применяются в большинстве современных симметричных криптоалгоритмов. Они предназначены для перемешивания входных данных и имеют существенное значение в обеспечении устойчивости против известных криптоаналитических атак (дифференциального, линейного, алгебраического и других методов криптоанализа). Однако случайное формирование нелинейных подстановок с нужными показателями является чрезвычайно сложной математической задачей. В статье исследуются эвристические техники информированного поиска S-блоков, в частности рассматриваются различные функции стоимости, применяемые в большинстве известных алгоритмов (например, локального поиска, градиентного подъема, имитации отжига, генетического поиска и т.д.). Цель исследования – определение конкретных параметров эвристических функций, которые, с одной стороны, не снижают степень информированности относительно узлов поиска, а с другой – не требуют значительных вычислительных затрат. Исследуется влияние отдельных параметров на значение функции стоимости и сложности ее вычисления. Также предоставляются конкретные рекомендации по формированию параметров для эвристического поиска S-блоков, которые существенно влияют на эффективность генерации нелинейных подстановок для симметричной криптографии.

Ключевые слова: эвристические техники; информированный поиск; нелинейные подстановки; симметричная криптография.

Табл. 1. Ил. 9. Библиогр.: 44 назв.

UDC 004.056.5

Investigation of heuristic search functions for nonlinear substitutions for symmetric cryptography / *A.A. Kuznetsov, N.A. Poluyanenko, V.A. Katrich, S.O. Kandii, Yu.A. Zaichenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №206. P. 53 – 63.

Nonlinear substitutions (S-boxes) are used in most modern symmetric cryptoalgorithms. They are designed to mix input data and play a significant role in ensuring resistance against known cryptanalytic attacks (differential, linear, algebraic and other cryptanalysis methods). However, random generation of nonlinear substitutions with the desired indicators is an extremely difficult mathematical problem. This article explores the heuristic techniques for S-boxes informed search, in particular, discusses various cost functions used in most of the known algorithms (for example, local search, hill climbing, simulated annealing, genetic search, etc.). The aim of the study is to determine the specific parameters of heuristic functions, which, on the one hand, do not reduce the degree of awareness of the search nodes, and on the other hand, do not require significant computational costs. The article examines the influence of individual parameters on the value of the cost function and complexity of its calculation. It also provides specific recommendations for the formation of parameters for heuristic search for S-boxes, which significantly affect the efficiency of generating nonlinear substitutions for symmetric cryptography.

Key words: heuristic techniques; informed search; nonlinear substitutions; symmetric cryptography.

1 tab. 9 fig. Ref: 44 items.

УДК 004.056.5

Оптимізація параметрів алгоритму локального пошуку для генерації нелінійних підстановок / *О.О. Кузнецов, М.О. Полуяненко, С.Л. Бердник, С.О. Кандій, Ю.О. Заиченко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 206. С. 64 – 76.

Важливим компонентом сучасних алгоритмів симетричною криптографії є нелінійні підстановки (S-блоки). Вони ускладнюють симетричні перетворення і вносять нелінійність в співвідношення «вхід-вихід», що забезпечує стійкість алгоритмів до деяких методів криптоаналізу. Генерація S-блоків може виконуватися різними способами. Однак найбільш перспективними є евристичні техніки. З одного боку, генеруються S-блоки, які мають вигляд випадкових постановок, що ускладнює алгебраїчний криптоаналіз. З іншого боку, евристичний пошук дозволяє досягти високих показників нелінійності і δ-рівномірності, що ускладнює лінійний і диференціальний криптоаналіз. В статті досліджується найпростіший алгоритм локального пошуку для генерації S-блоків. Для оцінки ефективності алгоритму вводиться поняття треку функції вартості. Проводяться численні експерименти, зокрема, досліджується вплив числа внутрішніх і зовнішніх циклів локального пошуку на трудомісткість генерації цільового S-блоку. Обгрунтовуються оптимальні (з точки зору мінімальних затрат часу) параметри алгоритму локального пошуку для генерації S-блоків з цільової нелінійністю 104 і кількістю паралельних обчислювальних потоків 30. Показано, що з вибраними (оптимальними) параметрами вдається надійно формувати S-блоки з нелінійністю 104.

Ключові слова: симетрична криптографія; нелінійні підстановки; S-boxes; алгоритм локального пошуку; оптимізація параметрів.

Табл. 1. Іл. 8. Бібліогр.: 32 назв.

УДК 004.056.5

Оптимизация параметров алгоритма локального поиска для генерации нелинейных подстановок / *А.А. Кузнецов, Н.А. Полуяненко, С.Л. Бердник, С.О. Кандий, Ю.А. Заиченко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 206. С. 64 – 76.

Важным компонентом современных алгоритмов симметричной криптографии являются нелинейные подстановки (S-блоки). Они усложняют симметричные преобразования и вносят нелинейность в соотношения «вход-выход», что обеспечивает устойчивость алгоритмов к некоторым методам криптоанализа. Генерация S-блоков может выполняться разными способами. Однако наиболее перспективными являются эвристические техники. С одной стороны, генерируемые S-блоки имеют вид случайных постановок, что усложняет алгебраический криптоанализ. С другой стороны, эвристический поиск позволяет достичь высоких показателей нелинейности и δ-равномерности, что усложняет линейный и дифференциальный криптоанализ. В статье исследуется простейший алгоритм локального поиска для генерации S-блоков. Для оценки эффективности алгоритма вводится понятие трека функции стоимости. Проводятся многочисленные эксперименты, в частности исследуется влияние числа внутренних и внешних циклов локального поиска на трудоемкость генерации целевого S-блока. Обосновываются оптимальные (с точки зрения минимальных затрат времени) параметры алгоритма локального поиска для генерации S-блоков с целевой нелинейностью 104 и количеством параллельных вычислительных потоков 30. Показано, что с выбранными (оптимальными) параметрами удается надежно формировать S-блоки с нелинейностью 104.

Ключевые слова: симметричная криптография; нелинейные подстановки; S-boxes; алгоритм локального поиска; оптимизация параметров.

Табл. 1. Ил. 8. Библиогр.: 32 назв.

UDC 004.056.5

Optimization of local search algorithm parameters for generating nonlinear substitutions / *A.A. Kuznetsov, N.A. Poluyanenko, S.L.Berdnik, S.O. Kandii, Yu.A. Zaichenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №206. P. 64 – 76.

Nonlinear substitutions (S-boxes) are an important component of modern symmetric cryptography algorithms. They complicate symmetric transformations and introduce nonlinearity into the input-output relationship, which ensures the stability of the algorithms against some cryptanalysis methods. Generation of S-boxes can be done in different ways. However, heuristic techniques are the most promising ones. On the one hand, the generated S-boxes are in the form of random substitutions, which complicates algebraic cryptanalysis. On the other hand, heuristic search allows one to achieve high rates of nonlinearity and □-uniformity, which complicates linear and differential cryptanalysis. This article studies the simplest local search algorithm for generating S-boxes. To assess the efficiency of the algorithm, the concept of a track of a cost function is introduced in the article. Numerous experiments are carried out, in particular, the influence of the number of internal and external loops of local search on the complexity of generating the target S-box is investigated. The optimal (from the point of view of minimum time consumption) parameters of the local search algorithm for generating S-blocks with a target nonlinearity of 104 and the number of parallel computing threads 30 are substantiated. It is shown that with the selected (optimal) parameters it is possible to reliably form S-blocks with a nonlinearity of 104.

Key words:

1 tab. 8 fig. Ref: 32 items.

УДК 004.056.5

Дослідження обчислювальної складності методів приховування інформації у кластерні стеганосистеми / *К.Ю. Шеханін, С.В.Пшенична, О.О. Кузнецов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 206. С. 77 – 87.

На даний час відомо декілька методів технічної стеганографії. Приховування інформації у модель під час 3D-друку, дана галузь приховування інформації має певні переваги та недоліки, а саме: відносно більшу вартість при створенні прихованого повідомлення та складності при зчитуванні інформації. Другий напрямок технічної стеганографії пов'язаний із мережевим трафіком. У даному методі інформація може приховуватись, наприклад, у поля заголовків протоколів, чи, наприклад, передача прихованого повідомлення шляхом посилання певної послідовності пакетів. Також існують методи приховування інформації у структуру файлової системи але відомі методи або здатні приховати малу кількість інформації, або мають належний рівень стійкості до детектування. Таким чином, актуальною задачею є розробка методу приховування інформації, яка здатна приховати більшу кількість інформації та має більший рівень стійкості до детектування із задовільним рівнем обчислювальної складності.

Представлено методи технічної стеганографії, що базуються на структурній особливості файлових систем у носіях інформації. А саме, приховування інформації у файловій системі FAT шляхом перемішування кластерів певних, ключових файлів. Методи приховування інформації у структуру кластерної файлової системи шляхом перемішування кластерів покриваючих файлів потребують значних обчислювальних ресурсів. Досліджено методи підвищення обчислювальної ефективності за кількістю необхідної оперативної пам'яті та за кількістю необхідних операцій для приховування повідомлення.

Ключові слова: стеганографія; методи приховування інформації; обчислювальна складність; оперативна пам'ять.

Табл. 6. Іл. 4. Бібліогр.: 14 назв.

УДК 004.056.5

Исследование вычислительной сложности методов сокрытия информации в кластерные стеганосистемы / *К.Ю. Шеханин, С.В.Пшеничная, А.А. Кузнецов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 206. С. 77 – 87..

В настоящее время известны несколько методов технической стеганографии. Сокрытие информации в модель при 3D-печати. Данная отрасль сокрытия информации имеет определенные преимущества и недостатки, а именно: относительно большую стоимость создания скрытого сообщения и сложности при считывании информации. Второе направление технической стеганографии связано с сетевым трафиком. В данном методе информация может скрываться, например, в поля заголовков протоколов, или, например, передача скрытого уведомлением путем отправления пакетов в определенной последовательности. Также существуют методы сокрытия информации в структуру файловой системы, но известные методы или способны скрыть малое количество информации, или имеют недостаточный уровень устойчивости к детектированию. Таким образом, актуальной задачей является разработка метода сокрытия информации, которая способна скрыть большее количество информации и имеет больший уровень устойчивости к детектированию, с удовлетворительным уровнем вычислительной сложности.

Представлены методы технической стеганографии, основанные на структурной особенности файловых систем в носителях информации. В частности, сокрытие информации в файловой системе FAT путем перемешивания кластеров определенных, ключевых файлов. Методы сокрытия информации в структуру кластерной файловой системы путем перемешивания кластеров покрывающих файлов требуют значительных вычислительных ресурсов. Проведены исследования касательно методов повышения вычислительной эффективности по количеству необходимой оперативной памяти и по количеству необходимого количества операций для сокрытия сообщения.

Ключевые слова: стеганография; методы сокрытия информации; вычислительная сложность; оперативная память.

Табл. 6. Ил. 4. Библиогр.: 14 назв.

УДК 004.056.5

Investigation of the computational complexity of methods for hiding information in cluster steganosystems / *K.Yu. Shekhanin, S.V.Pshenichnaya, A.A. Kuznetsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №206. P. 77 – 87.

Several methods of technical steganography are currently known. Hiding information in a model in 3D printing, this industry of hiding information has certain advantages and disadvantages, namely: the relatively high cost of creating a hidden message and the difficulty in reading the information. The second area of technical steganography is related to network traffic. In this method, information can be hidden, for example, in the header fields of protocols, or, for example, the transmission of a hidden message by sending packets in a certain sequence. There are also methods of hiding information in the structure of the file system, but the known methods are either capable of hiding a small amount of information, or have an insufficient level of resistance to detection. Thus, an urgent task is to develop a method for hiding information, which is able to hide more information and has a higher level of resistance to detection, with a satisfactory level of computational complexity.

This paper presents methods of technical steganography based on the structural features of file systems in storage media, in particular, hiding information in the FAT file system by mixing clusters of certain key files (cover files). Methods of hiding information in the structure of a clustered file system by mixing clusters of cover files require significant computational resources. In this paper, research has been carried out on methods to increase computational efficiency in terms of the amount of required RAM, and the number of the required number of basic operations to hide a message.

Key words: steganography; methods of hiding information; computational complexity; RAM.

6 tab. 4 fig. Ref: 14 items.

УДК 004.056

Модель захисту бази даних на основі системи безпеки з повним перекриттям / *В.В. Вілігура, В.І. Єсін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 206. С. 88 – 105.

Безпека (захищеність) є однією з найважливіших характеристик якості інформаційних систем в цілому і баз даних, як їх основною складовою, зокрема. Тому наявність системи захисту інформації як комплексу програмних, технічних, криптографічних, організаційних та інших методів, засобів і заходів, що забезпечують цілісність, конфіденційність, автентичність і доступність інформації в умовах впливу на неї загроз природного або штучного характеру, є невід'ємною рисою практично будь-якої сучасної інформаційної системи і бази даних. Разом з тим, щоб можна було перевірити висновки про ступінь забезпечення безпеки, її необхідно якимось чином виміряти. У роботі розглядається модель захисту бази даних, заснована на моделі системи безпеки з повним перекриттям, яка традиційно вважається основою формального опису систем захисту. Завдяки розширен-

ню моделі Клементса – Хоффмана за рахунок включення множини вразливостей (як окремо об'єктивно існуючої категорії – слабкого місця активу або засобу управління, яке може бути використано однією або більше загрозою), що дозволяє більш адекватно оцінювати вірогідність небажаного інциденту (реалізації загрози) в двохфакторній моделі (в якій один з факторів відображає мотиваційну складову виникнення загрози, а другий – враховує існуючі уразливості); визначеному інтегральному показнику захищеності бази даних (як величини зворотної до сумарного залишкового ризику, складові компоненти якої представляються у вигляді відповідних лінгвістичних змінних); розробленому методу оцінювання основних компонент бар'єрів безпеки і захищеності бази даних в цілому, що спирається на теорію нечітких множин та ризику, стає можливим використання розробленої моделі для проведення кількісної оцінки безпеки аналізованої бази даних.

Ключові слова: модель безпеки; система безпеки з повним перекриттям; база даних.

Табл. 2. Іл. 7. Бібліогр.: 48 назв.

УДК 004.056

Модель защиты базы данных на основе системы безопасности с полным перекрытием / *В.В. Вилигура, В.И. Есин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 206. С. 88 – 105.

Безопасность (защищенность) является одной из важнейших характеристик качества информационных систем в целом и баз данных, как их основной составляющей, в частности. Поэтому наличие системы защиты информации как комплекса программных, технических, криптографических, организационных и иных методов, средств и мероприятий, обеспечивающих целостность, конфиденциальность, аутентичность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера, является неотъемлемой чертой практически любой современной информационной системы и базы данных. Вместе с тем, чтобы можно было проверить выводы о степени обеспечения безопасности, ее необходимо каким-либо образом измерить. В работе рассматривается модель защиты базы данных, основанная на модели системы безопасности с полным перекрытием, традиционно считающейся основой формального описания систем защиты. Благодаря расширению модели Клементса – Хоффмана за счет включения множества уязвимостей (как отдельно объективно существующей категории – слабого места актива или средства управления, которое может быть использовано одной или более угрозой), что позволяет более адекватно оценивать вероятность нежелательного инцидента (реализации угрозы) в двухфакторной модели (в которой один из факторов отображает мотивационную составляющую возникновения угрозы, а второй – учитывает существующие уязвимости); определенному интегральному показателю защищенности базы данных (как величины обратной суммарному остаточному риску, составные компоненты которой представляются в виде соответствующих лингвистических переменных); разработанному методу оценивания основных компонент барьеров безопасности и защищенности базы данных в целом, опирающемуся на теорию нечетких множеств и риска, становится возможным использование разработанной модели для проведения количественной оценки безопасности анализируемой базы данных.

Ключевые слова: модель безопасности; система безопасности с полным перекрытием; база данных.

Табл. 2. Ил. 7. Библиогр.: 48 назв.

UDC 004.056

Database protection model based on security system with full overlap / *V.V. Vilihura, V.I. Yesin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №206. P. 88 – 105.

Security is one of the most important characteristics of the quality of information systems in general and databases, as their main component, in particular. Therefore, the presence of an information protection system, as a complex of software, technical, cryptographic, organizational and other methods, means and measures that ensure the integrity, confidentiality, authenticity and availability of information in conditions of exposure to natural or artificial threats, is an integral feature of almost any modern information system and database. At the same time, in order to be able to verify the conclusions about the degree of security, it must be measured in some way. The paper considers a database security model based on a full overlap security model (a covered security system), which is traditionally considered the basis for a formal description of security systems. Thanks to expanding the Clements-Hoffman model by including a set of vulnerabilities (as a separately objectively existing category necessary to describe a weakness of an asset or control that can be exploited by one or more threats), which makes it possible to assess more adequately the likelihood of an unwanted incident (threat realization) in a two-factor model (in which one of the factors reflects the motivational component of the threat, and the second takes into account the existing vulnerabilities); a defined integral indicator of database security (as a value inverse to the total residual risk, the constituent components of which are represented in the form of the corresponding linguistic variables); the developed technique for assessing the main components of security barriers and the security of the database as a whole, based on the theory of fuzzy sets and risk, it becomes possible to use the developed model to conduct a quantitative assessment of the security of the analyzed database.

Key words: security model; full overlap security system; covered security system; database.

2 tab. 7 fig. Ref: 48 items.

УДК 681.3.06

Криптоаналіз систем на основі проблеми слова з використанням логарифмічних підписів / *Є.В. Котух, Т.О. Охріменко, О.Ф. Дяченко, Н.Ю. Ротаньова, Л.С. Козіна, Д.В. Зеленський* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 206. С.106 – 114.

Стрімкий розвиток та досягнення у сфері квантових комп'ютерів сприяють розвитку криптосистем з відкритим ключем на основі математично складних або важко вирішуваних задач, адже загроза використання квантових алгоритмів для зламу сучасних традиційних криптосистем стає набагато реальнішою з кожним днем. Варто зазначити, що класичні математично складні проблеми факторизації цілих чисел та дискретних логарифмів більш не вважаються складними для квантових обчислень. Десятки криптосистем були розглянуті та запропоновані з різних складних проблем теорії груп у 2000-х роках. Одною з таких складних проблем є проблема слова. Одна з перших реалізацій криптосистеми на основі проблеми слова було запропоновано Магліверасом з використанням логарифмічних підписів для кінцевих груп перестановок та надалі запропоновано Лемпкеном та ін. для асиметричної криптографії з випадковими покриттями. Новаторство цієї ідеї полягає у поширенні важко вирішуваної проблеми слова на велику кількість груп. У статті узагальнено відомі результати криптоаналізу базових конструкцій криптосистеми MST_3 та визначено рекомендації для напрямків покращення криптографічних властивостей конструкцій MST_3 та використання некомутативних груп у якості базових конструкцій.

Ключові слова: постквантова криптографія; логарифмічний підпис; теорія груп; покриття; криптоаналіз.
Табл. 2. Бібліогр.: 21 назв.
УДК 681.3.06

Криптоанализ системы на основе проблем слова с использованием логарифмических подписей / *Е.В. Котух, Т.А. Охрименко, О.Ф. Дяченко, Н.Ю. Ротанева, Л.С. Козина, Д.В. Зеленский* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 206. С. 106 – 114.

Стремительное развитие и достижения в сфере квантовых компьютеров способствуют развитию криптосистем с открытым ключом на основе математически сложных или трудно решаемых задач, поскольку угроза использования квантовых алгоритмов для излома современных традиционных криптосистем становится гораздо реальнее с каждым днем. Следует отметить, что классические математически сложные проблемы факторизации целых чисел и дискретных логарифмов больше не считаются сложными для квантовых вычислений. Десятки криптосистем были рассмотрены и предложены по разным сложным проблемам теории групп в 2000-х годах. Одной из таких сложных проблем является проблема слова. Одна из первых реализаций криптосистемы на основе проблемы слова была предложена Магливерасом с использованием логарифмических подписей для конечных групп перестановок и в дальнейшем предложена Лемпкеном и т.д. для асимметричной криптографии со случайными покрытиями. Новаторство этой идеи состоит в распространении трудно решаемой проблемы слова на большое количество групп. В статье обобщены известные результаты криптоанализа базовых конструкций криптосистемы MST_3 и определены рекомендации для направлений улучшения криптографических свойств конструкций MST_3 и использования некоммутативных групп в качестве базовых конструкций.

Ключевые слова: постквантовая криптография; логарифмическая подпись; теория групп; покрытие; криптоанализ.
Табл. 2. Библиогр.: 21 назв.
UDC 681.3.06

Cryptanalysis of the system based on word problems using logarithmic signatures / *Y. Kotukh, T. Okhrimenko, O. Dyachenko, N. Rotaneva, L. Kozina, D. Zelenskyi* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №206. P. 106 – 114.

Rapid development and advances of quantum computers are contributing to the development of public key cryptosystems based on mathematically complex or difficult problems, as the threat of using quantum algorithms to hack modern traditional cryptosystems is becoming much more real every day. It should be noted that the classical mathematically complex problems of factorization of integers and discrete logarithms are no longer considered complex for quantum calculations. Dozens of cryptosystems were considered and proposed on various complex problems of group theory in the 2000s. One of such complex problems is the problem of the word. One of the first implementations of the cryptosystem based on the word problem was proposed by Magliveras using logarithmic signatures for finite permutation groups and further proposed by Lempken et al. for asymmetric cryptography with random covers. The innovation of this idea is to extend the difficult problem of the word to a large number of groups. The article summarizes the known results of cryptanalysis of the basic structures of the cryptosystem and defines recommendations for ways to improve the cryptographic properties of structures and the use of non-commutative groups as basic structures.

Key words: postquantum cryptography; logarithmic signature; group theory; coverage; cryptanalysis.
4 tab. 6 fig. Ref: 13 items.

РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ
РАДИОЛОКАЦИЯ И РАДИОНАВИГАЦИЯ
RADIOLOCATION AND RADIONAVIGATION

УДК 004.89: 621.396

Метод боротьби з нестаціонарними завадами природними та тих, що імітують об’єкт, в інтелектуальних оглядових РЛС / *В.В. Жирнов, С.В. Солонська, В.І. Зарицкий* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 206. С. 115– 121.

Розглядається метод боротьби з нестаціонарними завадами природними та тими, що імітують об’єкт, в інтелектуальних оглядових РЛС. При створенні відміток, що імітують об’єкт, використовується внесення амплітудної модуляції в ретранслюючий зондучий сигнал РЛС. В результаті аналізу вдалося з'ясувати, що в завадах, що імітують об’єкт, при цьому з'являються так звані «інтелектуальні» флуктуації пачкової структури помилкових відміток, які відрізняються від флуктуацій пачок реальних оцінок і можуть бути легко виявлені людиною-оператором. Метод заснований на визначенні семантичних складових на етапі формування і аналізу символьної моделі амплітудних флуктуацій пачки сигналів від нестаціонарних завад й тих, що імітують об’єкт, і від реальних рухомих об'єктів. При цьому семантичні ознаки амплітудних флуктуацій визначаються шляхом рішення предикатних рівнянь перетворення цих флуктуацій в символьні зображення відміток завад і реальних рухомих літальних апаратів. В результаті семантичного аналізу амплітудних флуктуацій пачки в часовій області отримані класифікаційні відмінні ознаки флуктуацій пачки сигналів від завад природних і тих, що імітують об’єкт, і повітряних об'єктів. Досліджено семантичні складові алгоритму прийняття рішень, які подібні до алгоритмів прийняття рішень людиною-оператором. Формалізовані процесні знання перетворення радіолокаційних сигналів в символьні зображення амплітудних флуктуацій пачки в часовій області. Формалізація процесів обробки символьних зображень включає систему предикатних рівнянь, рішення яких здійснює ідентифікацію типів амплітудних флуктуацій пачки. Ґрунтуючись на результатах експериментальних даних, проведені перетворення реальних радіолокаційних сигналів в символьні зображення флуктуацій пачки на основі алгебри кінцевих предикатів. Також авторам вдалося запропонувати ці перетворення використовувати як основу ефективного інструментарію для отримання класифікаційних відмінних ознак флуктуацій пачки від завад і від літальних апаратів.

Ключові слова: нестаціонарна завада природна та, що імітує об’єкт; символьне зображення; виявлення; розпізнавання; інтелектуальна система; символьна модель.

Іл. 3. Бібліогр.: 13 назв.

УДК 004.89: 621.396

Метод борьбы с нестационарными естественными и имитирующими помехами в интеллектуальных обзорных РЛС / *В.В. Жирнов, С.В. Солонская, В.И. Зарицкий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 206. С. 115– 121.

Рассматривается метод борьбы с нестационарными естественными и имитирующими помехами в интеллектуальных обзорных РЛС. При создании имитирующих отметок используется внесение амплитудной модуляции в ретранслируемый зондирующий сигнал РЛС. В результате анализа удалось выяснить, что в имитирующих помехах при этом появляются так называемые «интеллектуальные» флуктуации пачечной структуры ложных отметок, которые отличаются от флуктуаций пачек реальных отметок и могут быть легко обнаружены человеком-оператором. Метод основан на определении семантических составляющих на этапе формирования и анализа символьной модели амплитудных флуктуаций пачки сигналов от нестационарных естественных и имитирующих помех и от реальных подвижных объектов. При этом семантические признаки амплитудных флюктуаций определяются путем решения предикатных уравнений преобразования этих флюктуаций в символьные изображения отметок помех и реальных подвижных летательных аппаратов. В результате семантического анализа амплитудных флуктуаций пачки во временной области получены классификационные отличительные признаки флуктуаций пачки сигналов от естественных, имитирующих помех и воздушных объектов. Исследованы семантические составляющие алгоритма принятия решений, которые подобны алгоритмам принятия решений человеком-оператором. Формализованы процессные знания преобразования радиолокационных сигналов в символьные изображения амплитудных флуктуаций пачки во временной области. Формализация процессов обработки символьных изображений включает систему предикатных уравнений, путем решения которых осуществляется идентификация типов амплитудных флуктуаций пачки. Основываясь на результатах экспериментальных данных, проведены преобразования реальных радиолокационных сигналов в символьные изображения флуктуаций пачки на основе алгебры конечных предикатов. Также авторам удалось предложить эти преобразования использовать как основу эффективного инструментария для получения классификационных отличительных признаков флуктуаций пачки от помех и от летательных аппаратов.

Ключевые слова: нестационарная естественная и имитирующая помеха; символьное изображение; обнаружение; распознавание; интеллектуальная система; символьная модель.

Ил. 3. Библиогр.: 13 назв.

UDC 004.89: 621.396

Method for dealing with non-stationary natural and simulating interference in intellectual surveillance radars / *V. Zhyrnov, S. Solonskaya, V. Zarytskyi* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №206. P. 115– 121.

The article discusses a method for dealing with non-stationary natural and simulating interference in intelligent surveillance radars. When creating simulating marks, the introduction of amplitude modulation into the relayed radar sounding signal is used. As a result of the analysis, it was possible to find out that in the imitating noise, in this case, the so-called "intelligent" fluctuations of the burst structure of false marks appear, which differ from the fluctuations of the packs of real marks and can be easily detected by a human operator. The method is based on the definition of semantic components at the stage of formation and analysis of a symbolic model of amplitude fluctuations of a burst of signals from non-stationary natural and simulating interference and from real moving objects. In this case, the semantic features of amplitude fluctuations are determined by solving predicate equations for transforming these fluctuations into symbolic images of noise marks and real mobile aircraft. As a result of semantic analysis of the amplitude fluctuations of the burst in the time domain, classification distinctive features of fluctuations in the burst of signals from natural imitating noise and air objects were obtained. The semantic components of the decision-making algorithm are investigated, which are similar to the decision-making algorithms by a human operator. Process knowledge of transforming radar signals into symbolic images of amplitude fluctuations of a burst in the time domain is formalized. The formalization of the processing of symbolic images includes a system of predicate equations, by solving which the types of amplitude fluctuations of the burst are identified. Based on the results of experimental data, the transformations of real radar signals into symbolic images of burst fluctuations were carried out on the basis of the algebra of finite predicates. The authors also managed to propose these transformations to be used as the basis of an effective toolkit for obtaining classification distinctive features of packet fluctuations from interference and from aircraft.

Key words: non-stationary natural and imitating interference; symbolic image; detection; recognition; intelligent system; symbolic model.

3 fig. Ref: 13 items.

УДК 621.397.48:004.932.2

Виявлення безпілотних літальних апаратів з використанням розсіювання радіохвиль на акустичних обуреннях середовища, що створюються літальними апаратами / *В.М. Карташов, О.І. Харченко, В.О. Посошенко, В.І. Колесник, А.Б. Єгоров, Л.П. Тимошенко, А.І. Капуста* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 206. С. 122 – 130.

Безпілотні літальні апарати (БПЛА) отримали значне поширення, оскільки здатні виконувати широкий спектр корисних для людства функцій. У той же час БПЛА є джерелом потенційних загроз у ряді областей діяльності людини – військовій, господарській, повсякденній. Тому в останні роки сформувалася актуальна науково-технічна проблема виявлення і спостереження БПЛА з метою запобігання виконання ними несанкціонованих дій. Основними засобами спостереження БПЛА є радіолокаційні (як активні, так і пасивні), оптичні, інфрачервоні, акустичні станції, а також комплексні системи, в яких здійснюється спільна обробка інформації, що була одержана з використанням зазначених інформаційних каналів. Однак в цілому науково-технічна проблема спостереження БПЛА, особливо малих БПЛА, залишається невирішеною: ефективність виявлення БПЛА з використанням всіх зазначених методів залишається недостатньою, а потреби практики наявними засобами задовольняються далеко не в повній мірі.

Стаття присвячена аналізу відомих наукових і практичних результатів з метою оцінки можливості виявлення БПЛА за радіосигналами, розсіяними на акустичних збуреннях середовища, створюваних БПЛА, і формулювання актуальних наукових і технічних завдань в даній області знань.

Ключові слова: безпілотний літальний апарат; виявлення; розпізнавання; радіолокаційна станція; акустична хвиля; розсіювання; радіоакустичне зондування.

Іл. 4. Бібліогр.: 38 назв.

УДК 621.397.48:004.932.2

Обнаружение беспилотных летательных аппаратов с использованием рассеяния радиоволн на акустических возмущениях среды, создаваемых летательным аппаратом / *В.М. Карташов, О.И. Харченко, В.А. Посошенко, В.И. Колесник, А.Б. Егоров, Л.П. Тимошенко, А.И. Капуста* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 206. С. 122 – 130.

Беспилотные летательные аппараты (БПЛА) получили в последнее время значительное распространение, поскольку способны выполнять широкий спектр полезных для человечества функций. В то же время БПЛА являются источником потенциальных угроз в ряде областей деятельности человека – военной, хозяйственной, повседневной. Поэтому в последние годы сформировалась актуальная научно-техническая проблема обнаружения и наблюдения БПЛА с целью предотвращения выполнения ими несанкционированных действий. Основными средствами наблюдения БПЛА являются радиолокационные (как активные, так и пассивные), оптические, инфракрасные, акустические станции, а также комплексные системы, в которых осуществляется совместная обработка информации, получаемой с использованием указанных информационных каналов. Однако в целом научно-техническая проблема наблюдения БПЛА, особенно малых БПЛА, остается нерешенной: эф-

фективность обнаружения БПЛА с использованием всех указанных методов остается недостаточной, а потребности практики имеющимися средствами удовлетворяются далеко не в полной мере.

Статья посвящена анализу известных научных и практических результатов с целью оценки возможности обнаружения БПЛА по радиосигналам, рассеянным на акустических возмущениях среды, создаваемых БПЛА, и формулированию актуальных научных и технических задач в данной области знаний.

Ключевые слова: беспилотный летательный аппарат; обнаружение; распознавание; радиолокационная станция; акустическая волна; рассеяние; радиоакустическое зондирование.

Ил. 4. Библиогр.: 38 назв.

UDC 621.397.48:004.932.2

Detection of unmanned aerial vehicle using radio wave scatter on acoustic disturbances of the environment created by aircraft / *V.M. Kartashov, O.I. Kharchenko, V.A. Pososhenko, V.I. Kolesnik, A.B. Yegorov, L.P. Tymoshenko, A I. Kapusta* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №206. P. 122 – 130.

Unmanned aerial vehicles (UAVs) have recently become widespread, because they are capable of performing a wide range of functions useful for mankind. At the same time, UAVs are a source of potential threats in a number of areas of human activity, namely, military, economic, and everyday life. Therefore, an urgent scientific and technical problem of detecting and observing UAVs has been formed recently to prevent them from performing unauthorized actions. The main means of UAV surveillance are radar (both active and passive), optical, infrared, acoustic stations, as well as complex systems in which joint processing of information obtained using these information channels is carried out. However, in general, the scientific and technical problem of monitoring UAVs, especially small UAVs, remains unresolved: the efficiency of UAV detection using all these methods remains insufficient, and the needs of practice are far from being fully satisfied with the available means.

This article is devoted to the analysis of currently known scientific and practical results aimed to assess the possibility of detecting UAVs by radio signals scattered by acoustic disturbances of the environment created by UAVs, and to formulate urgent scientific and technical problems in this aria of knowledge.

Key words: unmanned aerial vehicle; detection; recognition; radar; acoustic wave; scattering; radio acoustic sounding.

4 fig. Ref: 38 items.

ІНФОРМАЦІЙНІ МЕТОДИ РАДІОТЕХНІКИ
ИНФОРМАЦИОННЫЕ МЕТОДЫ РАДИОТЕХНИКИ
INFORMATION METHODS OF RADIO ENGINEERING

УДК 006.91:004.9

Особливості статистичної обробки даних засобами систем комп'ютерної математики / *І.О. Мощенко, О.М. Нікітенко, Ю.В. Козлов, Ю.Г. Жарко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 206. С. 131 – 136.

Проаналізовано процеси накопичення похибок під час проведення арифметичних операцій над статистичними даними, що отримані під час дослідження коливальних станів електровакуумних приладів зі схрещеними полями.

Досліджено особливості статистичної обробки даних, що отримано в результаті експериментальних досліджень, за допомогою найбільш широко розповсюджених комп'ютерних математичних пакетів.

Особливості обробки статистичних даних досліджено шляхом обробки вибірки з 80 значень частоти генерації магнетрону за допомогою популярних математичних пакетів Excel, Maple, Matlab та MathCad та порівняння отриманих результатів з розрахунками за теоретичними формулами. Результати розрахунків за допомогою усіх пакетів дають однакові результати для математичного сподівання, дисперсії та стандартного відхилення. Щодо коефіцієнтів асиметрії та ексцесу, то більшість результатів не збігаються.

Аналіз результатів розрахунків показав, що відмінність отриманих значень коефіцієнтів асиметрії та ексцесу обумовлений різними визначеннями цих показників математичними пакетами Excel, Maple, Matlab та MathCad. Доведено, що в Microsoft Excel ми не можемо правильно побудувати гістограму без використання додаткових операцій, оскільки межі інтервалів обчислюються з помилками. Це призводить до неправильного визначення кількості елементів у цих інтервалах. Для того щоб вірно побудувати гістограму за допомогою пакету Excel, необхідно заздалегідь розрахувати межі інтервалів.

Зроблено висновок, що перед використанням комп'ютерних математичних пакетів для обробки статистичних даних потрібно попередньо проаналізувати за якими формулами розраховані необхідні параметри та вжити відповідних заходів для усунення можливих розбіжностей з параметрами, розрахованими за теоретичними формулами.

Ключові слова: системи комп'ютерної математики; обробка даних; накопичення похибок; Excel; Matlab; Maple; MathCad.

Табл. 3. Іл. 5. Бібліогр.: 8 назв.

УДК 006.91:004.9

Особенности статистической обработки данных средствами систем компьютерной математики / *И.А. Мощенко, А.Н. Никитенко, Ю.В. Козлов, Ю.Г. Жарко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 206. С. 131 – 136.

Проанализированы процессы накопления погрешностей при проведении арифметических операций над статистическими данными, полученными в ходе исследования колебательных состояний электровакуумных приборов со скрещенными полями.

Исследованы особенности статистической обработки данных, полученных в результате экспериментальных исследований, с помощью наиболее широко распространенных компьютерных математических пакетов.

Особенности обработки статистических данных исследованы путем обработки выборки из 80 значений частоты генерации магнетрона с помощью популярных математических пакетов Excel, Maple, Matlab и MathCad и сравнения полученных результатов с расчетами по теоретическим формулам. Результаты расчетов с помощью всех пакетов дают одинаковые результаты для математического ожидания, дисперсии и стандартного отклонения. Что касается коэффициентов асимметрии и эксцесса, то большинство результатов не совпадают.

Анализ результатов расчетов показал, что различие полученных значений коэффициентов асимметрии и эксцесса обусловлено разными определениями этих показателей математическими пакетами Excel, Maple, Matlab и MathCad. Доказано, что в Microsoft Excel мы не можем правильно построить гистограмму без использования дополнительных операций, поскольку границы интервалов вычисляются с ошибками. Это приводит к неправильному определению количества элементов в этих интервалах. Для того чтобы верно построить гистограмму с помощью пакета Excel, необходимо заранее рассчитать границы интервалов.

Сделан вывод, что перед использованием компьютерных математических пакетов для обработки статистических данных необходимо предварительно проанализировать по каким формулам рассчитываются необходимые параметры и принять соответствующие меры для устранения возможных несовпадений с параметрами, рассчитанными по теоретическим формулам.

Ключевые слова: системы компьютерной математики; обработка данных; накопление погрешностей; Excel; Matlab; Maple; MathCad.

Табл. 3. Ил. 5. Библиогр.: 8 назв.

UDC 006.91:004.9

Feature of statistical data processing by computer mathematics systems tools / *I. Moshchenko, O. Nikitenko, Yu.V. Kozlov, Yu.H. Zharko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №206. P. 131 – 136.

Processes of error accumulation were analysed during arithmetic operations on statistical data obtained in the course of research on oscillations in cross-field electron vacuum devices.

The features of statistical data processing obtained as a result of experimental research were investigated using the most widespread computer mathematical packages.

The features of statistical data processing were investigated by processing a sample of 80 values of the magnetron generation frequency using popular mathematical packages Excel, Maple, Matlab and MathCad and comparing the results obtained with calculations using theoretical formulas. Calculation results for all packages give the same results for mean, variance and standard deviation. As for the coefficients of skewness and kurtosis, most of the results do not coincide.

Analysis of the calculation results showed that the difference in the obtained values of the skewness and kurtosis is due to different definitions of these indicators in mathematical packages Excel, Maple, Matlab and MathCad. It is proved that in Microsoft Excel we cannot correctly construct a histogram without using additional operations, because the interval limits are calculated with errors. It leads to an incorrect determination of the number of elements into these intervals.

To build correctly a histogram using the Excel package, it is necessary to calculate the interval limits in advance.

It is concluded that before using computer mathematical packages for processing statistical data, it is necessary to analyze first by what formulas the required parameters are calculated and take appropriate measures to eliminate possible discrepancies with the parameters calculated using theoretical formulas.

Key words: computer mathematics systems; data processing; error accumulation; Excel; Matlab; Maple; MathCad.

3 tab. 5 fig. Ref: 8 items.

БІОМЕДИЧНА РАДІОЕЛЕКТРОНІКА

БИОМЕДИЦИНСКАЯ РАДИОЭЛЕКТРОНИКА
BIOMEDICAL RADIO ELECTRONICS

УДК 621.372; 616.12-073.7

Модифіковані алгоритми виділення нелінійного тренду сигналів / *Н.О. Тулякова, О.М. Трофимчук* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 206. С. 137 – 151.

У багатьох практичних застосуваннях цифрової обробки сигналів існує задача виділення нелінійного (стрибкоподібного) тренду сигналів. Зокрема, в області обробки біомедичних сигналів актуальною проблемою є усунення стрибкоподібних спотворень базової лінії сигналу, спричинених рухами пацієнта. Для обробки таких сигналів, що містять стрибки та інші точки розриву похідної, лінійна фільтрація на основі дискретних Фур'є або косинусного перетворень призводить до значного згладжування сигналу. Для фільтрації зазначених сигналів успішно застосовуються медіанні алгоритми, що відносяться до нелінійних стійких (робастних) фільтрів, зокрема, високу ефективність забезпечують гібридні медіанні фільтри з кінцевою імпульсною характеристикою (КІХ). У статті розглянуто прості алгоритми класу КІХ-гібридних медіанних фільтрів, що використовуються для виділення нелінійного тренду сигналів. Запропоновано модифікувати ці алгоритми шляхом заміни операції знаходження медіани даних у ковзному вікні фільтра на обчислення їх міріади, а також додавання ваги (кількості дублювань) певним елементам вікна. Отримано статистичні оцінки ефективності фільтрів за критерієм середньоквадратичної помилки (СКП) для тестових сигналів видів “різкого” та “похилого” перепадів, трикутного піку та параболи. На основі аналізу вихідних сигналів фільтрів і статистичних оцінок їх якості показано високу ефективність застосування досліджуваних нелінійних фільтрів для перелічених типів тестових сигналів і поліпшення, досягнуті в результаті запропонованих модифікацій фільтрів. Наведено приклади обробки біомедичних сигналів електроенцефалограм, що ілюструють гарну якість придушення шуму і збереження різких змін сигналу, та видалення рухових артефактів без значних спотворень сигналу.

Ключові слова: нелінійний тренд; КІХ-гібридні медіанні фільтри; міріадна фільтрація; статистичні оцінки якості; електроенцефалограми; шум; рухові артефакти.

Іл. 11. Бібліогр.: 45 назв.

УДК 621.372; 616.12-073.7

Модифицированные алгоритмы выделения нелинейного тренда сигналов / *Н.О. Тулякова, А.Н. Трофимчук* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 206. С. 137 – 151.

Во многих практических приложениях цифровой обработки сигналов существует задача выделения нелинейного (скачкообразного) тренда сигналов. В частности, в области обработки биомедицинских сигналов актуальной проблемой является устранение скачкообразных искажений базовой линии сигнала, вызванных движениями пациента. Для обработки таких сигналов, содержащих скачки и другие точки разрыва производной, линейная фильтрация на основе дискретных Фурье или косинусного преобразований приводит к значительному сглаживанию сигнала. Для фильтрации данных сигналов успешно применяются медианные алгоритмы, относящиеся к классу нелинейных устойчивых (робастных) фильтров, высокую эффективность обеспечивают гибридные медианные фильтры с конечной импульсной характеристикой (КИХ). В статье рассмотрены простые алгоритмы класса КИХ-гибридных медианных фильтров, используемые для выделения нелинейного тренда сигналов. Предложено модифицировать данные алгоритмы путем замены операции нахождения медианы данных в скользящем окне фильтра на вычисление их мириады, а также добавления веса (количества дублирований) определенным элементам окна. Получены статистические оценки эффективности фильтров по критерию среднеквадратической ошибки (СКО) для тестовых сигналов видов “резкого” и “наклонного” перепадов, треугольного пика и параболы. На основе анализа выходных сигналов фильтров и статистических оценок их качества показано высокую эффективность применения исследуемых нелинейных фильтров для перечисленных типов тестовых сигналов и улучшения, достигнутые в результате предложенных модификаций фильтров. Приведены примеры обработки биомедицинских сигналов электроэнцефалограмм, иллюстрирующие хорошее качество подавления шума и сохранения резких изменений сигнала, и удаление двигательных артефактов без значительных искажений сигнала.

Ключевые слова: нелинейный тренд; КИХ-гибридные медианные фильтры; мириадная фильтрация; статистические оценки качества; электроэнцефалограммы; шум; двигательные артефакты.

Ил. 11. Библиогр.: 45 назв.

UDC 621.372; 616.12-073.7

Modified algorithms for signal nonlinear trend detection / *N.O. Tulyakova, O.M. Trofymchuk* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №206. P. 137 – 151.

There is a problem of nonlinear (abrupt) signal trend detection in many digital signals processing practical applications. In particular, in the field of biomedical signals processing, the actual task is the elimination of abrupt signal baseline distortions caused by the patient's movements. For processing such signals containing edges and other discontinues, linear filtering based on discrete Fourier or cosine transforms leads to significant smoothing of a signal. Median type algorithms related to nonlinear stable (robust) filters are successfully applied for filtering such signals, in particular, high efficiency is provided by median hybrid filters with finite impulse response (FIR). The article considers simple algorithms of the class of FIR-median hybrid filters used for signal nonlinear trend detection. It is proposed to modify

these algorithms by replacing the operation of finding the median of the data in the sliding filter window with the calculation of their myriad, as well as adding weights (number of duplications) to certain window elements. Statistical estimates of filter efficiency according to the mean square error (MSE) criterion for test signals like “step” and “ramp” edges, and triangular peak and parabola have been obtained. The high efficiency of the investigated nonlinear filters for the listed test signals types and the improvements achieved as a result of the proposed filter modifications are shown based on the analysis of the filter output signals and statistical estimates of their quality. Some examples of processing biomedical signals of electroencephalograms which illustrate good quality of noise suppression and signal abrupt changes preservation, and motion artifacts removal without large signal distortions are given.

Key words: nonlinear trend; FIR-median hybrid filters; myriad filtering; statistical estimates of quality; electroencephalograms; noise; motion artifacts.

11 fig. Ref: 45 items.

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТЕХНОЛОГІЇ
ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ТЕХНОЛОГИИ
INFORMATION MEASURING TECHNOLOGIES

УДК 004.45:004.057.02

Вимірювання якості програмного забезпечення на основі міжнародних стандартів / *О.В. Запорожець, Н.В. Штефан* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 206. С. 152 – 157.

Якість є одним із факторів, що забезпечують комерційний успіх та безпеку використання програмного забезпечення. Під якістю розуміють відповідність явним і неявним вимогам різних зацікавлених сторін. Необхідно забезпечити спільне взаєморозуміння між розробниками та користувачами, інженери повинні розуміти значення поняття якості, характеристики та важливість якості для розробленого або підтримуваного програмного забезпечення. Основою забезпечення якості є вимірювання. Воно є основним інструментом керування життєвим циклом програмних продуктів, оцінки виконання планів і моніторингу. Для кількісного визначення якості необхідно виміряти характеристики програмного забезпечення. Стандартизація передбачає уніфікацію вимог до якості, її вимірювання та оцінки. Використання стандартів дає безліч потенційних переваг для будь-якої організації, особливо у таких ключових областях, як вимірювання якості програмних продуктів, інформаційних та вимірювальних систем. Визнані міжнародні організації із стандартизації опублікували серію стандартів ISO/IEC 25000 щодо вимог та оцінки якості систем та програмного забезпечення SQuaRE, яка набуває широкого практичного застосування. У статті обговорюється серія міжнародних стандартів SQuaRE, аналізується взаємозв’язок між моделлю якості, характеристиками якості, показниками якості та новою концепцією – елементом показника якості програмного забезпечення, представлено вимірювання якості на основі цих стандартів.

Ключові слова: якість; програмне забезпечення; вимірювання; стандарт; показник якості.

Табл. 1. Іл. 3. Бібліогр.: 10 назв.

УДК 004.45:004.057.02

Измерение качества программного обеспечения на основе международных стандартов / *О.В. Запорожець, Н.В. Штефан* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 206. С. 152 – 157.

Качество – один из основных факторов, обеспечивающих коммерческий успех и безопасность использования программного обеспечения. Качество понимается как соответствие явным и неявным требованиям различных заинтересованных сторон. Необходимо обеспечить совместное понимание между разработчиками и пользователями, инженеры должны понимать смысл, вкладываемый в концепцию качества, характеристики и значение качества в отношении разрабатываемого или сопровождаемого программного обеспечения. Основой обеспечения качества являются измерения. Они – основной инструмент управления жизненным циклом программных продуктов, оценки выполнения планов и мониторинга. Для количественного определения качества необходимо измерить характеристики программного обеспечения. Стандартизация обеспечивает унификацию требований к качеству, его измерению и оценке. Использование стандартов дает множество потенциальных преимуществ для любой организации, особенно в таких ключевых областях, как измерение качества программных продуктов, информационных и измерительных систем. Признанные международные организации по стандартизации опубликовали серию стандартов ISO/IEC 25000 по требованиям и оценке качества систем и программного обеспечения SQuaRE, которая получает все более широкое практическое применение. В статье рассмотрена серия международных стандартов SQuaRE, проанализировано отношение между моделью качества, характеристиками качества, показателями качества и новым понятием – элементом показателя качества программного обеспечения, представлено измерение качества на основе этих стандартов.

Ключевые слова: качество; программное обеспечение; измерение; стандарт; показатель качества.

Табл. 1. Ил. 3. Библиогр.: 10 назв.

UDC 004.45:004.057.02

Measurement of software quality based on international standards / *O. Zaporozhets, N. Shtefan* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №206. P. 152 – 157.

Quality is one of the factors that ensure the commercial success and safety of using the software. Quality is understood as conformity the explicit and implicit requirements of various stakeholders. It is necessary to ensure a joint

understanding between developers and users, engineers need to understand the meaning of the concept of quality, characteristics and importance of quality for the developed or maintained software. Measurements are the basis for quality assurance. They are the main tool for managing the life cycle of software products, assessing the implementation of plans and monitoring. To quantify quality, it is necessary to measure the characteristics of the software. Standardization provides unification of requirements for quality, its measurement and assessment. The use of standards has many potential benefits for any organization, especially in key areas such as measuring the quality of software products, information and measurement systems. Recognized international standards organizations have published the ISO/IEC 25000 series of standards for systems and software quality requirements and evaluation (SQuaRE), which is gaining widespread practical application. The paper discusses a series of the SQuaRE international standards, analyzes the relationship between the quality model, quality characteristics, quality measures and a new concept, i.e., a quality measure element of the software, presents the measurement of quality based on these standards.

Key words: quality; software; measurement; standard; quality measure.

1 tab. 3 fig. Ref: 10 items.

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 206
Українською, російською, та англійською мовами

СБОРНИК НАУЧНЫХ ТРУДОВ
РАДИОТЕХНИКА
Выпуск 206
На украинском, русском и английском языках

COLLECTION OF SCIENTIFIC PAPERS
RADIOTEKHNIKA
Issue 206
In Ukrainian, Russian and English

Коректор Л.І. Сащенко

Підп. до друку 24.09.2021. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк. 10,4. Обл.-вид. арк. 9,36. Тираж 300 прим. Зам. № 478. Ціна договір.

Харківський національний університет радіоелектроніки (ХНУРЕ)
Просп. Науки, 14, Харків, 61166.

Оригінал-макет підготовлено і збірник надруковано у ПФ „Колегіум”, тел. (057) 703-53-74.
Свідоцтво про внесення суб’єкта видавничої діяльності до Державного реєстру видавців.
Сер. ДК №1722 від 23.03.2004.