УДК 004

Є.Одинцов, магістр гр. КН-22М-1
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ СТАТИСТИЧНОГО АНАЛІЗУ ТА ФІЛЬТРАЦІЇ ДАНИХ ЗІ ЗМІННИХ НОСІЇВ

У статті розроблено програмне забезпечення, яке призначено для системи статистичного аналізу та фільтрації даних зі змінних носіїв. Метою розробки є дослідження та програмна реалізація системи статистичного аналізу та фільтрації даних зі змінних носіїв. Об'єктом дослідження є процес статистичного аналізу та фільтрації даних зі змінних носіїв. Предметом дослідження є методи статистичного аналізу та фільтрації даних зі змінних носіїв. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи статистичного аналізу та фільтрації даних зі змінних носіїв. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Електронні стеганографічні методи можуть бути використані для кодування сигналу керування керуванням правами в інформаційний сигнал, що передається по незахищеному каналу зв'язку за допомогою змінних носіїв. Стеганографічні методи гарантують, що цифрова керуюча інформація практично непомітно і практично незмивно передається інформаційним сигналом. Ці методи можуть забезпечити наскрізний захист прав керування інформаційним сигналом незалежно від перетворень між аналоговим і цифровим. Електронний пристрій може відновлювати керуючу інформацію та використовувати її для електронного керування правами для забезпечення сумісності з віртуальним середовищем розповсюдження. В одному прикладі система кодує покажчики низької швидкості передачі даних у періоди часу сигналу вмісту з високою пропускною здатністю, щоб покращити загальний час читання/пошуку керуючої інформації.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи статистичного аналізу та фільтрації даних зі змінних носіїв.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи статистичного аналізу та фільтрації даних зі змінних носіїв.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем статистичного аналізу та фільтрації даних зі змінних носіїв.

– Дослідження системи статистичного аналізу та фільтрації даних зі змінних носіїв.

– Програмна реалізація системи статистичного аналізу та фільтрації даних зі змінних носіїв.

Об'єктом дослідження є процес статистичного аналізу та фільтрації даних зі змінних носіїв.

Предметом дослідження є методи статистичного аналізу та фільтрації даних зі змінних носіїв.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Дана робота може забезпечувати віртуальне середовище розповсюдження ("VDE"), в якому електронна керуюча інформація управління правами може бути доставлена через незахищені (наприклад, аналогові) канали зв'язку. Це віртуальне середовище розповсюдження є дуже гнучким і зручним, враховуючи існуючі та нові бізнес-моделі, а також забезпечуючи безпрецедентний ступінь гнучкості в сприянні спеціальному створенню нових домовленостей і відносин між електронною комерцією та учасниками ланцюга створення вартості – незалежно від того, чи вміст розповсюджується в цифрові та/або аналогові формати.

Дана робота додатково забезпечує наступні важливі та переваги:

– Незмивна та невидима безпечна техніка для надання інформації про керування правами.

– Незмивний метод зв’язування елементів електронної комерції та/або керування правами з аналоговим вмістом, таким як фільми, відео та звукозаписи.

– Постійний зв’язок елементів керування торгівлею та/або керуванням правами з вмістом від одного кінця системи розповсюдження до іншого – незалежно від кількості та типів перетворень між форматами сигналізації (наприклад, з аналогового на цифровий і з цифрового на аналоговий).

– Можливість вказати правила управління правами «без копіювання/одна копія/багато копій», а також більш складні моделі прав і ціноутворення транзакцій (такі як, наприклад, «оплата за перегляд» та інші).

– Можливість повної та бездоганної інтеграції з комплексними загальними електронними рішеннями для керування правами (такими як ті, що розкриті в патентній специфікації Гінтера та інших, згаданій вище).

– Безпечна доставка керуючої інформації в поєднанні з авторизованими аналоговими та іншими нецифровими та/або незахищеними механізмами доставки інформаційних сигналів.

– Можливість забезпечувати більш складні та/або більш гнучкі правила комерції та/або керування правами під час переходу вмісту з аналогової до цифрової сфери й назад.

– Гнучка здатність передавати правила торгівлі та/або керування правами, які впроваджують нові, оновлені чи додаткові бізнес-моделі, авторизованим аналоговим та/або цифровим пристроям.

Коротко кажучи, у цих роботах використовується «стеганографія» для фактично незмивного та практично непомітного кодування керування правами та/або правил електронної комерції та контролю в інформаційному сигналі, такому як, наприклад, аналоговий сигнал або оцифрована (наприклад, дискретизована) версія аналоговий сигнал.

Грецький термін «стеганографія» стосується різних методів секретного спілкування «прихованого письма», які дозволяють надійно передавати важливі повідомлення незахищеними каналами зв’язку. Ось кілька прикладів стеганографії:

У стародавній Персії важливе повідомлення колись було витатуйовано на поголеній шкірі голови довіреного посланця. Потім посланець дозволив своєму волоссю відростити, повністю приховавши повідомлення. Коли посланець дістався місця призначення, він знову збрив волосся, відкривши секретне повідомлення, щоб одержувач міг прочитати його на поголеній шкірі посланця. Див. Kahn, David, The Codebreakers, сторінка 81 і далі. і сторінка 513 і далі. (Макміллан 1967). Ця незвичайна техніка приховування повідомлення є однією з ілюстрацій «стеганографії».

Інша «стеганографічна» техніка кодує секретне повідомлення в іншому, звичайному повідомленні. Наприклад, повідомлення «Hey Elmer, Lisa Parked My Edsel» кодує секретне повідомлення «HELP ME» – перша літера кожного слова повідомлення, що утворює літери секретного повідомлення («Hey Elmer, Lisa Parked My Edsel»). Варіанти цієї методики можуть забезпечити додатковий захист, але основна концепція та сама – знайти спосіб приховати секретне повідомлення в інформації, яка може або буде надіслана незахищеним каналом.

Невидимі чорнила – це ще одна широко використовувана техніка «стеганографії». Секретне повідомлення пишеться за допомогою спеціального зникаючого або невидимого чорнила. Повідомлення можна написати на чистому аркуші паперу або, як правило, на зворотному чи лицьовому боці аркуша паперу, на якому міститься звичайний або законний лист або інше письмове повідомлення. Одержувач виконує спеціальний процес над отриманим документом (наприклад, піддає його хімічному або іншому процесу, який робить невидимі чорнила видимими), щоб він чи вона могли прочитати повідомлення. Будь-хто, хто перехопить папір, не зможе виявити таємне повідомлення – або навіть знати, що воно там – якщо перехоплювач не знає, що потрібно шукати невидиме повідомлення, а також не знає, як поводитися з папером, щоб зробити невидиме чорнило видимим

У цих роботах використовується стеганографія, щоб гарантувати, що закодована керуюча інформація є як практично невидимою, так і практично незмивною, коли вона проходить по незахищеному каналу зв'язку. На приймальній стороні захищений надійний компонент (наприклад, захищене середовище обробки, описане в Ginter та ін.) відновлює стеганографічно закодовану керуючу інформацію та використовує відновлену інформацію для керування електронними правами (наприклад, на аналоговому або іншому інформаційні сигнали, що передаються по одному каналу).

Один конкретний аспект, наданий цією роботою, включає стеганографічне кодування інформації керування цифровими правами в інформаційний сигнал, такий як, наприклад, аналоговий або оцифрований телевізійний, відео- або радіосигнал. Процес стеганографічного кодування по суті нерозривно переплітає цифрову керуючу інформацію з зображеннями, звуками та/або іншим вмістом, який несе інформаційний сигнал, але переважно без помітного погіршення або іншого впливу на ці зображення, звуки та/або інший вміст. Може бути важко виявити (навіть за допомогою освічених методів обробки сигналів), що аналоговий сигнал був стеганографічно закодований за допомогою контрольного сигналу керування правами, і може бути важко усунути стеганографічно закодований керуючий сигнал без руйнування або погіршення іншої інформації чи вмісту сигнал несе.

Дана робота також забезпечують безпечне, надійне захищене середовище обробки для відновлення стеганографічно закодованого керуючого сигналу з інформаційного сигналу та для забезпечення процесів керування правами на основі відновленого стеганографічно закодованого керуючого сигналу. Це дозволяє повністю інтегрувати (і зробити сумісним) механізм доставки інформаційного сигналу з цифровим віртуальним середовищем розповсюдження та/або іншою електронною системою керування правами.

Відповідно до ще одного аспекту, наданого цією роботою, стеганографічно закодована керуюча інформація управління цифровими правами може використовуватися разом із скремблованим і/або зашифрованим інформаційним сигналом. Скремблювання та/або шифрування можна використовувати для забезпечення управління правами, наданого відповідно до стеганографічно закодованої інформації керування керуванням правами. Наприклад, керуючий сигнал може бути стеганографічно декодований і використаний для контролю, принаймні частково, за яких обставин і/або як інформаційний сигнал повинен бути дешифрований і/або дешифрований.

Відповідно до ще однієї ознаки, наданої винаходом, цифрові сертифікати можуть використовуватися для безпечного забезпечення дотримання стеганографічно закодованої інформації керування правами.

Відповідно до ще однієї ознаки, наданої винаходом, стеганографія використовується для кодування інформаційного сигналу з інформацією управління правами у формі однієї або більше захищених організаційних структур, пов'язаних з електронними засобами керування. Електронні засоби керування можуть, наприклад, визначати дозволені та/або необхідні операції з вмістом, а також наслідки виконання та/або невиконання таких операцій. Організаційна(-і) структура(-и) може(-ють) ідентифікувати, неявно чи явно, вміст, до якого застосовуються електронні елементи керування. Організаційна(і) структура(и) також може визначати обсяг контенту та семантику контенту.

Тип, обсяг і характеристики стеганографічно закодованої інформації керування правами є гнучкими та програмованими, забезпечуючи багатий, різноманітний механізм для розміщення широкого спектру схем керування правами. Інформацію про керування можна використовувати для безпечного застосування простих наслідків безпечного керування правами, наприклад елементів керування типу «копіювання/без копіювання/одна копія», але жодним чином не обмежується такими моделями. Навпаки, даний винахід може бути використаний для того, щоб увімкнути та застосувати набагато багатші, складніші моделі керування правами, включаючи, наприклад, такі, що включають аудит використання, автоматичні електронні платежі та використання додаткових електронних мережевих з'єднань. Крім того, механізми контролю керування правами, надані цією роботою, можна нескінченно розширювати та масштабувати - повністю адаптувати майбутні моделі, коли вони комерційно розгортаються, зберігаючи при цьому повну сумісність з різними (і, можливо, більш обмеженими) моделями керування правами, розгорнутими на попередніх етапах.

Організаційна(і) структура(и) може бути стеганографічно закодована таким чином, щоб вона була захищена з метою забезпечення секретності та/або цілісності. Застосовувані стеганографічні методи можуть забезпечувати певний ступінь захисту секретності або інші методи безпеки (наприклад, цифрове шифрування, цифрові печатки тощо) можуть бути використані для забезпечення бажаного або необхідного рівня безпеки та/або захисту цілісності стеганографічно закодованого інформації.

В одному прикладі організаційна(і) структура(и) може включати цифрові електронні контейнери, які безпечно містять відповідну цифрову електронну керуючу інформацію. Такі контейнери можуть, наприклад, використовувати криптографічні методи. В інших прикладах організаційна(і) структура(и) може визначати асоціації з іншою електронною керуючою інформацією. Інша електронна керуюча інформація може надаватися незалежно через той самий або інший шлях зв'язку, який використовується для доставки організаційної структури(-й).

В одному прикладі використовувані стеганографічні методи можуть передбачати застосування інформації про організаційну структуру у формі високочастотного "шуму" до аналогового інформаційного сигналу. Спектральні перетворення можуть бути використані для застосування та відновлення такого стеганографічно закодованого високочастотного "шуму". Оскільки високочастотні шумові компоненти інформаційного сигналу можуть бути по суті випадковими, додавання псевдовипадкового стеганографічно закодованого компонента керуючого сигналу може практично не призвести до помітного погіршення інформаційного сигналу, і його може бути важко видалити після введення (принаймні без додаткових знань про як сигнал був включений, який може містити спільний секрет).

Відповідно до іншого аспекту, передбаченого винаходом, процес стеганографічного кодування аналізує інформаційний сигнал, щоб визначити, яка надлишкова смуга пропускання доступна для стеганографічного кодування. Процес стеганографічного кодування може використовувати кодування зі змінною швидкістю передачі даних, щоб застосувати більше керуючої інформації до частин інформаційного сигналу, які використовують набагато менше, ніж уся доступна смуга пропускання каналу зв'язку, і застосувати менше керуючої інформації до частин інформаційного сигналу, які використовують майже всі доступної пропускної здатності каналу зв'язку.

Відповідно до ще одного аспекту, наданого винаходом, численні організаційні структури можуть бути стеганографічно закодовані в межах даного інформаційного сигналу. Кілька організаційних структур можуть застосовуватися до різних відповідних частин інформаційного сигналу, і/або численні організаційні структури можуть бути повторами або копіями одна одної, щоб гарантувати, що електронний пристрій має «пізній вхід» і/або здатність виправляти помилки та/або може швидко знайти відповідну організаційну структуру (структури), починаючи з будь-якої довільної частини потоку інформаційного сигналу.

Відповідно до ще одного аспекту, передбаченого цією роботою, організаційна структура може бути стеганографічно закодована в конкретній частині інформаційного сигналу, що несе вміст, до якого застосовується організаційна структура, таким чином встановлюючи неявну відповідність між організаційною структурою та ідентифікацією та /або обсяг і/або семантика інформаційного вмісту, до якого застосовується організаційна структура. Кореспонденція може, наприклад, включати явні компоненти (наприклад, внутрішньо визначені початкові/кінцеві точки), зі сховищем або іншим фізичним зв'язком, визначеним для зручності (тобто може мати сенс розмістити організаційну структуру поблизу місця її використання, щоб не шукати носій інформації, щоб знайти його).

Відповідно до ще одного аспекту, забезпеченого цією роботою, покажчики можуть бути стеганографічно закодовані в частини потоку інформаційного сигналу, який має невелику надлишкову доступну смугу пропускання. Такі вказівники можуть використовуватися, наприклад, для спрямування електронного пристрою на частини потоку інформаційного сигналу, які мають більш доступну смугу пропускання для стеганографічного кодування. Такі покажчики можуть забезпечувати покращений час доступу до стеганографічного декодування - особливо, наприклад, у програмах, у яких потік інформаційних сигналів зберігається або іншим чином доступний на основі довільного доступу.

Розробка структурної схеми

Структурна схема розробленої системи зображена на рисунку 1. З метою вдосконалювання теоретичної бази проведений загальний аналіз стеганографічних методів і алгоритмів, використовуваних на справжній момент у програмних засобах схованої передачі електронних документів, з використанням змінних носіїв. Досліджено специфічні уразливості програмних засобів і систем схованої передачі електронних документів. Уведено загальну класифікацію атак на стеганографічні системи зв'язку залежно від використовуваних для проведення атак уразливостей. Крім того велика увага приділена також і сучасним моделям стеганографічних систем зв'язку, представленим у різних публікаціях і узагальненим за результатами аналізу існуючого програмного забезпечення.

У результаті проведеного аналізу відомих методів, моделей систем і програмних засобів виявлені наступні загальні недоліки існуючих рішень в області стеганографічного методу збереження конфіденційності інформації:

– відсутність загальних єдиних підходів і пророблених базових рішень до побудови стеганографічних систем;
– низька стійкість до різних методів стеганоаналізу;
– низька стійкість до руйнуючих впливів;
– низька перешкодозахищеність;
– сильна залежність ступеня скритності від особливостей контейнера;
– відсутність методів оцінки рівня надійності й докази стійкості до атак пасивного зловмисника;
– слабість застосовуваних алгоритмів перетворення повідомлень;
– складність перебудови стеганографічних алгоритмів залежно від використовуваного ключа приховання;
– складність побудови надійних систем із симетричними й відкритими ключами;
– загальна надійність систем сильно залежить від обсягів приховуваної інформації.

Комерційне використання програмних засобів ЗІ крім іншого накладає додаткові обмеження, що стосуються в першу чергу забезпечення можливості широкого поширення програмних продуктів.

Таким чином, для стеганографічних методів методу збереження конфіденційності інформації в системах електронного документообігу з використанням змінних носіїв першорядними стають питання забезпечення теоретичної й практичної стійкості. Найбільш перспективним у цьому напрямку, з огляду на сучасний стан теоретичної бази, бачиться побудова гібридних систем схованої передачі електронних документів на основі щільної

взаємодії або навіть синтезу методів криптографії й стеганографії. За результатами проведених досліджень пропонується сформулювати вимоги до криптографічного й стеганографічного алгоритмів, розробити методи й алгоритми їхнього узгодження, проробити відповідну теоретичну базу. Крім того, з огляду на малу пропрацьованість питань, що стосуються стеганографічних методів методу збереження конфіденційності інформації й ефективної протидії методам стеганоаналізу, пропонується приділити їм першорядне значення.

Проведений аналіз показав, що всі відомі методи стеганоаналізу мають певні границі застосовності, чутливості й вірогідності результатів. На справжній момент існує реальна можливість побудови стеганографічних методів, які мали би абсолютну стійкість до відомих методів аналізу, тобто були б не виявляємі.

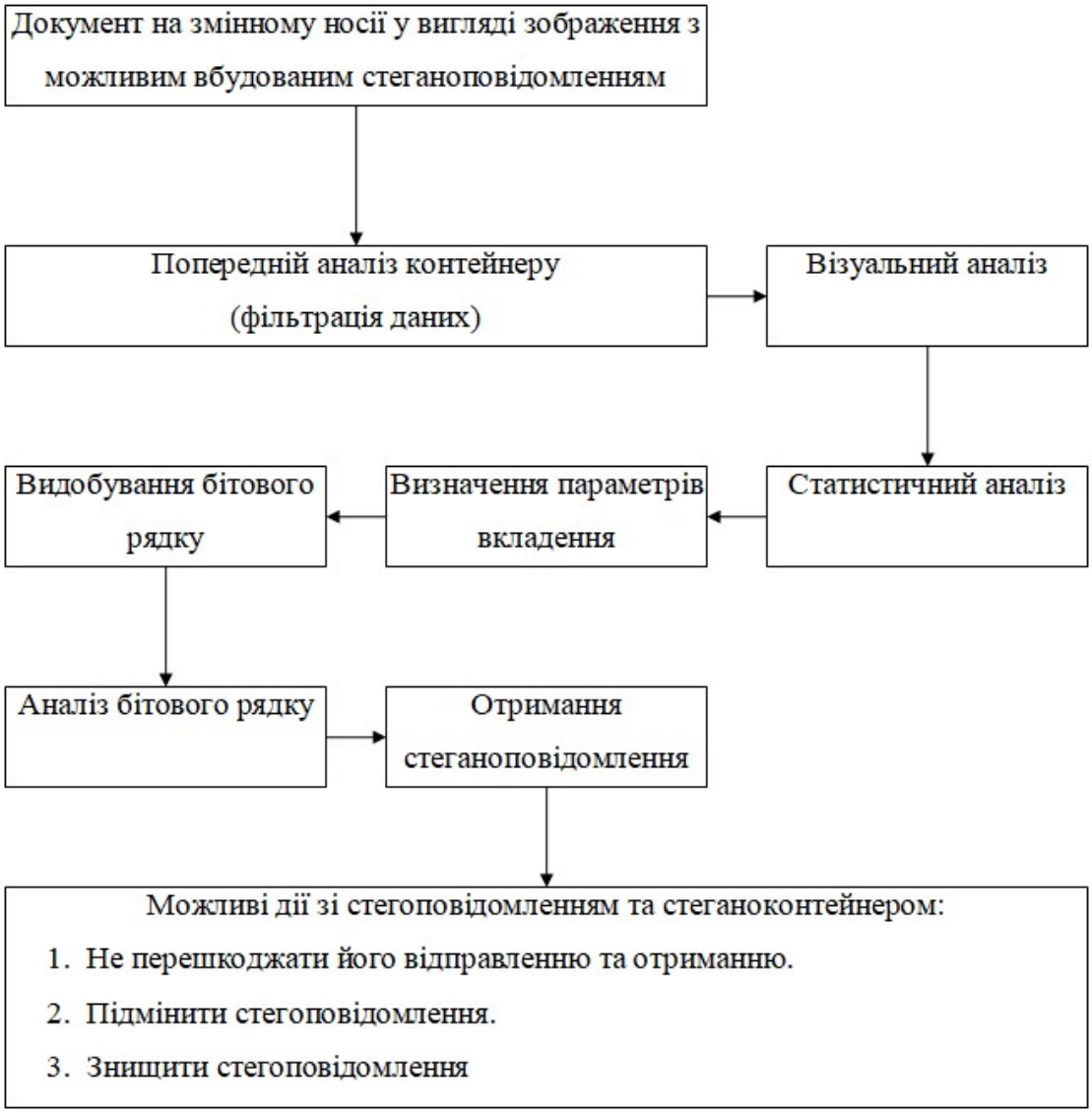

Рисунок 1 – Структурна схема системи

Цікавим фактом є те, що з урахуванням деяких обмежень ряд існуючих стеганографічних методів є, що виявляються не при вбудовуванні зверхмалих обсягів інформації. Даний факт обумовлений тим, що навіть найсучасніші методи аналізу мають певні пороги чутливості. Так, якщо після вбудовування повідомлення аналізовані показники контейнера перебувають у межах припустимих погрішностей, він буде прийнятий за порожній. Крім зазначених висновків за результатами аналізу в першій частині були також сформульовані пропозиції по протидії сучасним методам стеганоаналізу.

Дані пропозиції рекомендується враховувати при побудові нових стеганографічних методів.

Криптостеганографічною системою будемо називати систему схованої передачі інформації на відкритих каналах зв'язку, засновану на спільному застосуванні криптографічних алгоритмів, стеганографічних методів, а також алгоритмів узгодження вхідних і вихідних даних зазначених алгоритмів і методів.

Криптографічна частина (E, D) забезпечує криптографічне закриття (попереднє шифрування) переданих повідомлень. Відповідає за перетворення переданих повідомлень до псевдовипадкового виду з рівномірним розподілом.

Стеганографічна частина (S) здійснює безпосереднє приховання й добування переданих даних, що пройшли процедуру попереднього шифрування, у контейнерах з C.

Алгоритми узгодження (MT) забезпечують узгодження криптографічної й стеганографічної частин системи по вхідним і вихідним даним. Відповідають за пряме приведення й зворотне перетворення отриманих з виходу криптографічної частини даних до двійкових послідовностей, аналогічним по своїх статистичних властивостях двійковим послідовностям, що витягається з порожніх контейнерів.

Модель криптостеганографічної системи представлена на рисунку 1. Для даної моделі криптостеганографічної системи зв'язку розглянуті можливості зловмисника по виявленню схованого каналу й добуванню схованих повідомлень. Показано, що при виконанні ряду вимог до компонентів системи успішна атака на системи даного виду можлива лише у випадку успішної атаки на криптографічні алгоритми. Тобто стійкість системи до атак пасивного зловмисника визначається стійкістю до злому криптографічної частини.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів статистичного аналізу та фільтрації даних зі змінних носіїв. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем статистичного аналізу та фільтрації даних зі змінних носіїв; Досліджена система статистичного аналізу та фільтрації даних зі змінних носіїв; На основі отриманих результатів досліджень створена програмна реалізація системи статистичного аналізу та фільтрації даних зі змінних носіїв. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання статистичного аналізу та фільтрації даних зі змінних носіїв. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Frontoni, E., Kandiy, S., Smirnov, O., Ulianovska, Y., Kobylianska, O. «Heuristic Search for Nonlinear Substitutions for Cryptographic Applications». Lecture Notes on Data Engineering and Communications Technologies, 2023. vol 180. Springer, Cham. pp. 288-298.
2. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the Age of ASIC Resistance». CEUR Workshop Proceedings, 2023, 3628, pp. 93-105.
3. Kuznetsov O., Frontoni E., Kuznetsova Ye., Smirnov O., Chevardin V. «Achieving Enhanced Security in Biometric Authentication: A Rigorous Analysis of Code-Based Fuzzy Extractor». CEUR Workshop Proceedings, Volume 3624, 2023, pp. 330-339.
4. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
5. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». CEUR Workshop Proceedings, Volume 3504, 2023, pp. 1-11.
6. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
7. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp.

21-34.
8. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
9. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
10. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
11. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.
12. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58.
13. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
14. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
15. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
16. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131.
17. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14.
18. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84.
19. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.
20. Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I.,Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 166-171.
21. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
22. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
23. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
24. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43.
25. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.