УДК 004

В.Кострик, магістр гр. КН-22М-1
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ОБМІНУ ІНФОРМАЦІЄЮ У МЕРЕЖІ НА ОСНОВІ ПРОТОКОЛУ SIGNAL

У статті розроблено програмне забезпечення, яке призначено для системи обміну інформацією у мережі на основі протоколу Signal. Метою розробки є дослідження та програмна реалізація системи обміну інформацією у мережі на основі протоколу Signal. Об'єктом дослідження є процес обміну інформацією у мережі на основі протоколу Signal. Предметом дослідження є методи обміну інформацією у мережі на основі протоколу Signal. Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи обміну інформацією у мережі на основі протоколу Signal. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Спілкування змінилося раз і назавжди, коли люди почали використовувати гаджети та програми для здійснення дзвінків та обміну текстовими повідомленнями. На перший погляд все чудово. Ми можемо спілкуватися з іншими людьми з будь-якої точки світу та витрачати менше грошей на міжнародні дзвінки. Всі перераховані вище фактори сприяють популярності месенджерів.

Однак є певні недоліки, які підривають нашу довіру до зазначених месенджерів – конфіденційність і безпека даних. Ось чому захищені програми обміну повідомленнями стають дедалі популярнішими. Програма для обміну повідомленнями Signal, популярне рішення для обміну зашифрованими повідомленнями, є чудовим прикладом того, як зробити спілкування безпечним

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-20] було виявлено певні прогалини у забезпеченні системи обміну інформацією у мережі на основі протоколу Signal.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи обміну інформацією у мережі на основі протоколу Signal.

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

– Огляд існуючих систем обміну інформацією у мережі на основі протоколу Signal.
– Дослідження системи обміну інформацією у мережі на основі протоколу Signal.
– Програмна реалізація системи обміну інформацією у мережі на основі протоколу Signal.

Об'єктом дослідження є процес обміну інформацією у мережі на основі протоколу Signal.

Предметом дослідження є методи обміну інформацією у мережі на основі протоколу Signal.

Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Програми обміну повідомленнями мають мільярди користувачів по всьому світу. За даними дослідження Messenger People, база користувачів

WhatsApp і Facebook Messenger нараховує 1,5 мільярда користувачів у всьому світі. Це означає, що дані мільйонів користувачів знаходяться під загрозою зламу.

Щороку відбувається багато порушень даних. Business Insider заявляє, що в 2018 році особиста інформація мільйонів людей по всьому світу була скомпрометована.

Безпека програми Signal є головною проблемою для розробників, які стоять за програмою. Ось чому програма використовує наскрізне шифрування, оскільки це означає, що всі повідомлення шифруються перед надсиланням і можуть бути розшифровані лише на пристрої одержувача. Єдиний спосіб прочитати повідомлення – на пристрої відправника або одержувача.

Програма приватного обміну повідомленнями Signal покладається на такі криптографічні протоколи:

– Розширений потрійний Діффі-Хеллман (X3DH).
– Алгоритм Double Ratchet, Curve25519.
– AES-256.
– HMAC-SHA256.

Застосовувані протоколи забезпечують захист від MITM (man-in-the-middle).

Після одного конкретного оновлення Signal усі голосові та відеодзвінки були захищені тим самим протоколом Signal, який використовувався для захисту лише текстових повідомлень. Цей протокол був розроблений у 2013 році компанією Open Whisper Systems і вперше реалізований у додатках TextSecure×, на основі яких пізніше було розроблено додаток для обміну повідомленнями Signal.

Шифрування сигналу також надає користувачам додаткові функції безпеки, такі як захист повідомлень і сповіщень за допомогою парольної фрази. Клавіатура працює в режимі інкогніто і не збирає дані про те, який текст набирається. Крім того, повідомлення про зникнення сигналу досить корисні, як і ті, які використовує Snapchat.

Додаток для обміну повідомленнями Signal також надає механізм перевірки ідентичності ваших контактів за допомогою унікального безпечного номера (відбитка пальця).

Що саме означає бути в безпеці? За даними Electronic Frontier Foundation (EFF), існує сім критеріїв для оцінки того, наскільки безпечним є додаток для чату. Вони є:

– зв'язок, зашифрований під час передачі;
– жоден провайдер не має доступу до ключа, за допомогою якого зашифровано зв’язок;
– незалежна перевірка особи кореспондента;
– захистити минулі комунікації, якщо ключі будуть вкрадені;
– код відкритий для незалежного перегляду;
– добре задокументований криптографічний дизайн;
– незалежний аудит безпеки.

На відміну від інших додатків, месенджер Signal відповідає всім стандартам. Крім того, нижче ви можете побачити оцінку безпеки програми для обміну зашифрованими повідомленнями Signal у порівнянні з іншими програмами для чату:

Разом із ідеєю розробки власного додатка для однорангового чату ви також повинні враховувати всі ризики та можливості, які це може принести. Основною особливістю приватного месенджера Signal є зашифрований обмін повідомленнями, але він, безперечно, має більше функцій, про які варто згадати. Фактично, програма може виконати всі вимоги навіть для найвибагливіших користувачів:

– Реєстрація за номером телефону. Зручність – головне, а коли справа доходить до реєстрації, усе стає ще простіше, коли вам не потрібно запам’ятовувати паролі чи дані для входу. Ось чому програма обміну повідомленнями Signal використовує номер телефону та код підтвердження для перевірки реєстрації та входу користувача.

– Повідомлення, що зникають. Користувач може встановити таймер від 5 секунд до 1 тижня для зникнення всіх побачених повідомлень. Неможливо навіть зробити скріншот чату,

тому що програма просто не дозволяє це зробити. Однак push-сповіщення з повідомленнями про зникнення Signal (незалежно від того, зникає воно чи ні) можна зробити за допомогою знімка екрана, оскільки безпека програми для обміну повідомленнями Signal, яка працює у фоновому режимі, не може блокувати стандартні функції пристрою.

– Голосові та відеодзвінки. Додаток для обміну повідомленнями Signal надає своїм користувачам можливість здійснювати кришталево чисті та безпечні голосові та відеодзвінки, що робить додаток придатним для ділового спілкування.

– Групові чати. За допомогою безпечних чатів «один на один» користувачі можуть вести приватні зашифровані розмови зі своїми друзями. Крім того, сервер програми обміну повідомленнями Signal не має доступу до будь-яких метаданих груп, включаючи піктограми, заголовки та списки учасників.

– Обмін контентом і розваги. Оскільки додаток для обміну повідомленнями Signal досить популярний, він ніколи не припиняє розвиватися та впроваджувати нові функції. Поки що програма безпечного чату дозволяє користувачам ділитися не тільки текстами, але й гіфками, фотографіями, відео, місцезнаходженням, будь-яким документом чи файлом і навіть голосовими повідомленнями (це дуже зручно для швидкого обміну інформацією).

– Особливості платформи. На Android користувачі можуть встановити приватний месенджер Signal як програму за замовчуванням для SMS/MMS, яка дозволяє надсилати та отримувати SMS-повідомлення користувачам, які не є користувачами Signal, або за відсутності підключення до Інтернету. Єдине застереження полягає в тому, що ці повідомлення не шифруються.

– Безпека та шифрування. Впровадження протоколів безпеки – завдання не з легких, скоріше, потребує величезних зусиль. Однак є кілька порівняно простіших варіантів. Один із них, наприклад, використовує Telegram API (ще один безпечний додаток для чату). Перевагою є те, що вам не потрібно розробляти бек-енд і базу даних, що заощадить ваш час і гроші. Це рішення також має свої недоліки; у вас немає доступу до бази даних або контролю над нею, тому неможливо змінити потік або бути на 100% впевненим у безпеці даних користувача.

Відсутність наскрізного шифрування не означає, що вся ваша історія чату буде пошкоджена та використана з поганими намірами. Насправді, на відміну від додатка для обміну повідомленнями Signal, багато відомих месенджерів отримали свою популярність і базу користувачів без впровадження суперпротоколів безпеки. Візьмемо, наприклад, такі гіганти, як Facebook Messenger і WhatsApp, які лише нещодавно стали шифруватись за допомогою протоколу Signal (розробленого Open Whisper Systems).

Більшість із нас не часто ділиться дуже конфіденційними даними у своїх повідомленнях. Однак наскрізне шифрування служить додатковим заходом безпеки, коли ви надсилаєте будь-яку особисту інформацію, як-от платіжні дані, номери соціального страхування, імена користувачів, паролі тощо. Наскрізне шифрування сигналу та зникнення повідомлень можуть дати вам спокій і впевненість у безпеці даних.

Конфіденційні дані користувача можуть бути викрадені або, що ще гірше, використані шантажистами чи оприлюднені. Таким чином, питання безпеки даних стає ще більш відчутним. І саме тут такі програми, як Signal, потрапляють у центр уваги.

Отже, що таке Signal і що робить його найбезпечнішим додатком для обміну повідомленнями? Приватний месенджер Signal був побудований на основі існуючих додатків RedPhone і TextSecure і був запущений у березні 2015 року компанією Open Whisper Systems. Він використовує протоколи обміну повідомленнями з наскрізним шифруванням (Curve25519, AES-256 і HMAC-SHA256), щоб захистити зв’язок і забезпечити відсутність атак MITM (людина посередині). Що також відрізняє його від інших програм для чату, так це те, що його вихідний код доступний на GitHub для всіх, хто хоче вивчити його або перевірити наявність недоліків у безпеці.

Але що саме означає бути в безпеці? За даними Electronic Frontier Foundation (EFF), існує сім критеріїв для оцінки того, наскільки безпечним є додаток для чату. Вони є:

– передача зашифрована;
– відсутність доступу провайдера до зашифрованого ключа;
– незалежна перевірка особи кореспондента;
– захистити минулі комунікації, якщо ключі будуть вкрадені;
– код відкритий для незалежного перегляду;
– добре задокументований криптографічний дизайн;
– незалежний аудит безпеки.

Відповідно до цих критеріїв, Signal вважається гравцем А.

Як розробити безпечну програму обміну миттєвими повідомленнями, як-от Signal

Основною функцією програми Signal є обмін приватними миттєвими повідомленнями, але вона безумовно має більше функцій, про які варто згадати. Фактично, програма може виконати всі вимоги навіть для найвибагливіших користувачів.

Реєстрація за номером телефону

Зручність – головне, і коли справа доходить до реєстрації, стає набагато простіше, коли вам не потрібно запам'ятовувати паролі чи дані для входу. Ось чому Signal використовує надісланий номер телефону та код підтвердження для перевірки реєстрації або входу користувача.

Повідомлення, що зникають

Користувач може встановити таймер від 5 секунд до 1 тижня для зникнення всіх побачених повідомлень. Неможливо навіть зробити скріншот чату, тому що програма просто не дозволяє цього робити.

Голосові та відеодзвінки

Signal надає своїм користувачам можливість здійснювати кристально чисті та безпечні голосові та відеодзвінки, тому ця програма також підходить для ділового спілкування.

Групові чати

Разом із безпечними чатами «один на один» користувачі також можуть вести приватні зашифровані розмови зі своїми друзями. Крім того, сервер Signal не має доступу до будь-яких метаданих груп, включаючи значки, заголовки та списки учасників.

Обмін контентом і розваги

Signal ніколи не припиняє розвиватися та впроваджувати нові функції. Поки що додаток дозволяє ділитися не тільки текстом, але й gif-файлами, фото, відео, місцем розташування, будь-яким документом або файлом і навіть голосовими повідомленнями.

Особливості платформи

На Android користувачі можуть встановити Signal як програму для SMS/MMS за замовчуванням, яка дозволяє надсилати й отримувати SMS-повідомлення користувачам, які не користуються Signal, або якщо немає підключення до Інтернету. Єдине, що ці повідомлення не зашифровані.

Безпека та шифрування

Впровадження протоколів безпеки непросте завдання. Це вимагає величезних зусиль. Звичайно, є порівняно прості варіанти. Одним із них є, наприклад, використання Telegram API (ще одна безпечна програма для чату). Перевагою є те, що вам не потрібно буде розробляти бек-енд і базу даних, що заощадить ваш час і гроші. Але це рішення також має свої недоліки. Ви не матимете доступу до бази даних або контролю над нею, тому буде неможливо змінити потік або бути на 100% впевненим у безпечному розміщенні даних користувача.

Відсутність наскрізного шифрування не означає, що вся ваша історія чату буде пошкоджена та використана з поганими намірами. Насправді, багато відомих месенджерів починали і завойовували свою популярність і базу користувачів без впровадження суперпротоколів безпеки. Візьмемо для прикладу таких гігантів, як Facebook Messenger або WhatsApp, які почали шифруватися лише нещодавно за допомогою протоколу Signal (розробленого Open Whisper Systems).

Більшість із нас рідко ділиться конфіденційними даними у своїх повідомленнях. Однак наскрізне шифрування служить додатковим заходом безпеки, коли ви надсилаєте свою особисту інформацію, як-от платіжні дані, номер соціального страхування, ім'я користувача, пароль тощо. Отже, використання наскрізного шифрування та зникнення повідомлень може дати вам сердечність і впевненість.

Отже, скільки коштує розробка такого рішення, як додаток для обміну повідомленнями Signal? Ціна та терміни значною мірою залежатимуть від функцій, які зрештою матиме ваш месенджер, їхньої складності, дизайну програми (на основі власних або користувацьких елементів керування) і постачальника, якого ви наймете. Ці фактори ускладнюють надання точної оцінки, не знаючи деталей.

Існують сотні різноманітних програм для обміну повідомленнями, але лише кілька десятків із них здобули широку популярність і успіх. Просто клонувати існуючу програму для обміну повідомленнями Signal – не дуже гарна ідея сама по собі. Щоб успішно вийти на ринок, вам слід подумати про інноваційні та унікальні функції або розробити нішевий додаток. Іншими словами, зробити його відмінним від того, що вже існує – виділити його з натовпу. Візьміть найкращі практики приватного месенджера Signal і додайте свій власний штрих.

Давайте використаємо найпростіші функції, які має мати кожна програма для чату, щоб розрахувати мінімальний необхідний бюджет для такого рішення, як програма для обміну повідомленнями Signal. Вони включають наступне:

Реєстрація:

– Увійти за допомогою номера телефону.
– Підтвердження номера телефону.

Контакти:

– Доступ до всіх контактів.
– Сегментація контактів на ті, у яких встановлений месенджер і не встановлений.

Запрошення та обмін:

– Можливість запросити друзів або поширити інформацію за допомогою вбудованої функції обміну.

Чат:

– Обмін миттєвими повідомленнями один на один.
– Статуси повідомлень (прочитані, непрочитані).
– Редагувати або видаляти повідомлення.
– Надсилайте фотографії з галереї або камери.
– Push-повідомлення.

Додаткові можливості:

– Голосові повідомлення.
– Наклейки.

Розробляючи абсолютно новий безпечний чат-сервіс, слід враховувати, що приватний месенджер Signal не є єдиним у світі. Є деякі сильні конкуренти, такі як Telegram, WhatsApp, Google Allo та Facebook Messenger, і це лише деякі.

Незважаючи на однакову основну функціональність, кожна з цих програм має власні налаштування та унікальні функції, які роблять їх маяками в нескінченному океані програм.

Якщо ви вважаєте, що ваша ідея програми може принести користь користувачам і задовольнити їхні потреби, її однозначно варто спробувати.

Розробка структурної схеми

Структурна схема розробленого програмного забезпечення обміну інформацією у мережі на основі протоколу Signal зображена на рисунку 1.

Розроблене програмне забезпечення складається з наступних блоків:

Серверна частина:

– База даних користувачів.
– База даних інформації про користувачів.

– База даних оффлайн повідомлень.

Клієнтська частина:

– Головне меню.

– Блок авторизації.

– Блок відображення контактів.

– Блок налаштувань.

– Блок встановлення статусів.

– Блок пошуку.

– Блок обміну текстовими повідомленнями.

– Блок обміну мовною інформацією.

– Блок обміну відеоінформацією.

– Блок історії повідомлень по контактам.

У основі програмного забезпечення лежить протокол Signal. Signal – відкритий, але не вільний мережний протокол, що забезпечує обмін миттєвими й оффлайновими текстовими повідомленнями. У цей момент використовується для систем: AIM (компанія AOL, керована Time Warner).

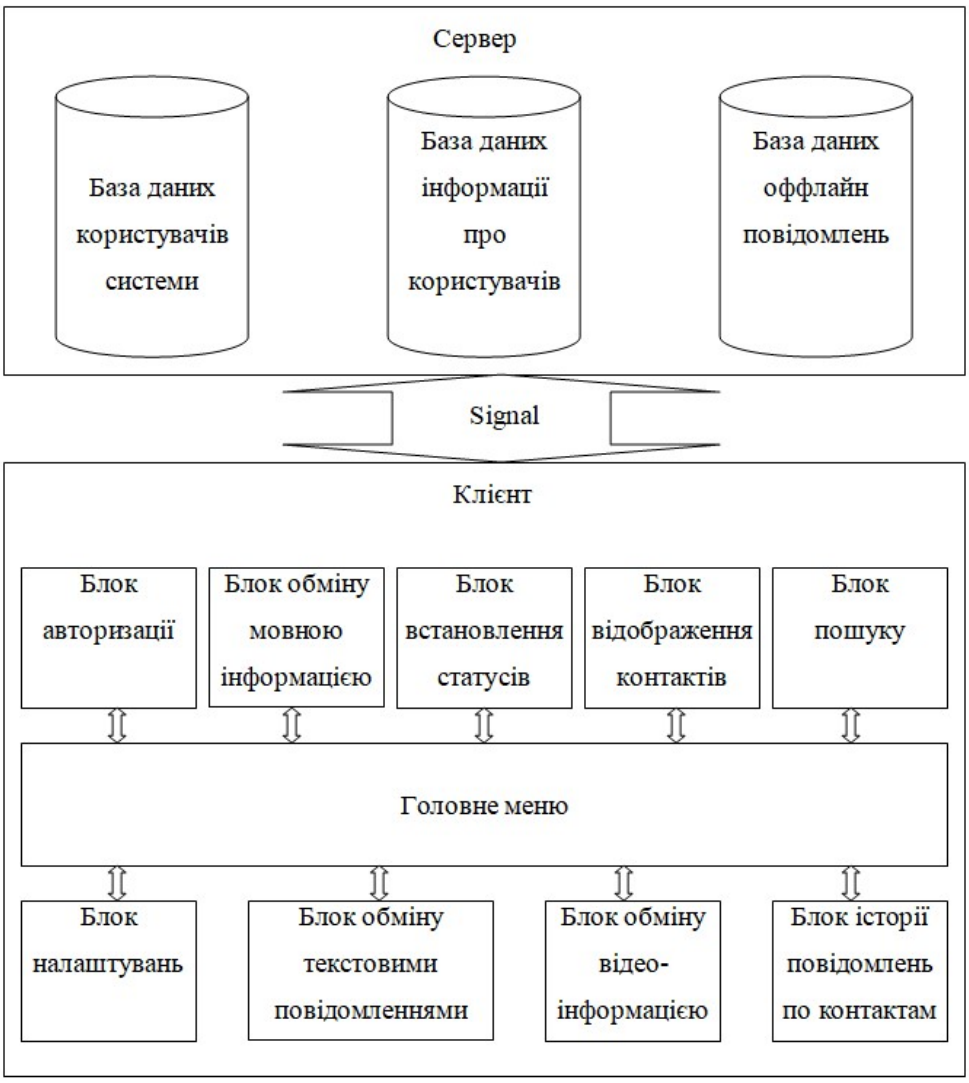

Рисунок 1 – Структурна схема системи

Особливості протоколу:

– Кожному користувачеві видається UIN (Unique Identification Number) – унікальний ідентифікаційний номер, по якому користувач однозначно визначається системою й іншими

користувачами. У цей час для сумісності з AIM замість UIN використовується поняття ScreenName.

– Користувач має можливість вибрати собі нік, що відіграє роль особистого імені в його повідомленнях. На відміну від UIN, ніки не унікальні для кожного користувача.

– В AOL Instant Messenger функцію UIN грають SN (Screen Name) – так звані екранні імена, унікальні для кожного користувача.

– Протокол підтримує кілька станів, у яких може перебувати користувач. Стани встановлюються користувачем.

Стани:

– Online – доступний.
– Free for chat (F4C) – вільний.
– Away – вдалині від комп'ютера (довго не працював).
– Not available (N/A) – недоступний.
– Occupied – зайнятий.
– Do not disturb (DND) – не турбувати.
– Invisible – не бачимий.
– Offline – відключений.

У програмах-клієнтах сторонніх розроблювачів деякі стани можуть бути відсутніми або мати місце додаткові.

Особливості програми

Програмна реалізація системи обміну інформацією у мережі на основі протоколу Signal надає всі функції, які ви очікуєте від найсучаснішого месенджера для організацій

Основні функції програми:

– Надсилайте текстові та голосові повідомлення.
– Здійснюйте голосові та відеодзвінки.
– Проведення групових дзвінків.
– Надсилайте файли будь-якого типу (PDF, Office документи тощо).
– Діліться фотографіями, відео та місцями.
– Використовуйте програму на робочому столі.

Особливості:

– Створіть опитування.
– Автоматично вимикати сповіщення в неробочий час.
– Мовчки погоджуйтеся або не погоджуйтеся з отриманими повідомленнями.
– Приховати конфіденційні чати та захистити їх паролем за допомогою PIN-коду або відбитка пальця (Android).
– Виберіть темну або світлу тему.
– Підтвердьте свої контакти за допомогою QR-коду.
– Додайте форматування тексту до повідомлень.
– Створення списків розсилки.
– Цитуйте текстові повідомлення

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів обміну інформацією у мережі на основі протоколу Signal. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем обміну інформацією у мережі на основі протоколу Signal; Досліджена система обміну інформацією у мережі на основі протоколу Signal; На основі отриманих результатів досліджень створена програмна реалізація системи обміну інформацією у мережі на основі протоколу Signal. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання обміну інформацією у мережі на основі протоколу Signal. 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. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
2. 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,
3. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheroz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». Sensors (Basel, Switzerland) Volume 22, Issue 16, 6223, 2022.
4. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. https://doi.org/10.1007/s42979-021-00739-w
5. 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.
6. 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.
7. 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.
8. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
15. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
16. 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.
17. Zhurakovskyi, B., Tsopa, N., Batrak, Y., Odarchenko, R., Smirnova, T «Comparative analysis of modern formats of lossy audio compression». Workshop Proceedings, 2020, 2654, стр. 315-327.
18. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
19. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
20. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 .P.517-522.
21. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.