УДК 004

Є.Прокопенко, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ АПАРАТНО-ПРОГРАМНИХ КОМПЛЕКСІВ ДЛЯ ВИЯВЛЕННЯ АТАК НА РІВНІ ІОТ-ПРИСТРОЇВ З ВИКОРИСТАННЯМ КВАНТОВАНИХ НЕЙРОМЕРЕЖ

У статті розроблено програмне забезпечення, яке призначено для автономного виявлення та протидії кібератакам у мережах Інтернету речей (IoT) за допомогою технологій Edge AI. Метою розробки є підвищення рівня захищеності мереж IoT шляхом розробки та реалізації апаратно-програмного комплексу виявлення вторгнень на основі адаптованих легковажих нейромереж. Об'єктом дослідження є процеси функціонування та обміну даними в мережах інтернету речей в умовах кібернетичного впливу та ресурсних обмежень апаратної платформи. Предметом дослідження є методи та апаратно-програмні засоби нейромережевого виявлення аномалій, оптимізовані для виконання на мікроконтролерах. Методи дослідження базуються на методах системного аналізу для визначення вимог до системи, теорії штучних нейронних мереж для побудови моделі класифікації трафіку, математичній статистиці та методах розробки вбудованого програмного забезпечення. Результат роботи – апаратно-програмна реалізація системи виявлення атак на базі мікроконтролера ESP32-S3 з використанням квантованих нейронних мереж. В процесі роботи над програмною моделлю виконано аналіз існуючих систем захисту IoT-інфраструктури, обґрунтовано вибір апаратної платформи з підтримкою векторних інструкцій та методів компресії моделей TinyML. В повній мірі описані всі компоненти розробленого програмного забезпечення.

виявлення та протидія кібератакам, Інтернет речей (IoT), Edge AI

Постановка проблеми. Швидке зростання кількості підключених пристроїв у глобальній мережі Інтернет речей (IoT) призводить до стрімкого збільшення векторів кібератак. Різноманітність пристроїв та використання спрощених протоколів обміну даними роблять цей сегмент вразливим до несанкціонованого втручання, що підтверджується зростанням кількості інцидентів, пов'язаних із ботнетами та DDoS-атаками [1, 2].

Для запобігання таких інцидентів необхідно захищати кінцеві вузли, які функціонують в умовах жорстких апаратних обмежень (енергоспоживання, обчислювальна потужність, обсяг пам'яті). Традиційні засоби захисту, такі як класичні системи виявлення вторгнень (IDS) або антивірусне програмне забезпечення, не можуть бути ефективно розгорнуті на мікроконтролерах через високі вимоги до ресурсів системи.

Враховуючи що перенесення функцій аналізу безпеки у хмарне середовище створює деяккі затримки в реакції на інциденти та залежність від стабільності каналу зв'язку. Перспективним напрямом вирішення цієї проблеми є концепція Edge AI (граничний штучний інтелект), що передбачає виконання алгоритмів машинного навчання безпосередньо на кінцевому пристрої. Застосування оптимізованих легковагих нейронних мереж дозволяє забезпечити автономне виявлення аномалій у мережевому трафіку в реальному часі.

Таким чином, дослідження та реалізація апаратно-програмного комплексу для виявлення атак на рівні IoT-пристроїв з використанням легковагих нейромереж є актуальною науково-прикладною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні дослідження та реалізація апаратно-програмних комплексів для виявлення атак на рівні iot-пристроїв з використанням квантованих нейромереж.

Мета й завдання дослідження. Метою роботи є підвищення рівня захищеності мереж IoT шляхом розробки та реалізації апаратно-програмного комплексу виявлення вторгнень на основі адаптованих ейзеносних нейромереж.

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

1. Провести огляд існуючих систем виявлення вторгнень в IoT та методів розгортання нейромереж на мікроконтролерах.
2. Обґрунтувати вибір апаратної платформи та програмних засобів для реалізації граничних обчислень.
3. Розробити структурну та функціональну схеми комплексу виявлення атак на базі вибраного мікроконтролера.
4. Здійснити програмну реалізацію модуля інференсу нейронної мережі з використанням векторних інструкцій для аналізу трафіку в реальному часі.
5. Провести експериментальне дослідження ефективності розробленого комплексу при виявленні типових мережевих атак.

Виклад основного матеріалу. Ініціалізація комплексу та конфігурація пам’яті

При своєму запуску система ініціює виконання завантажувача другого рівня. Для цього важливим етапом ініціалізації є розгортання карти пам’яті відповідно до попередньо визначеної таблиці розділів. Це потрібно задля стабільності роботи нейромережі та можливості оновлення прошивки «по повітрю». Нами була використана схема розмітки Flash-пам’яті на 4 мегабайти яка наведена в таблиці 1.

Таблиця 1 – Розподіл простору Flash-пам’яті

Тип	Підтип	Зсув	Розмір	Призначення
data	nvs	0x9000	20 КБ	Енергонезалежне сховище налаштувань
data	phy_init	0xe000	4 КБ	Калібрувальні дані радіомодуля
app	factory	0x10000	1.5 МБ	Основний образ прошивки
app	ota_0	0x180000	1.5 МБ	Слот для оновлення прошивки
data	coredump	0x300000	64 КБ	Збереження дампу пам’яті при критичних збоях

Після монтування файлової системи виконується налаштування таймерів для забезпечення відмовостійкості. Враховуючи високе навантаження на процесор під час роботи нейромережі нами було запроваджено таку систему контролю:

1. Interrupt Watchdog – це апаратний таймер, що гарантує перемикання контексту переривань. Тайм-аут встановлено на рівні 300 мс для запобігання блокуванню системи драйвером Wi-Fi.
2. Task Watchdog – являє собою програмний механізм FreeRTOS, що відстежує стан задач. Задача нейромережевого аналізу повинна періодично скидати таймер, підтверджуючи нормальне функціонування алгоритму [29].

Далі відбувається переміщення статичного буфера Tensor Arena у зовнішній модуль PSRAM. Таким чином використання зовнішньої пам’яті через високошвидкісний інтерфейс

Octal SPI дозволяє виділити неперервний блок розміром до 2 МБ для зберігання вхідних, вихідних та проміжних тензорів, що унеможливлює помилки викликані розподіломресурсів під час роботи системи.

Після ініціалізації стека TCP/IP та встановлення захищеного з'єднання з MQTT-брокером, радіомодуль переводиться у режим прослуховування.

Цикл збору даних та структура кадрів

Механізм щодо бору даних реалізований нами на механіки зворотних викликів, що спрацьовують при виявлені підходящого фрейму стандарту IEEE 802.11. Функція обробки promiscuous_rx_cb отримує доступ до сирого пакету, структура якого відповідає стандарту 802.11 MAC Header загальною довжиною 24 байти (без врахування поля QoS Control).

Ключові поля заголовка, що підлягають аналізу:

— Frame Control (2 байти): містить ідентифікатори версії протоколу, типу (Management, Control, Data) та підтипу (Beacon, Probe Request, Deauthentication) кадру. Також включає прапори ToDS та FromDS, що визначають напрямок руху пакету відносно точки доступу.

— Duration/ID (2 байти): визначає час, на який середовище передачі буде зайнято. Аномально великі значення в цьому полі можуть свідчити про спробу атаки «Virtual Jamming» (Nav Attack).

— Address Fields (6 байт x 3): MAC-адреси приймача (DA), передавача (SA) та точки доступу (BSSID).

Для буферизації потоку даних було створено структуру кільцевого буфера фіксованої ємності N. Керування доступом здійснюється за допомогою двох індексів з яких Head (голова) для запису нових даних та Tail (хвіст) для читання нейромережевим модулем. Розрахунок індексу для запису наступного елемента розраховується за формулою:

$$Index_{next} = (Index_{current} + 1) \bmod N \quad (1)$$

Для запобігання пошкодженню даних, що знаходяться в процесі аналізу, застосовано стратегію «Drop on Full». У випадку, коли буфер заповнений (умова (Head + 1) mod N == Tail), нові пакети ігноруються до моменту звільнення місця задачею аналізу. Це гарантує цілісність часового вікна, яке вже сформовано та передано на вхід нейромережі.

Нейромережевий аналіз

Основною логікою виявлення аномалій являється обробка вектора ознак, сформованих з сирих даних буфера. Цей процес називається розрахунком інженерії ознак яка передбачає перетворення статистичних характеристик трафіку в числовий вектор V.

Для детектування складних атак обчислюються наступні метрики: ентропія Шеннона, середньоквадратичне відхилення інтервалів прибуття, співвідношення керуючих кадрів (R_{mgmt}).

Використання ентропії Шеннона щодо розмірів пакетів потрібна для виявлення тунелювання даних або аномального розподілу навантаження.

$$H(X) = -\sum_{i=1}^{n} P(x_i) log_2 P(x_i), \quad (2)$$

де $P(x_i)$ - ймовірність появи пакету розміром x_i у поточному вікні. Низька ентропія характерна для DDoS-атак, висока - для нормального трафіку.

Середньоквадратичне відхилення інтервалів прибуття дозволяє виявити автоматизовані інструменти сканування, які генерують пакети з фіксованою періодичністю, на відміну від стохастичної природи людської активності.

Співвідношення керуючих кадрів це частка кадрів управління до загальної їх кількості. Різке зростання R_{mgmt} свідчить про атаки типу Deauthentication Flood.

Перед подачею на вхідний шар нейромережі вектор ознак підлягає квантуванню. Оскільки модель TensorFlow Lite оптимізована для цілочисельних обчислень (int8), дійсні значення ознак x_{float} (формат float32) перетворюються у цілі числа x_{quant} за формулою афінного квантування:

$$x_{quant} = clamp\left(\left\lfloor\frac{x_{float}}{S}\right\rfloor + Z, -128,127\right), \quad (3)$$

де S (Scale) - масштабний коефіцієнт, Z (Zero-point) - зміщення нуля, визначені на етапі навчання моделі. Операція clamp обмежує значення діапазоном 8-бітного знакового цілого. Такий підхід зменшує вимоги до пам'яті для зберігання ваг моделі з 4 байт до 1 байта на параметр, що є необхідним для обмеженої кількості ресурсів до будь якого мікроконтролера [30].

Механізм реагування на інциденти

Логіка прийняття рішень та керування режимами роботи системи реалізована у вигляді скінченного автомата. Визначено наступні стани системи:

— STATE_IDLE: початкова ініціалізація, очікування підключення до Wi-Fi/MQTT.
— STATE_MONITOR: пасивне накопичення даних у кільцевий буфер.
— STATE_ANALYSIS: активна фаза інференсу нейромережі.
— STATE_ALERT: формування та відправка сповіщення про загрозу.
— STATE_ISOLATION: виконання активних контрзаходів (блокування).

Перехід у стан STATE_ALERT відбувається за умови, що ймовірність атаки P(Attack), розрахована нейромережею, перевищує порогове значення Threshold. Для запобігання перевантаженню каналу зв'язку та перенасичення одноманітними повідомленями впроваджено алгоритм.

Алгоритм обмежує частоту відправки повідомлень про один і той самий тип атаки. Нове повідомлення генерується лише за умови виконання нерівності:

$$t_{current} - t_{lastalert} > \Delta T_{cooldown}, \quad (4)$$

де $\Delta T_{cooldown}$ — період «охолодження» (наприклад, 5000 мс). Якщо атака триває, система лише інкрементує лічильник інцидентів у локальному лозі, але не ініціює нову транзакцію MQTT, доки не спливе час затримки.

У стані STATE_ISOLATION система може відправляти спеціально сформовані пакети (наприклад, Channel Switch Announcement) для міграції пристроїв на інший частотний канал, ізолюючи їх від джерела перешкод.

Архітектура системи декомпозована на функціональні рівні, що забезпечують збір, первинну обробку, аналіз та передачу інформації.

Обґрунтування топології мережі

Мережева архітектура реалізована за топологією типу «Зірка». Роль центрального концентратора та арбітра безпеки виконує інтелектуальний шлюз. Зовнішні вузли (сенсори, актуатори) функціонують як клієнти, трафік яких підлягає моніторингу та аналізу.

Застосування топології згаданої вище обумовлено необхідністю мінімізації часових затримок при передачі тривожних сповіщень. На відміну від децентралізованих мереж, де маршрутизація пакетів здійснюється через ланцюжок проміжних вузлів, централізована схема виключає затримки при ретрансляції. Такий підхід є необхідним для системи виявлення вторгнень, де час реакції на атаку має складати мілісекунди.

Фізичним середовищем для передачі даних є радіоканал стандарту IEEE 802.11n (Wi-Fi) у діапазоні 2.4 ГГц.

Апаратна реалізація центрального вузла

Основою обчислювального ядра є високоефективна система ESP32-S3-WROOM-1-N16R8. Архітектура мікроконтролера включає два 32-розрядних процесори Xtensa LX7, що

працюють на тактовій частоті 240 МГц. Вибір даної платформи обумовлений наявністю розширеного набору векторних інструкцій, що забезпечують апаратне прискорення операцій матричного множення та згортки, які складають основу обчислювального навантаження згорткових нейронних мереж.

Підсистема пам'яті та інтерфейс Octal SPI

Критичною особливістю обраної модифікації модуля (N16R8) є розширена підсистема пам'яті, що включає:

1. Flash-пам'ять складає 16 МБ і підключена через інтерфейс Quad SPI. Вона використовується для зберігання прошивки, файлової системи LittleFS та статичних вагових коефіцієнтів нейромережі.

2. Оперативна пам'ять (зокрема PSRAM) складає 8 МБ і підключена через високошвидкісний інтерфейс Octal SPI (надалі OPI).

Використання OPI PSRAM є визначальним проектним рішенням. На відміну від стандартної внутрішньої SRAM (512 КБ), якої недостатньо для розміщення складних моделей глибокого навчання, зовнішня пам'ять дозволяє виділити значний обсяг адресного простору під Tensor Arena - безперервну ділянку пам'яті для зберігання вхідних/вихідних тензорів та проміжних результатів активації нейронів. Інтерфейс OPI забезпечує передачу даних по 8 лініях за один такт, що гарантує високу пропускну здатність шини, необхідну для динамічного завантаження шарів моделі без суттєвих затримок інференсу.

Додатково, наявність 8 МБ оперативної пам'яті дозволяє реалізувати глибокий кільцевий буфер (Ring Buffer) для захоплення мережевих пакетів. Це забезпечує режим моніторингу Zero-drop sniffing, нівелюючи ризик втрати пакетів під час пікових навантажень на центральний процесор при обробці результатів нейромережі.

Зовнішні інтерфейси та підсистема реєстрації

Для забезпечення автономності функціонування та реалізації режиму «Чорної скриньки», структурна схема передбачає підключення зовнішнього накопичувача – карти пам'яті MicroSD. Обмін даними реалізовано через апаратний інтерфейс SPI (режим VSPI). Накопичувач використовується для ведення журналів подій безпеки та збереження дампів аномального трафіку для подальшого криміналістичного аналізу.

Комунікація із зовнішнім світом здійснюється через вбудований радіомодуль Wi-Fi, який підтримує роботу в режимі прослуховування. Цей режим потрібен для захоплення кадрів канального рівня без підключення до конкретної точки доступу. Передача телеметрії на сервер здійснюється через захищений канал MQTTS.

Структурна схема комплексу

Графічне представлення архітектури системи, що ілюструє логічні зв'язки та високошвидкісні інтерфейси обміну даними між основними функціональними блоками, наведено на рисунку 1.

Запропонована схема, завдяки використанню розширеної пам'яті OPI PSRAM, забезпечує необхідний апаратний ресурс для розгортання повноцінних моделей глибокого навчання на периферійному пристрої, зберігаючи при цьому стабільність роботи в режимі реального часу.

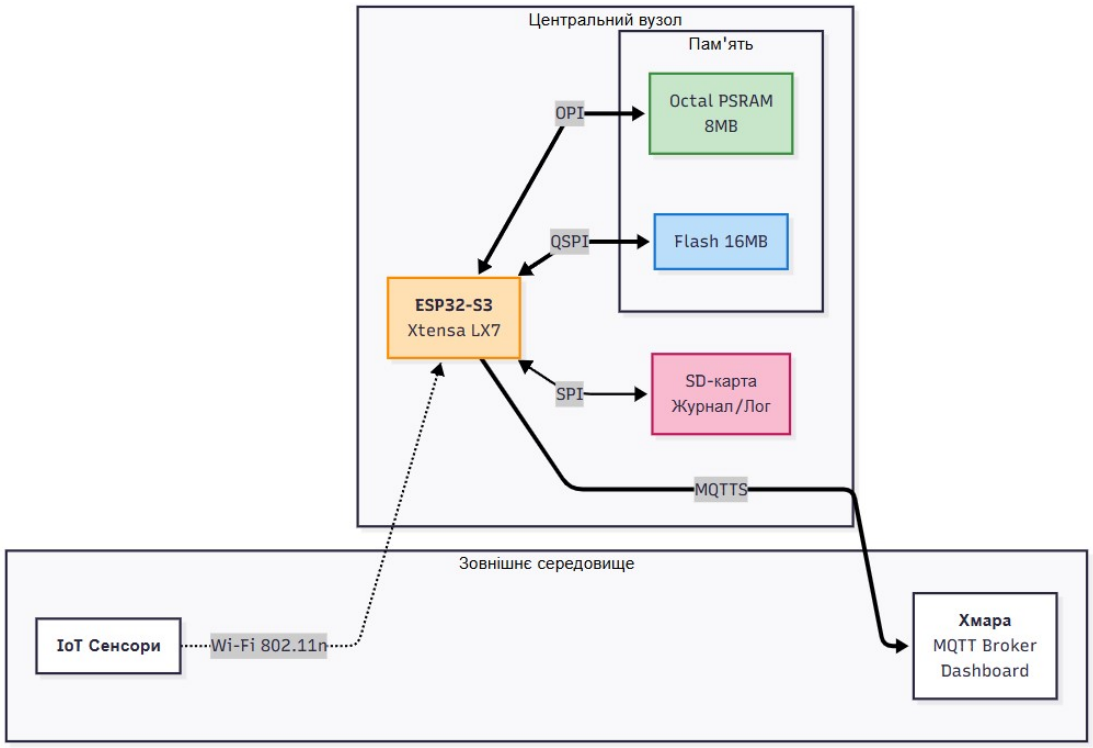

Рисунок 1 – Структурна схема апаратно-програмного комплексу

Висновки. У статті наведено теоретичне узагальнення та розв'язання науково-технічного завдання щодо впровадження легковажних нейронних мереж у вбудовані системи. Досягнення поставленої мети базувалося на послідовному виконанні таких етапів:

— Проведено аналітичний огляд існуючих систем виявлення вторгнень та архітектурних рішень для інтернету речей.

— Досліджено методи оптимізації нейромережевих моделей TinyML для роботи в умовах обмежених апаратних ресурсів мікроконтролерів.

— На основі отриманих результатів створено програмну реалізацію комплексу детекції аномалій трафіку безпосередньо на периферійному вузлі.

Розроблені алгоритми інференсу, адаптовані під векторні інструкції архітектури Xtensa LX7, дозволяють успішно вирішувати завдання ідентифікації кіберзагроз у реальному часі з мінімальною латентністю. У ході аналізу предметної галузі було ідентифіковано ключові об'єкти взаємодії, визначено їхні функціональні характеристики та побудовано математичну модель детектора атак.

Список літератури

1. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». Cybersecurity Defensive Walls in Edge Computing, 2025. pp. 21-61.
2. Вінтенко, Б.Ю., Миронець, І.В., Смірнов, О.А., Коваленко, О.В., Усік, П.С., Буравченко, К.О., Лисенко, І.А. «Логіко-структурна модель комп'ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». Кібербезпека: освіта, наука, техніка. 2025. Том 2 № 30. С. 413-427, 2025.
3. Смірнова, Т.В. «Дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави». Кібербезпека: освіта, наука, техніка. 2025. Том 2 № 30. С.195-208, 2025.
4. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 193–224.
5. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 225–257.

6. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.
7. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка» (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.
8. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». International Review on Modelling and Simulations 18 (1), 2025. pp. 32-42.
9. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». Центральноукраїнський науковий вісник. Технічні науки. 2025. Вип. 11(42), ч. II. С.52-62.
10. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості інтелектуальних систем підтримки оператора». VIII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – 2025. – С. 44-46.
11. Вінтенко, Б., Миронець, І., Смірнов, О., Коваленко, А., Конопліцька-Слободенюк, О., Смірнова, Т., Константинова, Л. «Дослідження застосування систем підтримки оперативного персоналу об'єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 6-26.
12. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
13. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
14. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
15. 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.
16. 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.
17. 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.
18. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 3(73), С. 155-166.
19. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
20. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
21. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
22. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
23. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
24. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67).

С. 84-89.
25. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
26. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
27. 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.
28. 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.
29. 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.
30. 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.