УДК 004

О.Сосна, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КОНТРОЛЮ ІНТЕРНЕТ ШЛЮЗІВ НА БАЗІ ОС UBUNTU

У статті розроблено програмне забезпечення, яке призначено для системи контролю Інтернет шлюзів на базі ОС Ubuntu. Метою розробки є дослідження та принципи побудови системи контролю Інтернет шлюзів на базі ОС Ubuntu. Об'єктом дослідження є процес контролю Інтернет шлюзів на базі ОС Ubuntu. Предметом дослідження є методи контролю Інтернет шлюзів на базі ОС Ubuntu. Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи контролю Інтернет шлюзів на базі ОС Ubuntu. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

контроль Інтернет шлюзів, ОС Ubuntu

Постановка проблеми. У світі мереж шлюз за замовчуванням відіграє ключову роль у спрямуванні мережевого трафіку між вашою локальною мережею та ширшим Інтернетом. Ubuntu 20, як популярний дистрибутив Linux, дозволяє користувачам ефективно налаштовувати та керувати своїми мережевими параметрами. Дана робота проведе вас через процес зміни шлюзу за замовчуванням в Ubuntu 20, забезпечуючи вам повний контроль над вашим мережевим трафіком.

Перш ніж заглибитися в процес, важливо зрозуміти, що таке шлюз за замовчуванням. Шлюз за замовчуванням – це IP-адреса маршрутизатора, який з'єднує вашу локальну мережу з ширшим Інтернетом. Коли пристрою у вашій локальній мережі потрібно зв'язатися з пристроєм в іншій мережі, він надсилає дані до шлюзу за замовчуванням, який потім пересилає їх до потрібного пункту призначення.

Перш ніж почати, переконайтеся, що у вас є такі передумови:

- Система Ubuntu 20 працює.
- Адміністративний доступ до системи.
- IP-адреса нового шлюзу за замовчуванням.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи контролю інтернет шлюзів на базі ОС Ubuntu.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи контролю Інтернет шлюзів на базі ОС Ubuntu.

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

- Огляд існуючих систем контролю Інтернет шлюзів на базі ОС Ubuntu.
- Дослідження системи контролю Інтернет шлюзів на базі ОС Ubuntu.
- Програмна реалізація системи контролю Інтернет шлюзів на базі ОС Ubuntu.

Об'єктом дослідження є процес контролю Інтернет шлюзів на базі ОС Ubuntu.

Предметом дослідження є методи контролю Інтернет шлюзів на базі ОС Ubuntu.

Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Зі зростанням Інтернету речей (IoT) потреба в надійних, гнучких та ефективних шлюзах стає дедалі важливішою. Шлюз IoT діє як міст між пристроями IoT та хмарою, забезпечуючи безперебійну передачу даних та інтелектуальну обробку. Однією з найкращих платформ для розробки та розгортання шлюзів IoT є Ubuntu, універсальна та широко використовувана операційна система з відкритим кодом. У цій статті розглядаються переваги використання Ubuntu для шлюзів IoT та те, як він може революціонізувати ваші рішення IoT.

Що таке шлюз Інтернету речей?

Шлюз Інтернету речей (IoT) – це пристрій або програмна платформа, яка забезпечує зв'язок між пристроями Інтернету речей та хмарними сервісами. Він збирає, обробляє та передає дані, підтримуючи різні протоколи та керуючи підключеннями пристроїв. Ефективний шлюз Інтернету речей забезпечує низьку затримку, підвищує безпеку та спрощує локальну обробку даних.

Чому варто обрати Ubuntu для шлюзів Інтернету речей?

1. Переваги відкритого коду

Будучи програмою з відкритим вихідним кодом, Ubuntu дозволяє розробникам налаштовувати та модифікувати ОС відповідно до потреб конкретного проекту. Ця гнучкість є критично важливою в IoT-додатках, де задіяні різноманітні пристрої та протоколи.

2. Багата екосистема

Ubuntu підтримує широкий спектр бібліотек, фреймворків та інструментів, спеціально розроблених для розробки Інтернету речей. Від Python та Node.js до бібліотек машинного навчання, розробники мають доступ до безлічі ресурсів.

3. Зручний інтерфейс

Ubuntu пропонує зручний інтерфейс, що спрощує розробникам налаштування та керування шлюзами, незалежно від того, чи використовують вони Ubuntu Server, чи Ubuntu Core, розроблені спеціально для IoT-застосунків.

4. Надійна підтримка громади

Маючи сильну спільноту розробників та користувачів, Ubuntu надає розширені ресурси, підтримку з усунення несправностей та документацію, що може бути безцінним під час подолання труднощів.

5. Функції безпеки

Ubuntu включає різні заходи безпеки, включаючи регулярні оновлення, вбудовані брандмауери та дозволи користувачів, які життєво важливі для захисту даних і пристроїв у середовищі Інтернету речей.

Налаштування шлюзу Інтернету речей за допомогою Ubuntu

Щоб проілюструвати, як налаштувати шлюз Інтернету речей за допомогою Ubuntu, давайте розглянемо кілька важливих кроків:

1. Виберіть свою версію Ubuntu

Залежно від ваших потреб, виберіть між Ubuntu Server та Ubuntu Core. Ubuntu Core особливо підходить для пристроїв Інтернету речей завдяки своїй легкості та системі керування пакетами (snap).

2. Встановлення

Завантажте вибрану версію Ubuntu та дотримуйтесь інструкцій з встановлення. Переконайтеся, що у вас є необхідне обладнання, яке відповідає специфікаціям ваших пристроїв Інтернету речей.

3. Налаштуйте параметри мережі

Налаштуйте мережеве з’єднання, щоб ваш шлюз міг взаємодіяти з пристроями Інтернету речей та Інтернетом. Це може включати налаштування параметрів Wi-Fi або Ethernet.

4. Встановлення IoT-фреймворків

Залежно від вимог вашого проекту, ви можете встановити різні IoT-фреймворки, такі як:

Node-RED: Інструмент програмування на основі потоків для з'єднання пристроїв Інтернету речей.

MQTT: Легкий протокол обміну повідомленнями для невеликих датчиків та мобільних пристроїв, оптимізований для мереж з високою затримкою або ненадійних мереж.

Платформа Інтернету речей: Для візуалізації даних, зібраних з пристроїв Інтернету речей.

Розробка та розгортання додатків: Створюйте додатки, які використовують можливості обробки даних, аналітики та локального прийняття рішень. Python або JavaScript є популярним вибором для розробки цих додатків.

5. Захистіть свій шлюз

Впроваджуйте протоколи безпеки, такі як шифрування даних під час передачі та використання безпечних методів автентифікації, для захисту вашої екосистеми Інтернету речей.

Висновок

Використання Ubuntu для шлюзів Інтернету речей пропонує надійну, гнучку та безпечну платформу, яка може ефективно впоратися зі складнощами комунікації Інтернету речей. Завдяки відкритому коду, багатій екосистемі та сильній підтримці спільноти, Ubuntu є чудовим вибором для розробників, які прагнуть створювати інтелектуальні рішення Інтернету речей. Оскільки ландшафт Інтернету речей продовжує розвиватися, використання можливостей Ubuntu, безсумнівно, покращить підключення, ефективність та інновації в численних додатках.

Впроваджуючи та розгортаючи шлюзи Інтернету речей за допомогою Ubuntu, компанії та розробники можуть відкрити нові можливості та стимулювати майбутнє інтелектуальних технологій.

Системи контролю Інтернет шлюзів на базі ОС Ubuntu – це за фактом міжмережевий екран (брандмауер), який працює під керуванням відповідної ОС. Брандмауери – це не щось привабливе. Вони рідко потрапляють у заголовки газет, а коли працюють добре, ви їх майже не помічаєте. Однак у 2025 році, коли ваш бізнес залежить від хмарних додатків, віддалених користувачів та постійно активних сервісів, скромний брандмауер все ще має велику вагу. Уявіть собі свою мережу як будівлю. У вас є двері, коридори, ліфти та постійний потік відвідувачів. Брандмауер – це стійка реєстрації та служба безпеки. Він впускає потрібних людей, не пускає не потрібних і виявляє дивну поведінку, перш ніж вона стане проблемою.

Що таке брандмауер?

По суті, брандмауер перевіряє трафік, який намагається увійти або вийти з вашого середовища, і застосовує встановлені вами правила. Ці правила можуть бути простими, наприклад, «дозволити цьому офісу доступ до цієї служби», або дуже специфічними, наприклад, «дозволити цьому користувачеві доступ до цієї програми лише в робочий час». Сучасні брандмауери йдуть далі. Вони розуміють програми та користувачів, а не лише IP-адреси та порти. Вони можуть переглядати трафік, щоб виявляти відомі загрози, підозрілі закономірності або ризикований контент. Вони ведуть детальні журнали, щоб ви могли довести, хто до чого мав доступ і коли.

Шифрування є ключовою частиною цієї історії. Більшість бізнес-трафіку зараз передається через TLS. Це чудово для конфіденційності, але також може приховувати атаки. За умови правильного проектування та політик брандмауер може розшифрувати трафік на периферії, застосовувати перевірки безпеки, а потім повторно зашифрувати його для подальшого передавання. Якщо все зроблено добре, користувач не помічає різниці, але ви усуваєте основну сліпу зону. Результатом є точка контролю, яка поєднує видимість із можливістю діяти в режимі реального часу.

Реальні виклики 2025 року

Зловмисники швидкі, терплячі та організовані. Один фішинг може дати їм плацдарм. Звідти вони намагаються переміщатися по вашій мережі, знаходити цінні дані та непомітно викрадати їх, перш ніж з’явиться будь-яке повідомлення з вимогою викупу. Водночас ваші

активи зростають. Співробітники підключаються до мережі як з дому, так і в дорозі. Партнери та постачальники інтегруються з вашими системами. Ви використовуєте поєднання хмарних та локальних сервісів. Кожне підключення – це ще один шлях, який може спробувати зловмисник.

Операції також перебувають під тиском. Команди зайняті, інструментів безпеки багато, а зміни накопичуються. Зі зміщенням акценту на безпеку до сучасніших рішень, таких як XDR, SSE, CNAPP та CTEM, брандмауери часто страждають від проблеми «встановив і забув». Правила швидко додаються для вирішення бізнес-проблеми, а потім ніколи не очищаються. З часом ви отримуєте захаращені політики, тіньові правила та широкі «тимчасові» дозволи. Це послаблює безпеку та може уповільнити продуктивність. Якщо сам брандмауер вийде з ладу, наслідки можуть бути негайними. Персонал не може отримати доступ до потрібних програм. Клієнти не можуть зв’язатися з вами. Для багатьох організацій збій брандмауера є збоєм у роботі бізнесу.

Відповідність додає ще один рівень. Вам може знадобитися продемонструвати відповідність вимогам CIS Controls, ISO 27001, PCI DSS або контрактним вимогам. Аудитори очікують побачити чіткі граничні засоби контролю, історію змін та докази того, що зашифрований трафік не є неконтрольованою прогалиною. Ніщо з цього не є складним окремо, але вимагає регулярної уваги та турботи.

Основна функція брандмауера

Основна функція брандмауера – охороняти вашу безпечну внутрішню мережу та публічний Інтернет. Ця роль є вирішальною для пояснення функції брандмауера в захисті системи та інформаційних активів, оскільки вона гарантує, що проходить лише авторизований трафік. Брандмауери захищають цінні цифрові активи, зосереджуючись на трьох основах інформаційної безпеки:

– Конфіденційність: Запобігання несанкціонованому доступу для збереження конфіденційності даних.

– Цілісність: Блокування шкідливого програмного забезпечення, яке може змінити або пошкодити дані.

– Доступність: Захист від атак, таких як відмова в обслуговуванні (DoS), метою яких є зробити системи недоступними.

Невпинно моніторячи мережевий трафік, брандмауери запобігають проникненню хакерів, вірусів і черв'яків у вашу мережу або викраданню конфіденційних даних.

Основні переваги впровадження брандмауера

Впровадження надійного брандмауера надає численні переваги, які пояснюють функцію брандмауера в захисті системи та інформаційних активів:

– Захист від загроз: Брандмауери діють як щит, запобігаючи несанкціонованому доступу, шкідливим програмам та кібератакам, що потрапляють у вашу приватну мережу.

– Фільтрація трафіку: Вони ретельно перевіряють усі пакети даних, регулюючи вхідний та вихідний трафік, щоб забезпечити потік лише легітимних даних, захищаючи від вірусів та спроб фішингу.

– Контроль доступу: Забезпечуючи дотримання правил безпеки, брандмауери визначають, хто може отримувати доступ до мережевих ресурсів, запобігаючи несанкціонованому доступу.

– Безпечний віддалений доступ: Брандмауери мають вирішальне значення для захисту підключень до віртуальної приватної мережі (VPN), що дозволяє віддаленим співробітникам безпечно отримувати доступ до корпоративних мереж.

– Сегментація мережі: Вони можуть розділити мережу на ізольовані сегменти, тому, якщо одна частина порушена, пошкодження локалізується і не може поширюватися.

– Відповідність нормативним вимогам: Багато нормативних актів (таких як HIPAA або PCI-DSS) вимагають використання брандмауерів для захисту конфіденційних даних, допомагаючи підприємствам уникати штрафів та шкоди репутації.

Як працюють брандмауери: огляд основних механізмів інспекції

Щоб пояснити функцію брандмауера в захисті системи та інформаційних активів, ми повинні зрозуміти, як вони перевіряють дані. Брандмауери – це інтелектуальні контролери трафіку, які постійно, за частки секунди, приймають рішення про те, що дозволяти або блокувати, на основі детального набору правил безпеки.

Ця фільтрація на основі правил діє як контрольний список для відхилення, визначаючи, що потрапляє, а що відхиляється. Для кожного пакета даних брандмауер приймає рішення про дозвіл або блокування, контролюючи як вхідний, так і вихідний трафік. Це запобігає проникненню загроз і запобігає виходу конфіденційних даних без дозволу.

Крім того, брандмауери надають можливості ведення журналу та аудиту, зберігаючи детальний облік мережевого трафіку. Ці журнали безцінні для розслідування підозрілої активності, підтвердження відповідності нормативним вимогам та вдосконалення політик безпеки.

Основні механізми: фільтрація пакетів, перевірка стану та проксі-сервери

Сучасні брандмауери використовують три основні методи перевірки, кожен з яких пропонує різний рівень захисту. Розуміння цих методів допомагає пояснити функцію брандмауера у захисті системи та інформаційних активів.

Фільтрація пакетів – це найбазовіша технологія брандмауера. Вона швидка та ефективна, перевіряючи заголовки пакетів на наявність такої інформації, як IP-адреси, номери портів та протоколи. Це як швидка перевірка ідентифікатора біля дверей, але їй бракує усвідомлення ширшого контексту з’єднання.

Перевірка стану є більш інтелектуальною. Вона використовує відстеження стану з’єднання, щоб запам’ятовувати активні, легітимні з’єднання. Розуміючи контекст потоку трафіку, вона знає, коли дозволити відповідь на запит, зроблений вашою мережею, що робить її набагато ефективнішою у блокуванні спроб несанкціонованого доступу.

Проксі-сервіси пропонують найретельнішу перевірку, працюючи на рівні додатків. Вони діють як посередники, отримуючи та повторно передаючи дані від імені вашої мережі. Ця перевірка на рівні додатків дозволяє їм перевіряти фактичний вміст комунікацій, забезпечуючи найвищий рівень безпеки для критично важливих додатків.

Запобігання шкідливому програмному забезпеченню та іншим кіберзагрозам

Коли ми пояснюємо функцію брандмауера для захисту системи та інформаційних активів, це зводиться до запобігання загрозам. Брандмауери працюють цілодобово, щоб зупинити різні кіберзагрози, перш ніж вони завдадуть шкоди.

– Блокування шкідливого коду: Брандмауери розпізнають підозрілі моделі трафіку, пов'язані з вірусами та черв'яками, зупиняючи їх на периметрі мережі до того, як може статися зараження.

– Запобігання DoS-атак: Коли зловмисники перевантажують мережу трафіком, брандмауери можуть виявляти ці незвичайні закономірності та блокувати джерело шкідливого програмного забезпечення, дозволяючи при цьому продовжувати легітимний бізнес-трафік.

– Зменшення спроб фішингу: Хоча брандмауери не є повним рішенням для боротьби з фішингом, вони можуть блокувати доступ до відомих шкідливих веб-сайтів, посилання на які містяться у фішингових електронних листах, забезпечуючи важливу систему безпеки.

– Зупинка несанкціонованого витоку даних: моніторячи вихідний трафік, брандмауери можуть виявляти та блокувати спроби шкідливого програмного забезпечення або інсайдерів надсилати конфіденційну інформацію з вашої мережі.

На рисунку 1 зображена структурна схема системи. На який розглянута розроблена система в цілому.

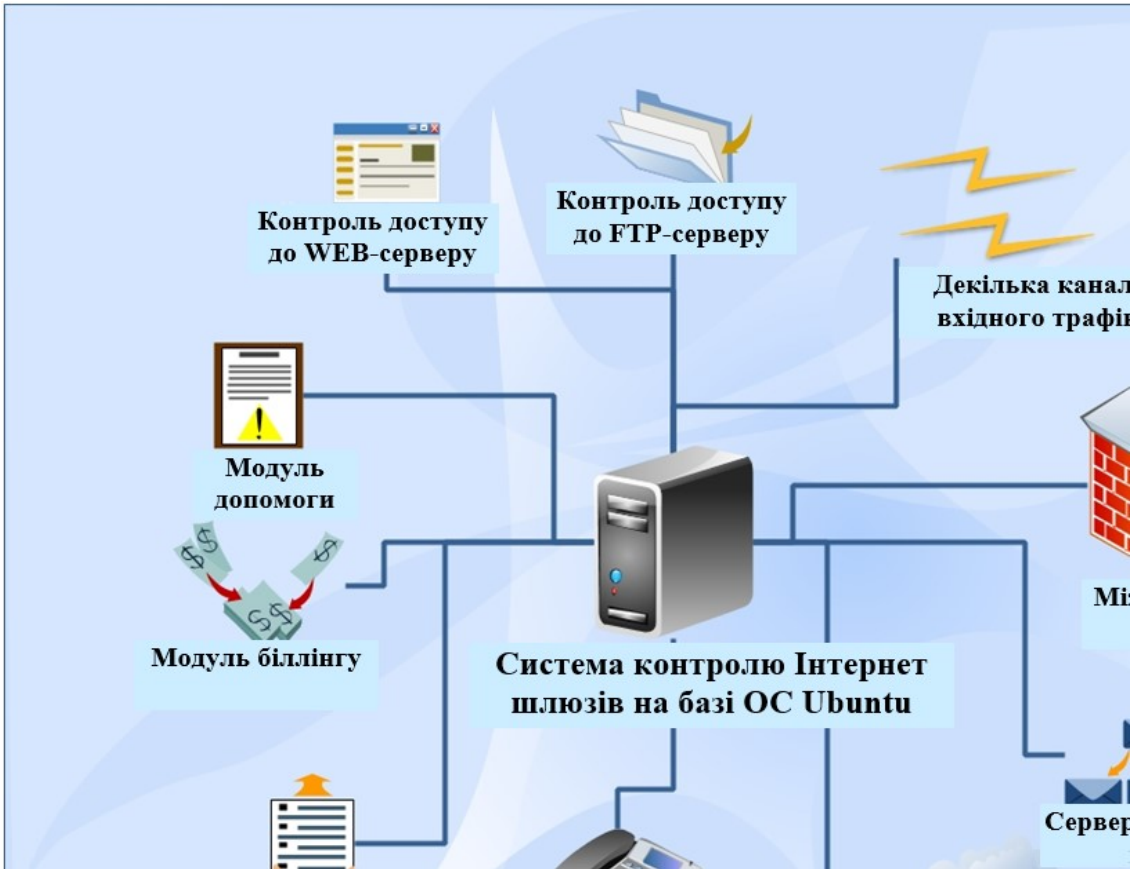

Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів контролю Інтернет шлюзів на базі ОС Ubuntu. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем контролю Інтернет шлюзів на базі ОС Ubuntu.

– Досліджена система контролю Інтернет шлюзів на базі ОС Ubuntu.

– На основі отриманих результатів досліджень створена програмна реалізація системи контролю Інтернет шлюзів на базі ОС Ubuntu.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання контролю Інтернет шлюзів на базі ОС Ubuntu. 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., 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.
2. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». 8th International Symposium on Intelligent Informatics, ISI 2023, 2025. vol 389. pp 377-389. Springer, Singapore.
3. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». CEUR Workshop Proceedings, 2024, 3909, pp. 227–241.
4. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream

Ciphers, Computational Modeling, and Security Analysis». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 379–402.
5. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 403–447.
6. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 170–188.
7. 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.
8. 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.
9. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.
10. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
11. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
12. 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
13. 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.
14. 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.
15. 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.
16. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об’єктах критичної інфраструктури». Кібербезпека: освіта, наука, техніка, №3(19), 2023, С. 176-196.
17. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». ІІ Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи hозвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
18. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
19. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
20. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп’ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв’язку, 2023, вип. 2(72), С. 170-178.
21. 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,
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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
28. 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.
29. 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.
30. 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.
31. 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.
32. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.