УДК 004

Б.Марченко, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРИ ДОСТУПІ ДО WEB-СЕРВЕРУ ЗА РАХУНОК ОПОРТУНІСТИЧНОГО ШИФРУВАННЯ

У статті розроблено програмне забезпечення, яке призначено для системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування. Метою розробки є дослідження та принципи побудови системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування. Об'єктом дослідження є процес забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування. Предметом дослідження є методи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування. Методи дослідження базуються на методах теорії захисту інформації та теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

забезпечення безпеки, доступ, WEB-сервер, опортуністичне шифрування

Постановка проблеми. Опортуністичний TLS схожий на згоду зустрітися з кимось для приватної розмови в людному громадському місці. Якщо є вільний куточок для приватної розмови, ви можете безпечно провести делікатну розмову; однак, якщо тихе місце вільне, ви будете вести розмову відкрито та ризикуватимете, що вас можуть підслухати. Спілкування відбувається, але його конфіденційність не гарантується. У світі електронної пошти, коли один поштовий сервер (наприклад, сервер вашої компанії) надсилає повідомлення на інший сервер (наприклад, сервер Gmail одержувача), він намагається встановити з'єднання, зашифроване за допомогою TLS. Зазвичай це робиться за допомогою команди STARTTLS у протоколі SMTP. Якщо сервер-отримувач підтримує STARTTLS і узгодження пройшло успішно, вміст електронного листа шифрується під час передачі. Однак, якщо сервер-отримувач не підтримує TLS або якщо проблема перешкоджає підтвердженню шифрування, електронний лист буде просто надіслано у вигляді звичайного тексту, тобто він не зашифрований і потенційно може бути прочитаний будь-ким, хто його перехопить.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

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

– Огляд існуючих систем забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

– Дослідження системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

– Програмна реалізація системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

Об’єктом дослідження є процес забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

Предметом дослідження є методи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

Методи дослідження базуються на методах теорії захисту інформації та теорії побудови комп’ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Примусовий TLS – це набагато суворіший підхід до шифрування. Примусовий TLS наполягає на тому, щоб ваша розмова проводилася в приватному місці; якщо немає вільного місця, розмова просто не відбудеться.

Примусовий TLS (також відомий як «Суворий TLS» або «Обов’язковий TLS») вимагає від сервера електронної пошти зашифрованого з’єднання із сервером-отримувачем. Якщо рукостискання TLS не вдається або якщо сервер-отримувач взагалі не підтримує TLS, електронний лист не буде доставлено. З’єднання просто розривається, і відправник зазвичай отримує повідомлення про повернення, що вказує на помилку доставки. Це гарантує, що електронний лист ніколи не буде передано у вигляді звичайного тексту.

Примусовий TLS часто передбачає попередньо налаштовані політики, які іноді називають «політиками TLS» або «конекторами» в системах електронної пошти, де ви явно вказуєте, що зв’язок із певними доменами має використовувати TLS. Це поширена функція в таких службах, як Opportunistic TLS у конфігураціях Office 365, під час налаштування суворих правил потоку пошти.

Переваги та ризики примусового TLS

Переваги:

– Максимальна безпека: Гарантує, що конфіденційна інформація завжди шифрується під час передачі, усуваючи ризик її незашифрованої передачі.

– Запобігає атакам зниження версії: Зловмисник не може змусити з'єднання стати розшифрованим.

– Необхідно для дотримання вимог: Вирішально важливо для виконання суворих нормативних вимог у різних галузях, таких як HIPAA та GDPR.

Ризики:

– Можливі збої доставки: якщо сервер одержувача не підтримує потрібну версію TLS або має проблеми з конфігурацією, електронний лист не буде доставлено.

– Накладні витрати на конфігурацію: Вимагає ретельного налаштування та постійного управління, щоб забезпечити підтримку та налаштування примусового TLS усіма цільовими доменами.

Випадки використання примусового TLS:

– Охорона здоров'я (комунікації, що відповідають HIPAA): Абсолютно необхідна для передачі захищеної медичної інформації (PHI) відповідно до таких правил, як HIPAA, які вимагають безпеки даних пацієнтів.

– Фінансові установи: використовуються для безпечного зв'язку, що включає конфіденційні фінансові дані, реквізити рахунків та транзакції, щоб відповідати стандартам відповідності, таким як PCI DSS.

– Урядові установи: Для обміну секретною або конфіденційною урядовою інформацією, що вимагає суворої конфіденційності.

– Внутрішня корпоративна електронна пошта: Багато організацій застосовують примусове використання TLS між власними внутрішніми поштовими серверами або з довіреними партнерами, щоб забезпечити безпеку всіх внутрішніх комунікацій.

– Висококонфіденційна комунікація B2B: обмін конфіденційною діловою інформацією між двома компаніями, які мають взаємну угоду про забезпечення максимальної безпеки.

Приклади примусового TLS:

– Лікарня надсилає записи пацієнтів до страхової компанії, де обидві сторони домовилися використовувати примусове TLS для всіх комунікацій між своїми доменами. Якщо TLS-з'єднання не вдається встановити, запис не надсилається.

– Система електронної пошти банку часто використовує примусовий TLS під час надсилання виписок з рахунку або конфіденційних сповіщень, гарантуючи шифрування цих листів під час передачі до вашого постачальника послуг електронної пошти (за умови, що ваш постачальник також підтримує необхідний TLS).

– Компанії, що використовують Microsoft 365, можуть налаштувати примусові правила TLS (часто їх називають «конекторами»), щоб електронні листи, надіслані до певних доменів партнерів або з них, повинні використовувати TLS, інакше вони відхиляються. Це допомагає забезпечити відповідність вимогам та надійний захист електронної пошти.

За замовчуванням Microsoft 365 (M365) не використовує примусовий TLS. Натомість він використовує опортуністичний TLS, який намагається зашифрувати електронну пошту під час передачі, якщо сервер-отримувач підтримує його. Якщо TLS недоступний, повідомлення надсилаються незашифрованими.

Однак, M365 можна налаштувати на використання примусового TLS через конектори або правила потоку пошти. За належного налаштування примусовий TLS у M365 гарантує, що електронна пошта надсилатиметься лише за умови встановлення безпечного з'єднання TLS, інакше доставка не вдасться. Коротше кажучи, примусовий TLS – це налаштовуваний параметр, а не поведінка за замовчуванням.

Gmail не використовує примусовий TLS за замовчуванням. Gmail покладається на опортуністичний TLS, тобто намагатиметься зашифрувати електронну пошту під час передачі, якщо сервер-отримувач підтримує TLS; якщо TLS недоступний, повідомлення доставляється незашифрованим.

Хоча Google підтримує примусове використання TLS для певних доменів за допомогою розширених налаштувань Gmail (переважно в Google Workspace), примусове використання TLS не є поведінкою за замовчуванням і має бути налаштоване явно. Крім того, коли TLS не підтримується, а примусове використання TLS налаштоване, альтернативою є те, що повідомлення не надсилатимуться, і цю проблему може вирішити безпечне рішення для електронної пошти Zivver.

Як опортуністичний TLS, так і примусовий TLS відіграють певну роль у безпеці електронної пошти. Однак для організацій, які мають справу з конфіденційними даними та дотримуються вимог до дотримання вимог, примусовий TLS є явним переможцем, оскільки він гарантує шифрування під час передачі. Хоча опортуністичний TLS пропонує підхід «найкращих зусиль», він не усуває ризик незашифрованої передачі, якщо умови не виконуються; у традиційних рішеннях електронної пошти, якщо сервер одержувача не підтримує TLS, ваше повідомлення не може бути надіслано.

Для справді надійної безпеки електронної пошти, яка виходить за рамки базових можливостей TLS, спеціалізоване рішення для шифрування електронної пошти, розширює поштові клієнти, такі як Microsoft 365 та Gmail, за допомогою розширених протоколів шифрування, гарантуючи захист конфіденційних листів та їх можливість читання на безпечному веб-порталі, захищеному потужною двофакторною автентифікацією (2FA). Окрім розширеного шифрування, додатково захищає конфіденційні листи за допомогою зручних функцій запобігання втраті даних, допомагаючи запобігти людським помилкам – усі ці важливі елементи захисту вашої інформації.

Опортуністичний TLS – це стандартна конфігурація безпеки транспортування пошти на всіх агентах передачі повідомлень (MTA) та поштових серверах. Сервери відправника та одержувача пошти домовлятимуться один з одним про те, яке шифрування вони можуть використовувати. Буде використано найбезпечніше з'єднання, яке можуть підтримувати обидві сторони. Це означає, що пошту можна надсилати взагалі без шифрування. Але ви можете це змінити.

Дивно, що ми посилюємо безпеку наших операційних систем і хвилюємося про те, як захищений Microsoft Teams. Іноді ми також звинувачуємо у будь-якому витоку даних прислів'я-стажера (що, до речі, неправильно). Але коли справа доходить до пошти, організації досить погано налаштовують належну автентифікацію пошти. Це все про SPF, DKIM, DMARC, SRS та ARC, я продовжую працювати над своїми соціальними мережами. Особливо є простір для вдосконалення, коли домен організації використовується в сторонніх поштових продуктах.

Шифрування повідомлень

Звичайно, ви можете підписати або зашифрувати свою електронну пошту за допомогою S/MIME, PGP або Microsoft Purview Mail Encryption. Це означає, що окреме поштове повідомлення було зашифровано, незалежно від того, як воно передається. Але, на мою скромну думку, це не дуже зручно для користувача. Вам потрібно попереднє налаштування, таке як отримання сертифікатів та обмін ключами. Шифрування повідомлень забезпечує безпеку, але часто конфліктує з процесами відповідності (наприклад, збереження/архівування). Purview забезпечує захист лише на стороні відправника (для нових листів).

Так, існують шлюзові рішення, але вони часто суттєво збільшують вартість (ліцензії на робоче місце, обслуговування тощо). Видима та прихована вартість електронної пошти зростатиме з кожним додаванням. Кілька причин, чому пошта є привабливим рішенням, – це високий рівень впровадження та сумісності. Вона також відносно проста у використанні та має відносно низьку вартість з майже миттєвою доставкою. (Справедливості заради, економічність пошти – це обґрунтоване припущення. Вона достатньо хороша та була першою, ймовірно, також є вагомими причинами).

Шифрування транспорту

Не зрозумійте мене неправильно. Шифрування повідомлень, безумовно, має свої варіанти використання. Мені здається, що воно іноді заважає думати про інші рішення чи практики. Наприклад, чи варто мені взагалі надсилати цю цінну інформацію, якщо вона потребуватиме шифрування повідомлень? Чи справді пошта є найкращим способом безпечного спілкування?

Хоча я починав із шифрування повідомлень, транспортне шифрування насправді є основною та неявною формою шифрування. Це означає, що наразі майже завжди використовується транспортне шифрування завдяки опортуністичному TLS. У більшості перевірених мною орендарів діапазон «Без TLS» знаходиться в межах 1%. І цей 1% «імовірність» може бути причиною для організації використовувати шифрування повідомлень, зменшуючи потенційні прогалини за допомогою транспортного шифрування та запобігаючи перехопленню повідомлень.

Як варіант, організації-партнери використовують обов'язкові TLS -з'єднання. Вони налаштовуються для забезпечення наявності шифрування транспорту перед надсиланням будь-якої пошти. Часто вони також мають форму автентифікації за IP-адресою або сертифікатом. Проблема, яку я бачу, полягає в тому, що вони вимагають спеціальної конфігурації та налаштування для кожного поштового домену, що збільшує витрати, а іноді вимагає контакту з вузлом для повідомлення правильної кінцевої точки SMTP. MTA-STS є покращенням, оскільки він певною мірою запобігає атакам Advisary-in-the-Middle, оскільки публікує кінцеву точку MX у файлі конфігурації на захищеному веб-сайті з тим самим доменом організації. Найкращим рішенням для безпеки транспорту на сьогодні є DANE. Він забезпечує навіть більший рівень безпеки, ніж обов'язковий TLS, оскільки значною мірою залежить від DNSSEC. На жаль, не всі організації можуть використовувати DNSSEC. (Azure DNS мав його в попередньому перегляді, але цього ярлика більше немає?). Особливо, коли Exchange Online підтримуватиме обов'язковий DANE пізніше у 2025 році. Це примусово використовуватиме DANE на основі клієнта або домену та не дозволить переходу на MTA-STS або опортуністичний TLS. Немає потреби в обов'язковому TLS або навіть маршрутизації через захищені приватні мережі.

Але і MTA-STS, і DANE страждають від тих самих проблем, що й інші акроніми, а саме від їхнього впровадження. Іноді це пов'язано з технічними причинами, але частіше з усвідомленням або розумінням їхніх переваг порівняно з тим, що використовується за замовчуванням, тобто опортуністичним TLS.

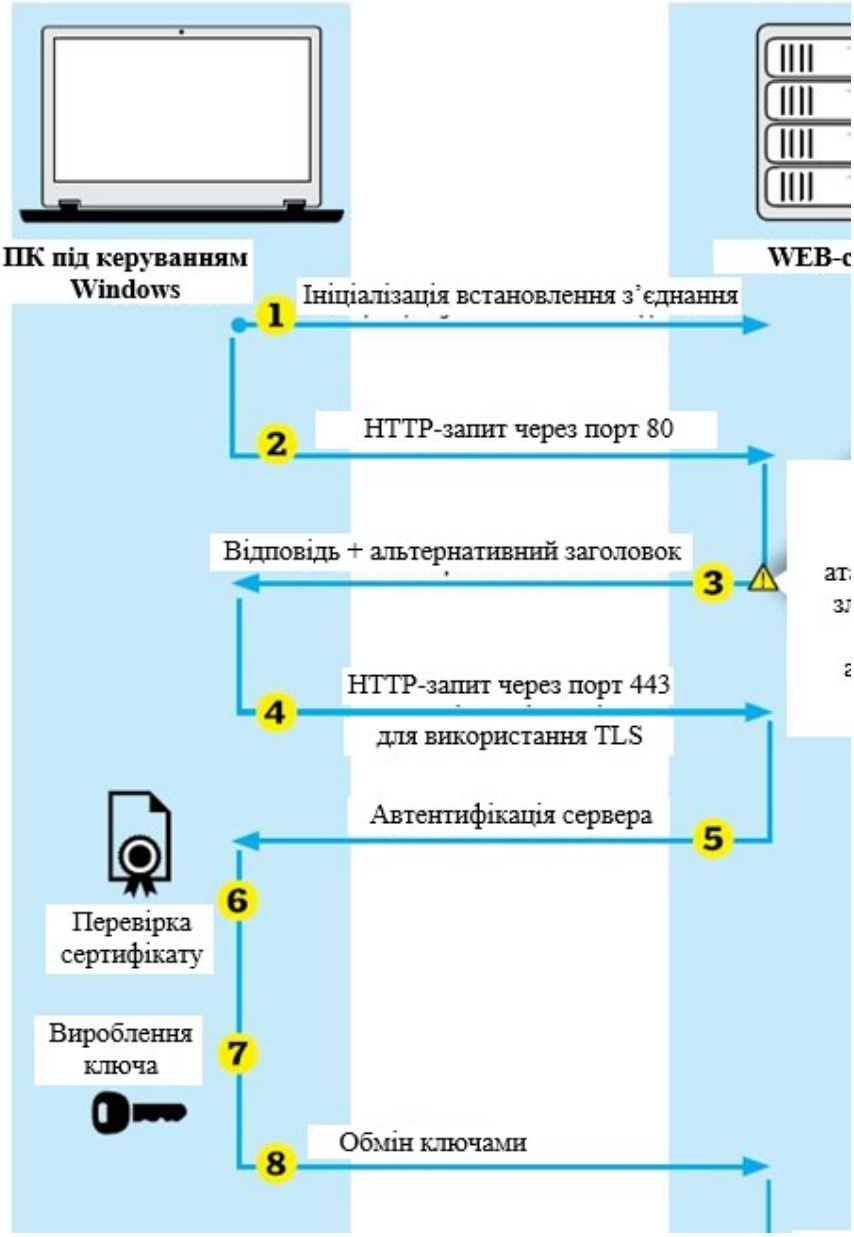

Рисунок 1 – Структурна схема системи

Примусове використання TLS в Exchange Online

Щоб примусово використовувати TLS для підключення SMTP за замовчуванням, потрібно налаштувати як вхідний, так і вихідний конектор. Базові однорядкові інструкції Exchange Online PowerShell у найпростішій формі (без виконання перевірки):

New-OutboundConnector -ConnectorType Partner -RecipientDomains * -TlsSettings EncryptionOnly -UseMXRecord $True -Name "Outbound Forced TLS"

New-InboundConnector -ConnectorType Partner -SenderDomains * -TlsSettings EncryptionOnly

Є три основні висновки: тип конектора – Партнер. Ви налаштовуєте домени одержувача та відправника за допомогою символу підстановки *. І останній етап – лише шифрування, а не перевірка сертифіката. Більш специфічні конектори (наприклад, ті, що мають IP-адреси та/або повні доменні імена) замінять ці конектори. Ви можете мати певні

конектори, які не потребують TLS, якщо вам це потрібно для прямого надсилання або ретрансляції SMTP.

Якщо ваша організація надає пріоритет отриманню пошти перед шифруванням транспортування, ви можете розглянути можливість початку роботи з вихідного конектора. У поєднанні з оповіщенням про чергу пошти або використанням вбудованих звітів про повідомлення ви можете відстежувати ситуацію та діяти відповідно.

Більш цілісний підхід до безпеки (пошти)

Організації повинні регулярно перевіряти весь свій підхід до обміну інформацією з іншими сторонами. Пошта – це просто, і майже завжди вона вже доступна. Але за останні кілька років з'явилися інші продукти або їх удосконалили до такого стану, що це може бути найкращим рішенням для цієї роботи. Вона також може бути дешевшою, простішою в управлінні та навіть безпечнішою.

Я б зосередився на транспортному шифруванні, такому як примусове використання TLS та впровадження як MTA-STS, так і DANE. Особливо (обов'язкове) DANE є значним покращенням і може бути причиною для переоцінки використання шифрування повідомлень у певних сценаріях.

Опортуністичне шифрування

Опортуністичне шифрування починається з незашифрованого запиту. Шифрування встановлюється тільки тоді, коли сервер відправляє альтернативний заголовок із пропозицією зашифрувати канал.

Робота системи проілюстрована структурною схемою, відображеної на рисунку 1.

Тут загрожує небезпека: за допомогою атаки посередника зловмисник може перехопити альтернативний заголовок.

Порт 80 – **WWW-сервер**. Показує присутність http-сервера в системі. За допомогою WWW-сервісу можна довідатися назву й версію програмного забезпечення встановленого на WEB-сервері.

Порт 443 – **Протокол HTTPS** (**SSL**). Варіант безпечного протоколу **HTTP**.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

– Досліджена система забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

– На основі отриманих результатів досліджень створена програмна реалізація системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування. Розроблені алгоритми дозволяють успішно вирішувати завдання забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування. 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. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». Кібербезпека: освіта, наука, техніка. 2025. Том 1 № 29. С.704–716, 2025.
2. 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.
3. 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.
4. 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.
5. Kuznetsov, O., Poluyanenko, N., Smirnov, O., Kozhakhmetova, D. «Optimized Simulated Annealing for Efficient Generation of Highly Nonlinear S-Boxes». Advancements in Cybersecurity Next Generation Systems and Applications, 2025. 146-174
6. Kuznetsov, O., Poluyanenko, N., Smirnov, O., Bekeshova, G. «Enhanced Cryptographic Security through Advanced S-Box Optimization: A Hybrid Heuristic Approach». Advancements in Cybersecurity Next Generation Systems and Applications, 2025. pp. 56-78.
7. Kuznetsov, O., Poluyanenko, N., Smirnov, O., Abduraimova, B «Enhancing Cryptographic Strength: A Novel Approach to S-Box Generation Using Modified Simulated Annealing». Advancements in Cybersecurity Next Generation Systems and Applications, 2025. pp. 79-116.
8. Kuznetsov, O., Derevianko, Y., Frontoni, E., Arnesano, M., Smirnov, O. «Factorial Representation of S-Boxes: A Novel Approach to Cryptographic Analysis and Optimization». Advancements in Cybersecurity Next Generation Systems and Applications, 2025. pp. 117-145.
9. Kuznetsov, O., Poluyanenko, N., Smirnov, O., Shaikhanova, A., Khruskov, B. «Innovative Cost Functions for Optimizing Cryptographic S-Box Generation». Advancements in Cybersecurity Next Generation Systems and Applications, 2025. pp. 29-55.
10. Kuznetsov, O., Smirnov, O., Akhmetov, B., Alimseitova, Z., Imoize, A.L. «Deep Learning Frontiers in Copy-Move Forgery Detection: Advances, Challenges, and Future Directions». Advancements in Cybersecurity Next Generation Systems and Applications, 2025. 202-229.
11. 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.
12. Kuznetsov, O., Smirnov, O., Mormul, M., Kotukh, Y., Zvieriev, V. «Comparative Research on Cryptocurrency Efficiency: An Objective Analysis of Key Metrics». International Journal of Computing 23(4), 2024. pp. 563-573.
13. Kuznetsov O., Frontoni E., Kuznetsova K., Smirnov O., Kostenko V. «Blockchain applications in metaverse environments: new horizons». Advanced Metaverse Wireless Communication Systems. pp. 255-293. 2024.
14. Kuznetsov, O., Frontoni, E., Chevardin, V., Smirnov, O., Imoize, A.L. «Advancing metaverse security with cryptographic innovations». Advanced Metaverse Wireless Communication Systems. pp 351-386. 2024.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. Kuznetsov, O., Frontoni, E., Kandiy, S., Smirnova, T., Prokopov, S., Bilanovych, A. «New Cost Function for S-boxes Generation by Simulated Annealing Algorithm». Lecture Notes on Data Engineering and Communications Technologies, 2023. vol 180. pp. 310-320. Springer, Cham.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». II 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.
28. 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.
29. 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.
30. 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.
31. 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.
32. 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,