УДК 004

В.Оніщук, магістр гр. КН-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ РИЗИКІВ БЕЗПЕКИ ПРИ ВИКОРИСТАНІ МІЖМЕРЕЖЕВИХ ЕКРАНІВ

У статті розроблено програмне забезпечення, яке призначено для системи інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів. Метою розробки є дослідження та принципи побудови системи інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів. Об'єктом дослідження є процес інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів. Предметом дослідження є методи інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів. Методи дослідження базуються на методах аналізу даних, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

інтелектуальний аналіз, ризик безпеки, міжмережеві екрані

Постановка проблеми. У сучасну цифрову епоху як організації, так і окремі особи сильно залежать від веб-додатків для широкого кола діяльності. Однак ця залежність від Інтернету також відкриває можливості для зловмисників використовувати слабкі місця безпеки, присутні в цих додатках. Брандмауери веб-додатків (WAF), як правило, є першою лінією захисту, захищаючи веб-додатки шляхом фільтрації та моніторингу HTTP-трафіку. Однак, якщо ці брандмауери не налаштовані належним чином, зловмисники можуть обійти їх або скомпрометувати. Зростаюча кількість атак, спрямованих на веб-додатки, підкреслює нагальну потребу в підвищенні їхньої безпеки. Дана робота пропонує поглиблений огляд існуючих досліджень з оцінки вразливостей веб-додатків та тестування на проникнення (VAPT).

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів.

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

– Огляд існуючих систем інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів.

– Дослідження системи інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів.

– Програмна реалізація системи інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів.

Об'єктом дослідження є процес інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів.

Предметом дослідження є методи інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів.

Методи дослідження базуються на методах аналізу даних, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Оцінка ризиків – це необхідна діяльність, яку необхідно проводити регулярно, щоб побачити загальний стан навколишнього середовища.

Ця оцінка є важливим процесом, який використовується для виявлення потенційних ризиків або небезпек у певній ситуації чи діяльності, а також для оцінки ймовірності та потенційних наслідків цих ризиків.

Існує кілька причин, чому важливо проводити оцінку ризиків.

Це може включати запобігання нещасним випадкам і травмам, дотримання правил, репутацію тощо.

Що стосується оцінки ризиків брандмауера, то це процес оцінки ефективності заходів безпеки брандмауера організації.

Оцінка ризиків брандмауера включає оцінку конфігурації, правил та політик брандмауера, щоб визначити, чи вони належним чином налаштовані та підтримуються для захисту мережі організації від зовнішніх загроз.

Метою оцінки ризиків брандмауера є виявлення потенційних слабких місць у заходах безпеки брандмауера та рекомендація кроків для покращення безпеки мережі організації.

Opinnate проводить оцінку ризиків брандмауера на основі найкращих галузевих практик, яка охоплює такі теми, як рівень дозволеності правила, використання кластера, використання IPS тощо. Детальні елементи перелічені як категорії тем наступним чином:

- Рівень вседозволеності правила.
- Правила доступу до периметра.
- Стан журналу брандмауера та кожного правила.
- Небезпечний доступ до послуг.
- Конфлікт корпоративної політики.
- Стан кластера брандмауера.
- Використання правила або об'єкта.
- Використання IPS.

Постійне розслідування цих елементів у режимі реального часу надаватиме інформацію про стан ризику в режимі реального часу, яку можна буде постійно переглядати на системних панелях, і відповідно вживати заходів. Крім того, для подальшого аналізу будуть створюватися звіти про оцінку ризиків для кожного брандмауера або системи.

Брандмауер – це пристрій мережевої безпеки, апаратний або програмний, який контролює весь вхідний та вихідний трафік і, на основі визначеного набору правил безпеки, приймає, відхиляє або відкидає цей конкретний трафік. Він діє як охоронець, який допомагає захистити ваш цифровий світ від небажаних відвідувачів та потенційних загроз.

Брандмауер:

– Прийняти: дозволити трафік.

– Відхилити: заблокувати трафік, але відповісти повідомленням «помилка недоступності».

– Відмова: блокування трафіку без відповіді.

Потреба в брандмауері

Брандмауер є важливим, оскільки мережі постійно піддаються впливу як безпечного, так і шкідливого трафіку з Інтернету чи інших мереж. Без брандмауера ваші системи не матимуть захисту від небажаного доступу, шкідливої діяльності чи випадкових витоків даних.

1. Запобігання несанкціонованому доступу

Уявіть, що двері вашого будинку завжди відчинені. Будь-хто, хто переходить повз, може зайти та забрати ваші речі. Брандмауер – це як замкнені двері з охоронцем, які впускають лише перевірених людей і не пускають незнайомців.

2. Блокування шкідливого трафіку

Подумайте про свою поштову скриньку електронної пошти. Без спам-фільтра ви б отримували шахрайські та спам-повідомлення. Брандмауер працює як цей спам-фільтр, він блокує шкідливі дані, перш ніж вони досягнуть вас.

3. Захист конфіденційної інформації

Це як зберігати свій банківський PIN-код у сейфі, а не залишати його на столі, де будь-хто може його побачити. Брандмауер гарантує, що ваші особисті та бізнес-дані залишаться прихованими від кіберзлочинців.

4. Запобігання кібератак

Якщо ви залишите свій автомобіль незамкненим на парковці, злодії можуть його вкрасти. Брандмауер блокує вашу мережу, щоб зловмисники не могли її викрасти.

5. Контроль використання мережі

Так само, як батьки встановлюють батьківський контроль, щоб діти не могли відвідувати небезпечні веб-сайти, брандмауери контролюють, де вашим комп'ютерам дозволено підключатися.

Робота брандмауера

Брандмауер працює як охоронець вашої мережі, стоячи між вашими внутрішніми системами, такими як комп'ютери, сервери та пристрої, та зовнішнім світом, таким як Інтернет чи інші мережі. Він ретельно перевіряє всі дані, що входять або виходять, щоб забезпечити проходження лише безпечного трафіку.

– Коли дані намагаються увійти до вашої мережі або вийти з неї, вони спочатку проходять через брандмауер.

– Брандмауер перевіряє пакети даних (невеликі фрагменти інформації) за допомогою заздалегідь визначених правил.

– Правила можна визначити на брандмауері на основі необхідності та політик безпеки організації.

– Брандмауер дозволяє приймати рішення, такі як: Дозволити → Якщо пакет відповідає правилам безпеки, або Блокувати → Якщо пакет підозрілий, походить з чорного списку джерела або містить шкідливий код.

– Брандмауер реєструє заблокований або незвичний трафік для перевірки командами безпеки.

– Сповіщення можуть надсилатися в режимі реального часу, якщо виявлено серйозну загрозу.

Політика за замовчуванням: Дуже важко чітко охопити всі можливі правила на брандмауері. З цієї причини брандмауер завжди повинен мати політику за замовчуванням. Політика за замовчуванням складається лише з дій (прийняти, відхилити або видалити). Припустимо, що на брандмауері не визначено жодного правила щодо SSH-підключення до сервера. Отже, він дотримуватиметься політики за замовчуванням. Якщо політика за замовчуванням на брандмауері встановлена на прийняття, то будь-який комп'ютер за межами вашого офісу може встановити SSH-підключення до сервера. Тому встановлення політики за замовчуванням як "відхилити" (або "скинути") завжди є гарною практикою.

Типи брандмауерів

1) Розміщення в мережі:
– Брандмауер фільтрації пакетів.
– Брандмауер з перевіркою стану.
– Проксі-брандмауер (рівень програми).
– Шлюз на рівні схеми.
– Брандмауер веб-застосунків (WAF).
– Брандмауер наступного покоління (NGFW).
2) Захищені системи:
– Мережевий брандмауер.
– Брандмауер на базі хоста.

3) Метод фільтрації даних:
– Периметральний брандмауер.
– Внутрішній брандмауер.
– Розподілений брандмауер.
4) Форм-фактори:
– Апаратний брандмауер.
– Програмний брандмауер.

Важливість брандмауерів

Мережевий брандмауер – це ваша перша лінія захисту в кібербезпеці. Він відстежує, фільтрує та контролює дані, що передаються в вашу мережу та з неї.

– Мережі вразливі до будь-якого трафіку, який намагається отримати доступ до ваших систем, незалежно від того, чи є він шкідливим, чи ні. Саме тому вкрай важливо перевіряти весь мережевий трафік.

– Коли ви підключаєте персональні комп'ютери до інших IT-систем або Інтернету, це відкриває багато переваг, таких як співпраця, спільний доступ до ресурсів та творчість. Але це також наражає вашу мережу та пристрої на ризики, такі як злом, крадіжка особистих даних, шкідливе програмне забезпечення та онлайн-шахрайство.

– Як тільки зловмисник знайде вашу мережу, він зможе легко отримати до неї доступ та створювати до неї загрозу, особливо за умови постійного підключення до Інтернету.

– Використання брандмауера є важливим для проактивного захисту від цих ризиків. Він допомагає користувачам захистити свої мережі від найгірших небезпек.

Брандмауер служить бар'єром безпеки для мережі, звужуючи поверхню атаки до однієї точки контакту. Замість того, щоб кожен пристрій у мережі був підданий доступу до Інтернету, весь трафік спочатку має пройти через брандмауер. Таким чином, брандмауер може фільтрувати та блокувати недозволений трафік, незалежно від того, чи він входить, чи виходить. Крім того, брандмауери допомагають створювати облік спроб підключень, підвищуючи обізнаність про безпеку.

Брандмауери регулюють як вхідний, так і вихідний трафік, захищаючи мережу від:

– Зовнішні загрози, такі як віруси, фішингові електронні листи, атаки типу «відмова в обслуговуванні» (DoS) та бекдори. Брандмауери фільтрують вхідний трафік, запобігаючи несанкціонованому доступу до конфіденційних даних та запобігаючи потенційним зараженням шкідливим програмним забезпеченням.

– Внутрішні загрози, такі як відомі зловмисники або ризиковані програми. Брандмауер може застосовувати правила та політики для обмеження певних типів вихідного трафіку, що допомагає виявляти підозрілу активність та запобігати витоку даних.

Брандмауери можуть захищати від різноманітних загроз, моніторячи та контролюючи вхідний і вихідний мережевий трафік. Ось основні загрози, від яких вони допомагають захиститися:

– Проникнення зловмисників: Брандмауери можуть блокувати підозрілі з'єднання, запобігаючи прослуховуванню та розширеним постійним загрозам (APT).

– Батьківський контроль: Батьки можуть використовувати брандмауери, щоб заборонити своїм дітям доступ до відвертого веб-контенту.

– Обмеження перегляду веб-сторінок на робочому місці: Роботодавці можуть обмежити працівників у використанні мережі компанії для доступу до певних сервісів та веб-сайтів, таких як соціальні мережі.

– Національно контрольована інтрамережа: Уряди можуть блокувати доступ до певного веб-контенту та послуг, які суперечать національній політиці чи цінностям.

Дозволяючи власникам мережі встановлювати певні правила, брандмауери пропонують настроюваний захист для різних сценаріїв, підвищуючи загальну безпеку мережі.

Практики безпеки брандмауера

Тримайте брандмауер увімкненим

Ніколи не вимикайте брандмауер лише для підключення до пристрою чи мережі. Натомість налаштуйте правила брандмауера та додайте довірені пристрої до списку дозволених пристроїв.

Будьте в курсі подій

Регулярно оновлюйте програмне забезпечення брандмауера або операційну систему, щоб виправляти вразливості та запобігати новим загрозам безпеці.

Підключення до VPN

VPN шифрує ваш інтернет-трафік, додаючи ще один рівень захисту поряд із вашим брандмауером. Тільки обов’язково налаштуйте правила брандмауера, якщо виникне конфлікт.

Відхилити невідомі запити

Якщо ви отримаєте підозрілий запит на доступ, негайно його заблокуйте. Розслідуйте це пізніше, перш ніж вносити будь-які постійні зміни.

Додайте додаткові інструменти безпеки

Брандмауери не блокують усі загрози, особливо шкідливі програми, які ви встановлюєте самостійно. Використовуйте перевірене антивірусне або антивірусне програмне забезпечення для повного захисту.

Рисунок 1 – Структурна схема системи

Брандмауер – це механізм безпеки, який може бути апаратним або програмним, здебільшого призначений для забезпечення безпеки. Його основна мета – забезпечити доступ до комп’ютера або мережі лише уповноваженим особам. Він виступає посередником між приватною мережею та публічним Інтернетом для регулювання доступу до трафіку відповідно до заданої політики безпеки.

Апаратні брандмауери діють як фізичні бар'єри між мережею та Інтернетом, тоді як програмні брандмауери – це додаткові програми для ПК або мережевих комп'ютерів.

Брандмауер можна уявити як охоронця, який стоїть між приватною мережею та публічним Інтернетом і дозволяє перетинати цей бар'єр лише такому трафіку.

Брандмауери функціонують, аналізуючи потоки мережевих пакетів або пакетів даних, що циркулюють у мережі. Вони визначають, чи пропускати пакет чи ні, залежно від встановлених параметрів безпеки. Це може включати аналіз джерела та пункту призначення пакета, використовуваного протоколу зв'язку та вмісту повідомлення.

Існують різні типи брандмауерів, зокрема:

– Фільтрація пакетів Брандмауер.
– Брандмауер проксі-сервісу.
– Брандмауер з перевіркою стану.
– Шлюзи рівня каналу Брандмауер.
– Брандмауер наступного покоління (NGFW).
– Програмні брандмауери.
– Апаратні брандмауери.
– Хмарні брандмауери.

Тепер перейдемо до функцій брандмауера, щоб зрозуміти, як вони допомагають компаніям та окремим особам створювати безперебійні та безпечні мережі.

Головна функція брандмауера – забезпечення безпеки. Ці системи пропонують численні цілі, які безпосередньо покращують безпеку, керованість та продуктивність мережі. Нижче ми пояснили деякі інші функції брандмауера.

Моніторинг мережевого трафіку

Важливою функцією брандмауера є регулювання руху трафіку між приватною мережею та публічним Інтернетом. Брандмауери аналізують кожен пакет інформації, який хоче ввійти або вийти через брандмауер, перевіряючи адресу джерела та призначення, а також використовуваний протокол. Цей пакет порівнюється з попередньо встановленими правилами безпеки; якщо брандмауер схвалює, пакет пропускається; в іншому випадку він блокується.

Контроль доступу

Брандмауери допомагають регулювати, хто може отримувати доступ до вашої мережі та який рівень свободи в ній є. Використовуючи правила доступу, ви можете вирішувати, хто або що може підключатися до вашої мережі. Наприклад, ви можете дозволити переглядати деякі дані лише певним користувачам, а іншим – заборонити.

Контроль доступу описується як список дозволів для вашої мережі, відомий як Список контролю доступу. Так само, як двері будинку зачинені для людей, яких ви не знаєте або не є вашими родичами, брандмауер дозволяє перебувати всередині мережі лише тим, кому дозволено.

Фільтрація пакетів

Фільтрація пакетів використовується в брандмауерах для перевірки мережевого трафіку на рівні пакетів. Брандмауери аналізують пакети, спочатку перевіряючи їх на рівні заголовка, який складається з інформації, що передається з кожним пакетом; він містить IP-адреси джерела та призначення. Потім брандмауери аналізують протокол зв'язку та номери портів, що використовуються.

Представлені тут пакетні дані можуть використовуватися брандмауерами та пов'язаними з ними системами для фільтрації та подальшого вжиття заходів, тобто «дозволу» або «заборони» різних типів трафіку відповідно до політик безпеки. Наприклад, брандмауер можна налаштувати так, щоб він забороняв підключення всього трафіку на стандартному веб-порті 80, щоб запобігти доступу хакерів до хостів на веб-серверах.

Фільтрація на рівні програми

Окрім фільтрації на рівні пакетів, сучасні брандмауери розширюють свою функціональність, фільтруючи на рівні програм. Брандмауери роблять це, розглядаючи вміст повідомлення та контекст мережевого трафіку, а не лише заголовок. Це також дозволяє їм

контролювати та забороняти або дозволяти певні програми чи служби, такі як перегляд веб-сторінок, електронна пошта або протокол передачі файлів.

Фільтрація на рівні програм через брандмауери забезпечує дотримання політик безпеки, таких як запобігання доступу до певних веб-сайтів або використання певних програм.

Фільтрація контенту

Ще однією важливою функцією брандмауерів є те, що їх також можна запрограмувати на фільтрацію контенту на основі різних критеріїв. Ця функція дозволяє організації або окремій особі заборонити будь-якій IP-адресі доступ до певних сайтів або контенту, доступного в Інтернеті та визнаного забороненим або небезпечним.

Фільтрація контенту схожа на батьківський контроль. Так само, як ви б налаштували батьківський контроль на телевізорі чи Інтернеті для своїх дітей, фільтрація контенту робить те саме для всієї мережі.

Система виявлення вторгнень та система запобігання вторгненням

Брандмауери також можуть виконувати роль IDPS, скорочення від intrusion detection and prevention systems (систем виявлення та запобігання вторгненням) . Таким чином, вони можуть шукати ознаки, що вказують на зловмисну активність, таку як мережева атака, спроба несанкціонованого доступу або будь-яка дивна активність у мережі. Коли йдеться про загрози безпеці, брандмауери можуть діяти ефективно та запобігати атаці або пом'якшувати її наслідки, якщо така є.

Ця функція виявлення та запобігання вторгненням допомагає захистити мережу та підключені до неї пристрої від багатьох видів кіберзагроз, таких як DDoS, мережеве шкідливе програмне забезпечення та незаконний доступ.

Підтримка віртуальної приватної мережі (VPN)

Сучасні брандмауери пропонують VPN- рішення як у своєму списку функцій, так і в основному наборі функцій. У випадку VPN-з'єднання, формування безпечного та зашифрованого тунелю між користувачем та мережею здійснюється за допомогою VPN, щоб користувач міг безпечно підключатися до мережі віддалено.

Брандмауери, що підтримують VPN, можуть допомогти організації розширити периметр своєї мережі та задовольнити потреби користувачів, яким доводиться або які бажають працювати віддалено в сучасному бізнес-середовищі.

Трансляція мережевих адрес (NAT)

Ще однією важливою функцією брандмауерів є те, що вони містять функції NAT, які дозволяють їм перетворювати одну схему мережевих адрес в іншу. Це особливо актуально, коли приватна мережа використовує інший набір IP-адрес, ніж публічна мережа.

Коли брандмауери виконують NAT, внутрішня фактична топологія мережі залишається прихованою від глобальної мережі, що робить її безпечнішою. Це може допомогти мінімізувати прямий доступ до внутрішніх пристроїв з Інтернету, тим самим зменшуючи ймовірність атаки.

Ведення журналів та звітність

Брандмауери зазвичай мають функції реєстрації та звітності, що дозволяють їм записувати та аналізувати мережевий трафік і події безпеки. Цю інформацію можна використовувати для різних цілей, таких як:

- Моніторинг та аудит мережевої активності.
- Виявлення та розслідування інцидентів безпеки.
- Створення звітів для цілей дотримання вимог та регулювання.
- Оптимізація конфігурацій брандмауера та політик безпеки.

Ось деякі з основних функцій брандмауера, які допомагають захистити вашу приватну мережу та пристрої.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів.

– Досліджена система інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів.

– На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів.

Розроблені алгоритми дозволяють успішно вирішувати завдання інтелектуального аналізу ризиків безпеки при використані міжмережевих екранів. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov O., Frontoni E., 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. Chulinda L., Smirnov O., Shapenko L., Ustynova I., Bohatiuk I., Kelyp S. «The role of innovation in ensuring the safety of international civil aviation». Ceur Workshop Proceedings, 2025, 4024, pp. 530–542.
3. Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін. «Системи інформаційної зброї та технології інформаційної війни»: підручник / Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед, Жарков Я.М., Смірнов О.А, Буравченко К.О., Давидюк А.В., Кононович В.Г., Корчинский В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка.– К.: Видавничий центр “Кафедра”, 2025.– 320 с.
4. 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
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
18. 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
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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,
28. 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.
29. 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.
30. 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.
31. 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.