УДК 004

С.Фоменко, магістр гр. КН-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПРОТИДІЇ ЗЛОВМИСНИМ ПРОГРАМАМ З ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ

У статті розроблено програмне забезпечення, яке призначено для системи протидії зловмисним програмам з використанням методів машинного навчання. Метою розробки є дослідження та принципи побудови системи протидії зловмисним програмам з використанням методів машинного навчання. Об'єктом дослідження є процес протидії зловмисним програмам з використанням методів машинного навчання. Предметом дослідження є методи протидії зловмисним програмам з використанням методів машинного навчання. Методи дослідження базуються на методах машинного навчання, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи протидії зловмисним програмам з використанням методів машинного навчання. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

протидія зловмисним програмам, машинне навчання

Постановка проблеми. Антивірусний бізнес зараз на підйомі. Тільки в 2025 році, за даними компанії Gartner, по усьому світі було продано програм безпеки на суму в 22 мільярда доларів. Однак скільки б засобів не витрачали підприємства й частки користувачі, стовідсоткового захисту не існує.

Особливо «улюбленим» у розроблювачів антивірусів підвидом шкідливого ПЗ є програми-здирники. Усього за третій квартал минулого року було заблоковано 821 865 подібних атак на користувачів продуктів.

Жахає при цьому те, наскільки зловмисники успішні у своїй справі: за інформацією цієї компанії, через відсутність мер протидії кожна третя жертва перераховує хакерам викуп – однак 20 відсотків таких користувачів ніколи не одержать від здирників код для дешифрування своїх даних. На кожному потерпілому злочинці заробляють у середньому близько 17 000 грн. – досить вигідний бізнес.

Щодня з'являються 300 000 нових видів шкідливого ПЗ – безперервна гра в кішки-мишки для антивірусів. Стандартними базами сигнатур з небезпекою впоратися практично неможливо. Тому сучасні захисні рішення роблять ставку на аналіз поводження. У цьому випадку захисне ПЗ в реальному часі перевіряє, як поводиться передбачуваний вірус на комп'ютері. При підозрілих зверненнях сканер блокує програму й повідомляє про це користувача.

Проблема: зловмисники розробляють методи для обходу евристики, наприклад, укриваючи своїх шантажистів у серйозних продуктах. Покласти кінець такому принципу дії здатні тільки зовсім нові техніки.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи протидії зловмисним програмам з використанням методів машинного навчання.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи протидії зловмисним програмам з використанням методів машинного навчання.

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

– Огляд існуючих систем протидії зловмисним програмам з використанням методів машинного навчання.

– Дослідження системи протидії зловмисним програмам з використанням методів машинного навчання.

– Програмна реалізація системи протидії зловмисним програмам з використанням методів машинного навчання.

Об'єктом дослідження є процес протидії зловмисним програмам з використанням методів машинного навчання.

Предметом дослідження є методи протидії зловмисним програмам з використанням методів машинного навчання.

Методи дослідження базуються на методах машинного навчання, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Опишемо які технології повинна реалізовувати сучасна система протидії зловмисним програмам з використанням методів машинного навчання.

Система протидії зловмисним програмам з використанням методів машинного навчання є платформою безпеки, призначення якої – виявлення й відбиття різних погроз, включаючи погрози нульового дня, як на робочих станціях, так і в мережі за допомогою міжмережних екранів (Firepower) або ж засобами захисту контенту. Вона дозволяє безпосередньо виявляти шкідливі програми, проводити історичний аналіз файлових подій на робочій станції або ж у мережі, взаємодіяти з «пісочницею». Функціонал ретроспективного аналізу допомагає виявити шкідливе ПЗ, що змогло обійти традиційні механізми безпеки. Наприклад, система протидії зловмисним програмам з використанням методів машинного навчання ідеально підійшла для виявлення й блокування на крапці входу недавніх WannaCry і Petya.

Безперервна аналітика

Використання хмарної аналітики (Talos) більших обсягів даних для визначення, чи є файл безпечним або шкідливим, що підвищує точність виявлення схованих атак на вході в систему й для закриття шляхів проникнення, а також мінімізації уразливостей.

Швидке виявлення погроз

За допомогою технології безагентового виявлення (аналіз і тестування поводження підозрілих файлів) здійснюється реєстрація всієї файлової активності й, як наслідок, швидке виявлення вірусів.

Ретроспективний аналіз

Автоматичний аналіз історії дій файлів (звідки проникнув, де виконувався, що робив) не тільки знижує до мінімуму ризик глобального поширення зловмисного ПЗ, але й дозволяє виявити точну локалізацію атаки.

Захист від атак

Забезпечення повсюдного захисту від погроз із використанням ретроспективної безпеки до традиційного виявлення, що значно підвищує ефективність, продуктивність мережі й охват потенційно шкідливих файлів.

Контроль ланцюжка атаки

Новий рівень аналітики в режимі реального часу для виявлення погроз, що зіставляє шаблони шкідливого поводження на окремому кінцевому пристрої й на всіх кінцевих пристроях мережі.

Розширена аналітика

Автоматизоване виявлення підозрілого поводження, що забезпечують розподілене подання всіх областей, які найбільш піддані ризику атаки.

Поведінковий аналіз

Цілеспрямований пошук порушень на підставі реальних подій.

Відстеження подій

Можливість спрощеної й швидкої розбивки ланцюжка атак для своєчасного виявлення основних причин зараження (окремі додатки, файли, документи, віруси й т.д.)

Моніторинг мережі

Звіти не обмежені збором і підрахунком подій. Звітність у системі протидії зловмисним програмам з використанням методів машинного навчання для прикінцевих пристроїв включає панелі, що дають можливість діяти, моніторингу й визначення тенденцій, що показує доречність із погляду бізнесу й вплив з погляду ризику.

Інтеграція з іншими рішеннями

Система протидії зловмисним програмам з використанням методів машинного навчання виконує передачу й кореляцію інформації про погрози по всій архітектурі, включаючи як екосистему система протидії зловмисним програмам з використанням методів машинного навчання, так і інші платформи безпеки, таких як Email і Web Security.

Джерелами найбільшої в галузі бази даних, сформованої на основі моніторингу погроз і аналізу більших даних, є системи колективної інформаційної безпеки, група по інформаційній безпеці й дослідженням і канали системи протидії зловмисним програмам з використанням методів машинного навчання.

Система протидії зловмисним програмам з використанням методів машинного навчання працює в такий спосіб:

– До початку атаки система протидії зловмисним програмам з використанням методів машинного навчання використовує глобальні аналітичні дані по погрозах, які надходять із відділу колективної інформаційної безпеки компанії, групи по інформаційній безпеці й дослідженням, а також по каналах дані системи протидії зловмисним програмам з використанням методів машинного навчання. Це допомагає підсилити захист від відомих і невідомих погроз.

– Під час атаки система протидії зловмисним програмам з використанням методів машинного навчання використовує аналітичні дані, відомі сигнатури файлів і динамічний аналіз на основі технології система протидії зловмисним програмам з використанням методів машинного навчання, щоб виявити й блокувати файли, що порушують політику безпеки, експлойти й шкідливе ПЗ, що намагається проникнути в мережу.

– Після завершення атаки або після первісної перевірки файлу система безупинно контролює й аналізує всю активність і трафік файлу, незалежно від його статусу, відслідковуючи будь-які ознаки шкідливого поводження. Якщо файл, що одержав раніше статус «невідомий» або «безпечний», діє підозріло, система протидії зловмисним програмам з використанням методів машинного навчання фіксує це й відправляє повідомлення в службу інформаційної безпеки із вказівкою потенційної погрози. система протидії зловмисним програмам з використанням методів машинного навчання забезпечує своєчасне одержання даних про те, звідки з'явилася шкідлива програма, які системи вона торкнулася й що робить у цей момент. Система надає інструменти, які дозволяють швидко реагувати на проникнення й усунути його за допомогою декількох клацань миші. Такі інструменти дозволяють службам інформаційної безпеки вчасно одержувати дані, допомагаючи швидко виявити атаку, оцінити масштаб вторгнення й знешкодити шкідливий код до того, як він завдасть шкоди

Машинне навчання складається із двох великих розділів: фази навчання й розпізнавання.

– Фаза навчання. На початку фахівці повинні пояснити комп'ютеру, що характеризує вірус. На наступних етапах комп'ютер буде стає усе розумніше до того ж почне вчитися.

– Розпізнавання. Потім натренований алгоритм на підставі поводження виконуваної програми здатний вирішити, чи йде мова про легітимний додаток або про схований у файлі вірусі.

У сучасні комерційні продукти безпеки інтегрований захист від програм-здирників. Вона в реальному часі постійно сканує систему на наявність дивних звертань до файлів. Одночасно із цим перевіряються показники системи, з'ясовується, чи не підвищується

раптово навантаження на процесор і чи не зростає стрімко число звертань до дисків (перші індикатори атаки).

В офіційних заявах затверджується, що розроблювачі антивірусів знають свою справу й гарантують ефективний захист від нападів. Однак інсайдери пошепки розповідають, що й у цієї технології є слабкі місця: кібергангстери послідовно встановлюють на ізольовану систему всі розповсюджені антивірусні рішення, а потім спокійно розробляють ідеальний вірус, що не буде замічений сканером і зможе обдурити навіть найсучаснішу евристику.

Проти таких, розроблених з більшими зусиллями, варіантів практично будь-який антивірусний продукт неспроможний. Незважаючи на те що розроблювачі протягом декількох годин після поширення вірусу підготовляють захист, до перших потерпілих протиотрута попадає занадто пізно.

Винуватий у цьому людський фактор: фахівцям зі шкідливого ПЗ необхідно вручну розібрати новий вірус, проаналізувати його й підготувати опис, що потрапить на систему клієнта при відновленні. У випадку зі складними «шкідниками» процес може зайняти кілька днів. На аналіз особливо вишуканого утвору злочинців можуть піти навіть місяці.

Деякі розроблювачі бачать майбутнє вірусного аналізу у відмові від людського фактора: у центрі будуть перебуває машини, що розпізнають шкідливе ПЗ й запускають відповідне відновлення.

Аналіз через машинне навчання

Усілякі компанії, від Symantec до Malwarebytes, сьогодні займаються розробкою методів, при яких роботу з аналізу вірусів візьмуть на себе IT-системи. У випадку з машинним навчанням дослідники «згодовують» суперкомп'ютеру кілька мільйонів файлів – як шкідливих, так і безпечних.

Програми з машинним навчанням. Malwarebytes починаючи із третьої версії робить ставку на автоматизоване навчання.

За допомогою так званих ознакових описів потім комп'ютеру пояснюється, як виглядає вірус, якими характеристиками він володіє і як звичайно поводиться на комп'ютері своєї жертви – абсолютно так само, як і при розвитку й вихованні дитини.

Таким чином, поступово машина знайде самостійність і буде усе надійніше розрізняти вірус і легітимну програму. І нехай частота помилок залишається ще досить високої, поступово вона буде знижуватися, а алгоритм удосконалюватися.

Компанія Symantec для машинного навчання звела навіть окремий обчислювальний центр у Великобританії

Однак такий розвиток вимагає часу й ресурсів. В Symantec є свій окремий обчислювальний центр для машинного навчання, де займаються оптимізацією методики.

У сучасних антивірусних продуктах цей алгоритм уже є елементом стратегії розпізнавання. Незважаючи на це на заднім тлі однаково присутні люди-дослідники, оскільки нова технологія ще страждає від дитячих хвороб.

Проблеми з панацеєю

Як би не була гарна ідея машинного навчання, до цих спостерігаються ключові недоліки, що затримують тріумфальний хід. У першу чергу, усе впирається в гроші.

Крім того, незважаючи на перехід до машинного навчання, на місці завжди повинна бути присутнім команда експертів. Вона контролює алгоритм і в неоднозначних випадках сама приймає рішення, вірус це чи ні, вносячи відповідні коректування.

Фірми, що скорочують витрати на персонал і стовідсотково належні на алгоритм, ризикують допустити в навчальний процес помилкові результати. Таким чином, їхня безпека стрімко знижується.

Одного лише машинного навчання недостатньо

Проблема машинного навчання впирається насамперед у мову. Якщо представити нинішній сценарій погрози у вигляді англомовної країни, такий алгоритм був би успішний лише в боротьбі зі шкідливим ПЗ англійською мовою.

Однак оскільки ландшафт погрози постійно змінюється, і відповідно постійно з'являється нова мова, доводиться увесь час із чистого аркуша адаптувати алгоритм під ситуацію, що змінилася. А це складно. Приміром, сімейство Trojan-Ransom.Win32.Shade складається з 30 000 підтипів. Одним лише розпізнаванням такого сімейства алгоритм не здатний забезпечити захист від всіх його підвидів. Для цього знадобилися б сотні прикладів на кожний вірус – лише так алгоритм навчається автоматично.

Утиліта машинного навчання також не здатна захистити від спеціалізованих атак. Просто відсутня база даних. На одній методиці машинного навчання далеко не виїхати. Вона може бути винятково шестірнею в складній антивірусній машині. Але навіть із машинним навчанням і іншими засобами антивірусні системи катастрофічно відстають від розроблювачів шкідливого ПЗ.

Всі захисні продукти роблять помилки

Навіть якщо в системі використовуються «пісочниці», карантин, евристичні методи й машинне навчання, зловмисники умудряються неї обманювати. Як уже було сказано вище, досить протестувати антивірусне рішення на ізольованій системі до релізу «шкідника» і знайти в такий спосіб пробіли в розпізнаванні.

Сучасні антивіруси повинні розпізнавати й зупиняти програми-здирники завчасно

Іншу небезпеку представляють самі антивіруси. Хакери, користуючись уразливостями, за допомогою перепрограмування можуть одержати за ними контроль так само, як над звичайним ПЗ. Так, у червні 2016 року постраждала компанія Symantec. Фахівці виявили сім критичних лазівок практично у всіх антивірусних продуктах цього розроблювача.

Приклавши мінімальні зусилля, зловмисники інфікують не тільки комп'ютери, але й цілі корпоративні мережі. Для використання уразливостей вони повинні примусити свою жертву до виклику модифікованої веб-сторінки. Оскільки антивірусним продуктам на комп'ютері видаються максимально розширені права, подібні уразливості стають фатальними. Гра в кішки-мишки між атакуючими й що обороняються, таким чином, триває. Однак машинне навчання в кожному разі ускладнить життя розроблювачам вірусів.

Напрямки розпізнавання

У сучасних антивірусних системах для розпізнавання використовується цілий ряд методів. Нові файли проходять через різні стадії за пару митей.

– **Аналіз поводження.** При виникненні підозр сканер запускає файл передбачуваного вірусу в пісочниці – захищеної області. Там рудиментарний алгоритм перевіряє, чи не заражена програма.

– **Швидка оцінка.** У майбутньому після впровадження машинного навчання нинішня модель буде пропонувати більше швидкий і надійний захист, а також відрізнятися підвищеною продуктивністю. Однак і в цьому випадку остаточне рішення, чи довіряти файлу або перемістити його в карантин, приймає користувач за комп'ютером.

Структурна схема розробленої, у результаті виконання магістерської роботи, системи зображена на рисунку 1.

З нього ми бачимо, що система складається з наступних структурних блоків:

– Модулю машинного навчання системи протидії злвмисни программам (антивірусної системи (АС)).

– Джерела погроз.

– Антивірусне програмне забезпечення на персональному комп’ютері.

– Загрози безпеці.

Розглянемо ці структурні блоки більш детально.

До джерел загроз відносяться наступні:

– Загрози з інтернету.

– Загрози при роботі зі змінними носіями інформації.

До антивірусного програмного забезпечення на персональному комп’ютері, відносяться наступні підсистеми:

– Підсистема контролю цілісності.
– Підсистема контролю процесів.
– Підсистема самозахисту антивірусу.
– Підсистема виявлення атак.
– Підсистема аналізу захищеності.
– Підсистема антивірусного захисту.
– Підсистема захисту від спаму.
– Підсистема мережного екранування.

Рисунок 1 – Структурна схема системи

Розглянемо їх більш детально.

Підсистема виявлення атак призначена для виявлення несанкціонованої вірусної активності за допомогою аналізу пакетів даних, циркулюючих в антивірусній системі, а також подій, що реєструються на серверах і робочих станціях користувачів.

Підсистема аналізу захищеності забезпечувати можливість виявлення технологічних і експлуатаційних уразливостей АС за допомогою проведення мережевого сканування.

Підсистема антивірусного захисту призначена для виконання наступних функцій: видаленої установки і деінсталяції антивірусних засобів на серверах і робочих станціях користувачів; видаленого управління параметрами роботи підсистем захисту, що входять до складу комплексної системи антивірусного захисту; централізованого збору і аналізу інформації, що поступає від інших підсистем.

Підсистема захисту від спаму. Антиспам дозволяє відслідковувати, фільтрувати та видаляти спам, що пересилається в вашу поштову скриньку. Система не видаляє повідомлення, які здадуться їй спамом. Вона лише робить відповідну позначку на них і доставляє їх, як завжди. Саме тому ці повідомлення також включаються до вашого трафіка. Рівень перевірки спаму – Spam check level – визначає, наскільки жорсткою буде фільтрація спаму. Антиспамові фільтри аналізують кожне електронне повідомлення, яке проходить крізь поштовий шлюз і оцінюють його за шкалою від 1 до 14. Чим більший номер, тим більша ймовірність того, що повідомлення буде віднесено до розряду спаму: Дуже жорстка фільтрація: гарантує, що до вашої поштової скриньки спам практично не буде надходити. Тим не менше, ви ризикуєте втратити і потрібні повідомлення (не пропускає повідомлення, що оцінені вище 2). Жорстка: практично всі спамові повідомлення будуть видалені, є ймовірність видалення потрібних повідомлень (не пропускає повідомлення, що оцінені вище 4). Нормальна: може заблокувати деякі розсилки (не пропускає повідомлення, що оцінені вище 7). Нежорстка: пропускає "другосортну" пошту (не пропускає повідомлення, що оцінені вище 10). М'яка: пропускає майже всю пошту (не пропускає повідомлення, що оцінені вище 14). Рівень оцінки за замовчуванням зазвичай дорівнює 5, проте адміністратор хостингової системи може його змінити. Обробка спаму: Mark as spam: – присвоєння позначки "спам" – до теми електронного повідомлення буде додане слово СПАМ, і потім це повідомлення буде переслане клієнту як вкладення із зазначенням деталей. Remove: видалення спамового повідомлення. Коли клієнт запустить команду надіслати/отримати, повідомлення зі спамом до нього не надійде. Move To: дозволяє вказати поштову скриньку, куди буде відправлено спам. Клієнти не отримають спам у свою поштову скриньку, проте зможуть переглянути його у вказаній скриньці.

Підсистема мережного екранування призначена для захисту робочих станцій користувачів від можливих мережевих вірусних атак за допомогою фільтрації потенційно небезпечних пакетів даних.

Підсистема контролю цілісності. Контролює все програмне забезпечення на брандмауері і присилає звіти про всі віддалені файли, що щойно з'явилися і змінилися.

Підсистема контролю процесів призначена для визначення які процеси відбуваються у системі, та чи є вони дозволеними операційною системою, чи ні.

Підсистема самозахисту антивірусу. Ефективна система самозахисту захищає його від зупинки або відключення навіть при проведенні цільових атак. Антивірус здатний створювати диск аварійної регенерації системи. Будь-які посилання на шкідливі або фішингові сайти програмою блокуються автоматично. У разі поразок антивірус після ліквідації загроз самостійно здатний відновити систему, повернувши її в стан, який був до виникнення проблем з руйнівним кодом або вірусом. Програма виконує діагностику системи, виявляючи існуючі пробіли та визначаючи відповідність її оновлень за допомогою бази даних. Але програмою, на жаль, не передбачено надання інформації про те, яка версія програми, яка має прогалини, встановлювалася. Дану інформацію доведеться виявляти самостійно. Крім того, повна інформація про сам процес усунення вразливих місць недоступна.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів протидії зловмисним програмам з використанням методів машинного навчання. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем протидії зловмисним програмам з використанням методів машинного навчання.

– Досліджена система протидії зловмисним програмам з використанням методів машинного навчання.

– На основі отриманих результатів досліджень створена програмна реалізація системи протидії зловмисним програмам з використанням методів машинного навчання.

Розроблені алгоритми дозволяють успішно вирішувати завдання протидії зловмисним програмам з використанням методів машинного навчання. 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. 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. 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., 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.
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. Смірнов, О.А., Константинова, Л.В., Конопліцька-Слободенюк, О.К., Козірова, Н.В, Якименко, Н.М., Доренський, О.П., Буравченко, К.О. «Дослідження інструментів штучного інтелекту для роботи з базами даних та аналізу даних». Кібербезпека: освіта, наука, техніка. 2025. №3(27), С. 429–448.
12. 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.
13. Smirnov O., Fedorov E., Neskorodieva A., Neskorodieva T. «Intellectual Classification method of Gymnastic Elements Based on Combinations of Descriptive and Generative Approache». CEUR Workshop Proceedings Volume 3664, 2024, Pages 11-23.
14. 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.
15. Malyukov V., Bebeshko B., Lakhno V., Smirnov O., Malyukova I., Mohylnyi H. «Managing the Purchase-Sale

Process of Digital Currencies Under Fuzzy Conditions». Lecture Notes in Networks and Systems, 2023, 729 LNNS, pp. 104–112.
16. 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.
17. 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.
18. 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.
19. Smirnov, O., Karapetyan, A., Fedorov, E., «Creating Neural Network and Single Solution Human-Based Metaheuristic Methods of Solving the Traveling Salesman Problem». CEUR Workshop Proceedings, Volume 3312, 2022, pp. 47-58.
20. 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, pp. 1-12.
21. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheroz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». Sensors (Basel, Switzerland) Volume 22, Issue 16, 6223, 2022.
22. 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.
23. Kuznetsov, A., Oleshko, I., Chernov, K., Bagmut, M., Smirnova, T. «Biometric authentication using convolutional neural networks». Lecture Notes in Networks and Systems. Volume 152, 2021, Pages 85-98.
24. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. https://doi.org/10.1007/s42979-021-00739-w.
25. Smirnov O., Neskorodieva T., Fedorov E., Rymar P. «Neural Network Modeling Method of Transformations Data of Audit Production with Returnable Waste». CEUR Workshop Proceedings Volume 3101, 2021, Pages 192-207.
26. 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.
27. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
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., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
31. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.