УДК 004

С.Батрак, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПРОАКТИВНОГО МОНІТОРИНГУ МЕРЕЖЕВОГО ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

У статті розроблено програмне забезпечення, яке призначено для системи проактивного моніторингу мережевого електронного документообігу. Метою розробки є дослідження та принципи побудови системи проактивного моніторингу мережевого електронного документообігу. Об’єктом дослідження є процес проактивного моніторингу мережевого електронного документообігу. Предметом дослідження є методи проактивного моніторингу мережевого електронного документообігу. Методи дослідження базуються на методах комп’ютерних мереж, методах великих даних, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи проактивного моніторингу мережевого електронного документообігу. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

проактивний моніторинг, мережевий електронний документообіг

Постановка проблеми. Багато глобальних організацій узгодили свою стратегію та діяльність за допомогою структури інтегрованої системи управління (ІСУ) на основі ISO, яка дозволяє їм об'єднувати системи управління якістю, навколишнім середовищем, охороною здоров'я та безпекою. У такому контексті наявність надійної системи електронного управління документами (СЕД) є важливою, особливо на глобальних підприємствах, де велика кількість документів, що генеруються процесами, проходить через різні робочі культури. Однак, не існує універсального рішення для СЕД, оскільки воно залежить від потреб, розміру та розподілу ресурсів організацій.

У цій роботі розглядається взаємозв'язок між СЕД та ІСУ, щоб запропонувати найкращу практику. Дана робота методологічно базується на якісному, інтерпретативному, поздовжньому емпіричному дослідженні на заводі вітрових турбін.

Удосконалення та ефективність ІСУ ігнорують СЕД як ключовий фактор у встановленні належної технологічної підтримки процесів ІСУ. Правильне застосування СЕД може додатково сприяти організаційному навчанню, точності документації та міжорганізаційній співпраці.

Теоретизація щодо ІСУ потребує глибшого розуміння технологічних обмежень та потенціалу базування ІСУ на СЕД.

ІСУ – це складні системи, що включають велику кількість адміністративних функцій. СЕД забезпечує формальне представлення з потенціалом автоматизації, що підвищує та забезпечує достовірність документів. ІСУ, як правило, залишається у професіоналів, наприклад, лінійних менеджерів та фахівців з контролю якості/якості/якісного менеджменту (QA/QMS). Напрямок обговорення СЕД передбачає ширше охоплення. Дослідження ІСУ як технологічної реалізації забезпечує кращу платформу для узгодження ІСУ з іншими бізнес-процесами та наближає ІСУ до операційної діяльності в межах підприємства.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи проактивного моніторингу мережевого електронного документообігу.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи проактивного моніторингу мережевого електронного документообігу.

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

– Огляд існуючих систем проактивного моніторингу мережевого електронного документообігу.

– Дослідження системи проактивного моніторингу мережевого електронного документообігу.

– Програмна реалізація системи проактивного моніторингу мережевого електронного документообігу.

Об'єктом дослідження є процес проактивного моніторингу мережевого електронного документообігу.

Предметом дослідження є методи проактивного моніторингу мережевого електронного документообігу.

Методи дослідження базуються на методах комп'ютерних мереж, методах великих даних, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Сьогодні нам кажуть, що простого моніторингу недостатньо. Щоб досягти справжньої оптимізації продуктивності та надійності, потрібно проводити моніторинг проактивно. Тому багато компаній звертаються до проактивного моніторингу.

На перший погляд, це цілком очевидно. Не потрібно бути досвідченим інженером з надійності сайтів (SRE), щоб знати, що краще застосовувати проактивний підхід до моніторингу, ніж чекати, поки щось піде не так, перш ніж виправляти це.

Але справжнє питання полягає в тому, як насправді здійснювати проактивний моніторинг. Легко говорити про важливість проактивного моніторингу, але важче підійти до нього на практиці.

Що таке проактивний моніторинг?

Проактивний моніторинг – це стратегія моніторингу, за якої команди прагнуть виявляти та вирішувати проблеми до того, як вони перетворяться на критичні збої.

Він відрізняється від звичайного реактивного моніторингу тим, що замість того, щоб чекати, поки щось піде не так, перш ніж вживати заходів для її вирішення, проактивний моніторинг зосереджується на використанні інформації з моніторингу для прогнозування проблем, що виникають, та придушення їх у зародку, перш ніж вони перетворяться на реальні проблеми.

Іншими словами, замість того, щоб чекати, поки сервер вийде з ладу або програма буде перевантажена трафіком, перш ніж вживати заходів щодо виправлення ситуації, проактивний моніторинг передбачає вжиття превентивних заходів для запобігання збою сервера або запуску іншого екземпляра програми, щоб уникнути збою.

Проактивний моніторинг – це автоматизований процес у режимі реального часу, який безперервно відстежує продуктивність системи, мережеву інфраструктуру та ключові показники для виявлення та запобігання потенційним проблемам, перш ніж вони спричинять простої або збої. Використовуючи прогнозну діагностику та виявлення аномалій, проактивний моніторинг виявляє проблеми на ранній стадії, сповіщає команди про необхідність негайного вжиття заходів та забезпечує ефективну та надійну роботу системи.

Такий підхід допомагає запобігти збоям серверів, оптимізувати продуктивність та захистити інфраструктуру, забезпечуючи масштабовані, інтегровані рішення для підприємств будь-якого розміру. Завдяки проактивному моніторингу проблеми вирішуються до їх загострення, мінімізуючи перебої та підтримуючи безперебійну роботу.

Знову ж таки, переваги проактивного моніторингу мають бути досить очевидними. Коли ви запобігаєте проблемам проактивно, ваші користувачі стикаються з меншою кількістю збоїв. Ви забезпечуєте набагато кращий клієнтський досвід – і, в свою чергу, збільшуєте бізнес-цінність – коли повністю уникаєте серйозних збоїв.

За допомогою реактивного моніторингу найкраще, на що ви можете сподіватися, це швидке вирішення проблем із збоями після того, як вони вже сталися. Це не ідеально з точки зору клієнтського досвіду чи бізнесу.

Проактивний проти реактивного моніторингу

Проактивний моніторинг передбачає використання загальносистемних процедур моніторингу для виявлення та вирішення основних проблем, *перш ніж* вони призведуть до збоїв. Реактивний моніторинг здійснюється лише *у відповідь на* проблему, яка вже виникла. Процедури реактивного моніторингу, по суті, слугують розслідуванням першопричини проблеми, тоді як проактивний моніторинг служить запобіжним заходом.

Хоча проактивний моніторинг часто передбачає «реагування» адміністраторів на невідповідності в продуктивності, ці дії все ще вважаються превентивними, оскільки кінцевий користувач ще не постраждав.

Чому проактивний моніторинг кращий за синтетичний моніторинг

Синтетичний моніторинг включає моделювання поведінки кінцевого користувача для тестування функціональності та виявлення проблем продуктивності та несправностей. Результати цих тестів використовуються для виявлення та усунення будь-яких збоїв, виявлених на шляхах користувача.

За своєю природою, синтетичний моніторинг можна вважати розширенням реактивного моніторингу, оскільки він спирається на вивчення досвіду кінцевого користувача і тому не може виявляти та діагностувати проблеми проактивно. Крім того, синтетичний моніторинг розглядає дані лише епізодично та не може протестувати весь набір можливих шляхів користувачів, що часто призводить до пропущених збоїв та проблем. Проактивний моніторинг, за визначенням, використовує цілісний підхід до IT-моніторингу та випереджає проблеми, шукаючи ранні індикатори.

Приклади проактивного моніторингу + ранні індикатори

Проблеми неможливо діагностувати, оцінюючи окремі IT-метрики. Однак, коли збираються історичні дані та встановлюється базовий рівень продуктивності, тенденції цих показників слугують ранніми індикаторами справжньої проблеми. Деякі приклади проактивного моніторингу ранніх індикаторів включають:

Приклад 1: Значна втрата пакетів

Пакет вважається «втраченим», коли він не досягає місця призначення після передачі. Системи покладаються на передачу пакетів для всієї інтернет-діяльності. У разі значної втрати пакетів кінцевий користувач може зіткнутися з повним перебоєм у роботі сервісу або повільним мережевим з’єднанням. Відсоток втрати пакетів необхідно контролювати, щоб переконатися, що на сервіс не впливають збої мережевого обладнання, несправності програмного забезпечення або порушення безпеки.

Приклад 2: Аномалії часу відгуку та тенденції до зниження

Забезпечення стабільної продуктивності передбачає встановлення базового рівня часу відгуку та визначення точок даних, які відрізняються від нього щонайменше на 100% або більше. Відхилення такого значного ступеня вимагає розслідування потенційних основних причин. Звідси мережеві адміністратори можуть дослідити розбіжність та вирішити будь-які проблеми, що перешкоджають продуктивності. Аномалія не завжди є показником серйознішої проблеми, проте закономірність низького або погіршеного часу відгуку, виявлена за допомогою проактивного моніторингу мережі, майже завжди є такою.

Приклад 3: Фактори навколишнього середовища

Визначення проактивного моніторингу виходить за рамки базових IT-метрик, таких як втрата пакетів та час відгуку. Навіть фактори навколишнього середовища, такі як температура в комп'ютерній кімнаті, підпадають під поняття проактивного моніторингу. Якщо ваша комп'ютерна кімната або центр обробки даних перегріється, ваше обладнання може зазнати величезних пошкоджень та можливого виходу з ладу. Такої події можна уникнути, просто встановивши датчики навколишнього середовища у вашому комп'ютері, які сповіщають вас про порушення певних температурних порогів.

Приклад 4: Проблеми з конфігурацією

Щось таке просте, як проблема з конфігурацією, може призвести до серйозного збою. Наприклад, інтерфейсне з'єднання на вашому маршрутизаторі відповідає за обробку інтернет-трафіку. Якщо це з'єднання перестає реагувати, це призводить до збоїв у роботі таких служб, як перегляд веб-сторінок та зовнішній трафік. Інші поширені помилки конфігурації включають незбереження конфігурації, випадкову зміну конфігурації пристрою або просто неправильне введення команд. Точні та функціональні конфігурації мають вирішальне значення для щоденної роботи вашої компанії, і успішні організації повинні мати можливість проводити проактивний моніторинг програм, щоб виявляти проблеми, пов'язані з неправильними конфігураціями, перш ніж вони вплинуть на кінцевого користувача.

Найкращі практики для проактивного IT-моніторингу

Створіть карту своїх IT-активів

Щоб контролювати свої пристрої, вам спочатку потрібно знати, де вони знаходяться відносно свого оточення. Збір цієї інформації та її відображення на проактивній карті моніторингу мережі не лише допоможе вам візуалізувати структуру вашої мережі, але й точно визначити, де виникають проблеми. Наявність процедур автоматичного виявлення та зіставлення пристроїв допоможе вам підтримувати актуальну картину вашого середовища.

Встановлення базових показників

Встановлення базових показників продуктивності на основі історичних даних пристроїв є основою для будь-якого проактивного моніторингу. Без базового рівня немає точки відліку для позначення точок даних як аномалій, запуску функцій сповіщень та сповіщень або спостереження за тенденціями. Базові показники слід визначати шляхом поєднання аналізу історичних даних та цільових показників, встановлених найкращими практиками.

Увімкнути сповіщення та сповіщення

Ваше програмне забезпечення для моніторингу повинно мати можливість проактивно попереджати IT-менеджерів, коли ресурс знаходиться на межі досягнення критичного порогу. Такі показники, як високий трафік на мережевому комутаторі або зменшення ресурсів на сервері, що підтримує критично важливі для бізнесу програми, необхідно враховувати якомога швидше. Менеджери повинні мати можливість налаштувати проактивні сповіщення, коли пристрій перебуває в стані тривоги, щоб вони могли усунути проблему, перш ніж це вплине на кінцевого користувача.

Майте інтелектуальний план потужностей

Наявність інтелектуального плану управління потужностями необхідна для забезпечення безперебійного взаємодії з кінцевим користувачем. Щоб випередити дефіцит або надлишок обчислювальних ресурсів, потрібен інтелектуальний та адаптивний план, що базується на поглибленому аналізі історичних даних. Організації повинні мати механізми для прогнозування своїх потреб у потужностях та проактивного моніторингу програм та інших активів на предмет будь-яких потенційних проблем із потужностями у найближчому майбутньому.

Оповіщення про тенденції, а не про порогові значення

Підхід до сповіщень за замовчуванням зазвичай полягає в налаштуванні сповіщень, які спрацьовують, коли показники перевищують певний поріг. Ви налаштовуєте свої інструменти так, щоб вони повідомляли вас, коли використання процесора сервера перевищує 80 відсотків, наприклад, або коли середній час відгуку програми перевищує 5 секунд.

Проблема з цими сповіщеннями на основі порогових значень полягає в тому, що вони, як правило, не повідомляють про проблеми, доки вони вже не перетворяться на збої. Якщо ваш сервер вже майже повністю завантажений процесором, може бути занадто пізно вирішувати проблему, перш ніж вона вийде з ладу.

Кращою стратегією є налаштування інструментів моніторингу таким чином, щоб вони сповіщали вас про відповідні тенденції, такі як стабільне збільшення використання

процесора або часу відгуку протягом фіксованого періоду часу. Таким чином, ви будете знати раніше, коли починає проявлятися проблемна тенденція, що збільшує ваші шанси на реагування до того, як щось дійсно станеться не так.

Розтин

Розбір інформації після збою, тобто огляди або звіти, які команди готують після збою, щоб оцінити, що пішло не так, є чудовим способом запобігти повторенню подібних проблем у майбутньому.

Вони також корисні для застосування проактивного підходу до моніторингу, оскільки дозволяють вашій команді бути в курсі тенденцій та даних, пов'язаних з перебоями в минулому. Ретельно оцінюючи минулі проблеми, ваші інженери мають кращі можливості для розпізнавання нових проблем у даних моніторингу в режимі реального часу.

Посібники реагування для проактивного моніторингу

Для фахівців з реагування на інциденти та IT-інженерів є поширеною практикою розробляти методичні посібники з реагування на інциденти, які допомагають їм вирішувати певні типи інцидентів. Однак, методичні посібники часто призначені для усунення проблем після того, як вони вже перетворилися на інциденти, а не для проактивного вирішення потенційних проблем на ранніх стадіях.

Ось чому варто інвестувати в посібники, які також враховують потреби раннього, проактивного вирішення проблем. Не обмежуйте свої посібники реагуванням на серйозні інциденти.

Зіставлення показників з впливом на бізнес

Не всі потенційні проблеми, які виявляють ваші інструменти моніторингу, матимуть однаковий вплив на бізнес. Іноді сервер може вийти з ладу або програма може вийти з ладу, фактично не порушуючи роботу користувачів, оскільки є резервні ресурси.

З цієї причини розумно класифікувати сповіщення залежно від рівня їхнього впливу на бізнес. Це допоможе вашій команді зрозуміти, на які проблеми, що виникають, слід звернути найбільшу увагу, а які можна відкласти, доки не збереться більше даних. В іншому випадку вони можуть витратити час на спроби вирішити некритичні проблеми проактивно, що ускладнить вирішення справді проблемних.

Як впровадити проактивний моніторинг

Крок 1: Визначте та під’єднайте своє обладнання

Скільки у вас маршрутизаторів і комутаторів? Скільки кінцевих точок? Окрім загального переліку пристроїв, вам потрібно знати, де розташований кожен з них і як він підключається до решти вашої мережі. Проактивні рішення для моніторингу з можливостями картографування дозволяють візуалізувати весь ваш IT-ландшафт, автоматично додавати та видаляти обладнання, а також відстежувати дані про стан пристроїв у режимі реального часу.

Крок 2: Визначте свої найважливіші активи

На цьому етапі ви повинні визначити, яка інформація є найважливішою для моніторингу та збору. IT-середовища можуть мати десятки тисяч кінцевих точок та пристроїв, тому важливо точно визначити, які з них мають найбільший вплив на успіх вашої організації. Пристрої в цій категорії зазвичай включають комутатори, маршрутизатори, брандмауери та сервери. Після визначення ви повинні визначити, які показники потрібно відстежувати, щоб забезпечити оптимальну роботу пристрою, і чи можете ви ділитися цими даними зі своїми серверами.

Крок 3: Впровадження проактивного рішення для моніторингу

Щойно ви отримаєте уявлення про свою IT-систему та чітко визначите структуру пріоритетів, ви зможете впровадити програмне забезпечення для моніторингу, яке автоматично записуватиме та аналізуватиме дані про пристрої та інфраструктуру всієї організації. На цьому етапі вам буде запропоновано налаштувати базові рівні та порогові значення продуктивності.

Після встановлення цих параметрів та запису історичних даних програмне забезпечення, ймовірно, зможе звітувати про показники пристрою, робити прогнози та

виявляти будь-які тенденції, які вимагатимуть розслідування потенційних причин. Це також сприятливий час для налаштування сповіщень на основі винятків для елементів та подій, які ви вважаєте критичними.

Крок 4: Підтримуйте свою інфраструктуру в належному стані

Ви повинні постійно переконатися, що основні комутатори, маршрутизатори та брандмауери, на яких базується ваша мережа, підтримують сучасні протоколи моніторингу продуктивності. Якщо ні, то ви будете обмежені в типі даних про продуктивність, які можете збирати, що значно ускладнить вам своєчасний моніторинг та вирішення будь-яких проблем.

Крок 5: Додайте кібербезпеку, автоматизацію та аналітику

Після впровадження основи вашої стратегії проактивного моніторингу ви можете додавати рівні для підвищення ефективності та заповнення прогалин у безпеці. Наприклад, автоматизацію можна інтегрувати для розгортання процедур усунення недоліків, щоб у разі перевищення або падіння показників нижче певного порогу заздалегідь запрограмована послідовність вирішувала проблему або передавала її відповідному персоналу.

Функції кібербезпеки, такі як виявлення та запобігання вторгненням, можуть використовувати вашу інфраструктуру моніторингу та зібрані нею дані для виявлення шкідливої поведінки у ваших системах. Автоматизовану аналітичну звітність можна налаштувати для генерування та надання зацікавленим сторонам зворотного зв'язку щодо ключових тенденцій і закономірностей у даних, що дозволить вашій організації постійно підвищувати продуктивність.

Електронне управління документами (СЕД) працює за допомогою інтелектуального захоплення та автоматизованого індексування, перетворюючи неструктуровані дані на стратегічні цифрові активи. У провідних системах СЕД оптичне розпізнавання символів (OCR) працює на базі штучного інтелекту (ШІ) для вилучення даних, метаданих та контексту зі сканованих файлів, електронних листів або форм.

Тим часом, алгоритми машинного навчання можуть класифікувати документи на основі змісту, призначення або нормативних вимог.

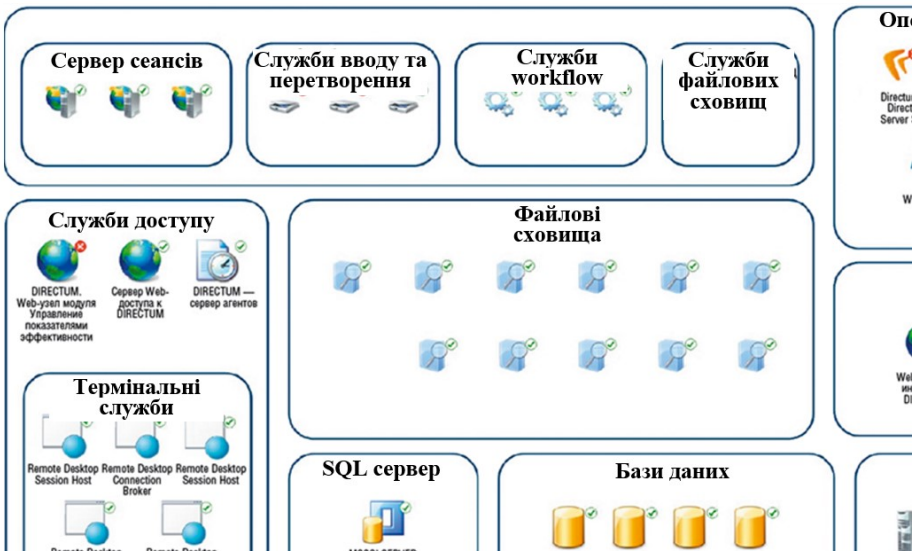

Рисунок 1 – Структурна схема системи

Після оцифрування документи зберігаються в централізованому хмарному сховищі, що забезпечує їх миттєвий пошук. Основні методи категоризації включають:

– Тегування метаданих (наприклад, ідентифікатор клієнта, назва проекту, термін дії).

– Повнотекстовий пошук на базі обробки природної мови (NLP).

– Контроль версій з відстеженням редагувань та затверджень.

– Автоматизовані правила зберігання для забезпечення відповідності нормативним вимогам.

Автоматизація робочих процесів спрощує операції: попередньо визначені правила направляють документи на перевірку, отримання електронних підписів або архівування.

Водночас, інструменти для співпраці в режимі реального часу дозволяють кільком користувачам одночасно редагувати, коментувати або затверджувати файли. Це усуває конфлікти версій та пришвидшує такі процеси, як укладення договору чи відповіді на аудит.

Зрештою, розширена аналітика та інтеграція перетворюють документи на стратегічні інструменти: штучний інтелект визначає тенденції або аномалії у використанні документів, а API-інтерфейси з'єднують систему СЕД з платформами ERP, CRM або відповідності. Варіанти перевірки на основі блокчейну можуть забезпечити захист від несанкціонованого доступу, а автоматизовані зашифровані резервні копії можуть захистити документи протягом усього їхнього життєвого циклу.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів проактивного моніторингу мережевого електронного документообігу. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем проактивного моніторингу мережевого електронного документообігу.

– Досліджена система проактивного моніторингу мережевого електронного документообігу.

– На основі отриманих результатів досліджень створена програмна реалізація системи проактивного моніторингу мережевого електронного документообігу. Розроблені алгоритми дозволяють успішно вирішувати завдання проактивного моніторингу мережевого електронного документообігу. 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. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
8. 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.
9. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
10. 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.
11. 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.
12. 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.
13. 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.
14. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
15. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
16. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
17. 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.
18. 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.
19. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
20. 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.
21. 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.
22. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
23. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
24. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
25. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
26. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
27. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
28. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
29. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
30. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
31. Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.