УДК 004

М.Кілочицька, магістр гр. КН-22МЗ,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВІДДАЛЕНОГО АДМІНІСТРУВАННЯ КОМП'ЮТЕРА У МЕРЕЖІ ДЛЯ ОРГАНІЗАЦІЇ ТЕХПІДТРИМКИ

У статті розроблено програмне забезпечення, яке призначено для системи віддаленого адміністрування комп'ютера у мережі для організації техпідтримки. Метою розробки є дослідження та програмна реалізація системи віддаленого адміністрування комп'ютера у мережі для організації техпідтримки. Об'єктом дослідження є процес віддаленого адміністрування комп'ютера у мережі для організації техпідтримки. Предметом дослідження є методи віддаленого адміністрування комп'ютера у мережі для організації техпідтримки. Методи дослідження базуються на методах теорії телекому, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи віддаленого адміністрування комп'ютера у мережі для організації техпідтримки. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Віддалене керування комп'ютерами для надання віддаленої підтримки сьогодні здобуває все більшу популярність. Це цілком обґрунтовано, тому що має безліч плюсів, наприклад, віддалене керування комп'ютером через Інтернет. Замислюючись про те, чи потрібна вам ця послуга віддалене керування комп'ютером, варто зрозуміти, що вона собою представляє.

У багатьох користувачів комп'ютерів і інших IT-систем може виникнути питання доцільності віддаленого керування, про те, наскільки воно вигідно й корисно. При цьому користь від нього очевидна:

1. Виключається необхідність виклику IT-персоналу при виникненні неполадок.
2. Виключається можливість раптової зупинки роботи через певні несправності, тому що дана послуга дозволяє здійснювати безперервний онлайн аудит системи й вчасно діагностувати й усувати проблеми по засобах віддаленого робочого стола.
3. Немає необхідності подовгу очікувати фахівця, щоб довідатися як підключиться до комп'ютера друга, тому що при виникненні неполадок фахівці, що здійснюють дистанційний контроль над станом системи, можуть приступитися до їхнього усунення негайно, задіявши remote desktop.
4. Підвищуються загальні результати роботи IT-систем в організації.

Це лише основні переваги, який характеризується робочий стіл віддалений доступ. І вже при обліку перерахованих переваг можна зробити вивід, що керування комп'ютером віддалено може стати необхідним при будь-яких умовах.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-20] було виявлено певні прогалини у забезпеченні системи віддаленого адміністрування комп'ютера у мережі для організації техпідтримки.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи віддаленого адміністрування комп'ютера у мережі для організації техпідтримки.

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

– Огляд існуючих систем віддаленого адміністрування комп’ютера у мережі для організації техпідтримки.

– Дослідження системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки.

– Програмна реалізація системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки.

Об’єктом дослідження є процес віддаленого адміністрування комп’ютера у мережі для організації техпідтримки.

Предметом дослідження є методи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки.

Методи дослідження базуються на методах теорії телекому, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Переваги віддаленої підтримки. Оперативність. Фахівцеві служби техпідтримки користувачів не потрібно виїжджати до робочого місця користувача (в офіс або додому), щоб вирішити проблему з комп'ютером, а досить запустити віддалений робочий стіл.

Широкі можливості для налаштування програмного забезпечення, устаткування й бізнес програмного забезпечення

С допомогою віддаленого доступу можна вирішувати проблеми, пов'язані із програмним забезпеченням, уникаючи відряджень: установка й налаштування програм, налаштування операційної системи, а іноді навіть і з устаткуванням (наприклад, проблеми з підключенням) – у цьому випадку теж можна допомогти віддалена підтримка, якщо направляти дії клієнта (у тому числі й за допомогою голосових повідомлень).

Економія часу й грошей

Вдаючись до допомоги віддаленої підтримки, вдається заощадити значну суму коштів і часу, як з боку служби техпідтримки, так і для користувача завдяки так званим відрядженням онлайн.

Невимогливість до каналу зв'язку й апаратному забезпеченню

Сучасне програмне забезпечення оптимізоване для каналів зв'язку з невисокою пропускною здатністю – можна віддалено працювати не тільки через ADSL, але й по GPRS і навіть по dial-up. Також віддалена підтримка не вимагає потужного комп'ютера – підійде й звичайна офісна робоча конячка.

Високий рівень безпеки

Всі передані дані (зображення на екрані, текстові й голосові повідомлення) піддаються шифруванню за допомогою стійких криптоалгоритмів. Є можливість парольного захисту й фільтрації доступу по IP-адресах (тобто доступ можна дозволити тільки із заданих вами комп'ютерів і підмереж).

Розмаїтість способів як управляти віддаленим комп'ютером

Програмне забезпечення для віддаленої підтримки може працювати в декількох режимах – керування комп'ютером віддалено, ассістування, перегляд робочого стола, копіювання файлів на комп'ютер користувача й назад, адміністрування.

Нові можливості для навчання

Використовуючи віддалену підтримку в режимі ассістування, можна організувати дистанційне навчання клієнтів або студентів: проводити навчальні онлайн семінари, віддалені курси семінари й т.п.

Розробка структурної схеми

Структурна схема розробленого програмного забезпечення системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки складається з наступних шести компонентів:

– Головний сервер.

– Сховище даних.

– SQL-сервер і база даних.

– Блок системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки.

– Клієнтський реєстратор.

– Центр керування.

Головний сервер

Програмне забезпечення основного сервера, що звичайно розташовується на тій же машині, що й SQL-сервер бази даних, забезпечує такі послуги, як відновлення програмного забезпечення й перевірку ліцензій для всіх комп'ютерів, зконфігурованих під додаток «Клієнтський реєстратор».

Сховище даних

Всі додатки «Клієнтський реєстратор» передають свою інформацію в сховище «Сховище даних» через попередньо встановлені інтервали часу. Ця інформація містить дані про подію, образи екранів і вкладення в електронну пошту. Потім «Сховище даних» пересилає ці дані в базу даних на SQL-сервері й зберігає образи екранів і вкладення електронної пошти в мережному каталозі, доступному через додаток «Блок системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки».

SQL-сервер і база даних

SQL-сервер і база даних зберігають всі записані події, зібрані за період часу на контрольованих комп'ютерах. Керування базою даних, включаючи резервне копіювання й архівування, виробляється через додаток «Блок системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки».

Блок системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки

Додаток «Блок системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки» є центральним пунктом для моніторингу дій на віддаленому комп’ютері у розроблене програмне забезпечення системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки. Додаток «Блок системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки» направляє запити до SQL-сервера на одержання даних про подію й витягає образи екрана й поштові вкладення з мережного каталогу. «Блок системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки» є додатком Windows на основі графічного інтерфейсу .NET. Є можливість установити в мережі більше одного додатка «Блок системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки». Також можливо зконфігурувати кілька баз даних, до кожної з яких буде доступ за допомогою «Блок системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки».

Основний сервер, сховище «Сховище даних» і SQL-сервер з базою даних можуть перебувати на одному комп'ютері рівня сервера або можуть бути розподілені між декількома машинами для поліпшення продуктивності. Додаток «Блок системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки» і «Центр керування» можуть перебувати на одній машині, але дуже часто ці компоненти ізольовані друг від друга по міркуваннях безпеки. Наприклад, особа, що відповідає за установку клієнтських компонентів, може бути не вповноважене для перегляду зібраних даних. В організації можуть бути розгорнуті кілька копій додатка «Блок системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки». Наприклад, можна надати копію додатка менеджерові по кадрам або лінійному керівникові, щоб він міг спостерігати за співробітниками для реалізації системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки. Перегляд з кожного екземпляра «Блок системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки» може бути обмежений для особи, що виконує аналіз даних, доступом тільки до інформації, що має відношення до системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки.

Запис подій

У розробленому програмному забезпеченні системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки реалізована передова технологія моніторингу комп'ютерів, що автоматично записує всі дії, включаючи що відправляються й прийняті повідомлення електронної пошти, спілкування в чатах і системах миттєвого обміну повідомленнями, відвідувані веб-сайти, набрані на клавіатурі дані, передані / надруковані / збережені файли й багато чого іншого.

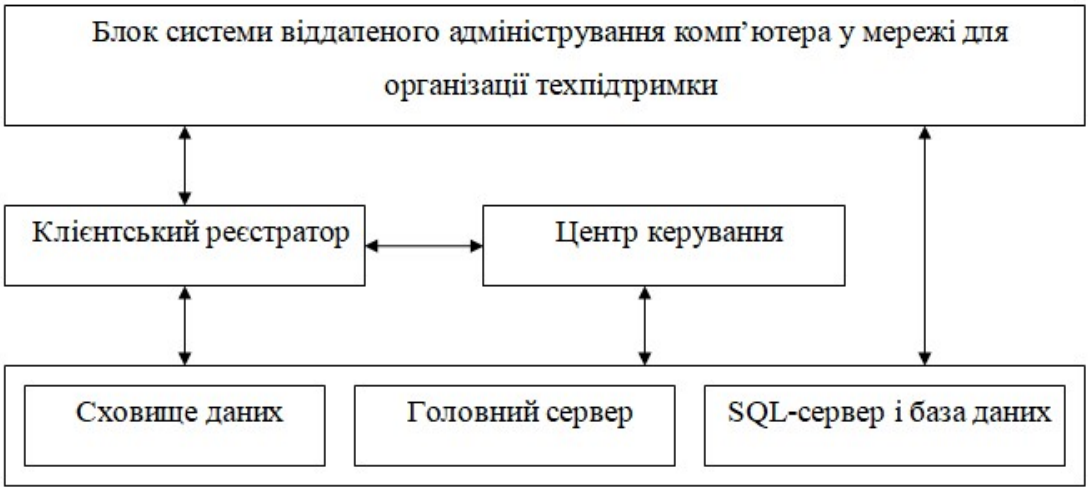

Рисунок 1 – Структурна схема системи

Опції й параметри конфігурації клієнта розробленого програмного забезпечення системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки

Додаток «Реєстратор» відповідає за реєстрацію всіх дій і запис образів екранів зі спостережуваних комп'ютерів і передачу цієї інформації в додаток «Сховище даних». Додаток «Реєстратор» добре конфігурується й може бути тонко настроєне для кожного екземпляра установки. Звичайно «Реєстратор» конфігурується за допомогою розробленого програмного забезпечення системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки «Центр керування» і потім установлюється на клієнтській машині.

Клієнтський реєстратор

Цей програмний компонент конфігурується й установлюється на кожний комп'ютер, що підлягає моніторингу й може працювати в “схованому режимі”, так що співробітники не будуть знати про спостереження за ними. Додаток «Клієнтський реєстратор» добре конфігурується й може використовуватися для фільтрації й блокування специфічного трафіку, диспетчеризації доступу до мережі, генерації оповіщення по ключових словах і інших функціях.

Центр керування

Всі клієнтські додатки «Клієнтський реєстратор» конфігуруються й управляються додатком розробленого програмного забезпечення системи віддаленого адміністрування комп’ютера у мережі для організації техпідтримки «Центр керування», що використовується для установки клієнтських додатків на комп'ютери, розташовані у внутрішній мережі компанії. Додаток «Центр керування» також відповідає за конфігурування сховища даних «Сховище даних».

Поради щодо забезпечення підтримки мережі для віддалених працівників

Підприємства повинні модернізувати свої мережі для підтримки віддаленої роботи, а IT-команди забезпечують належну пропускну здатність і безпеку мереж, а також спеціальну допомогу для віддалених працівників.

Віддалені працівники потребують надійної мережевої підтримки з боку керівництва організації.

З початком пандемії COVID-19 зросла популярність дистанційної роботи, яку також називають дистанційною роботою. Підприємствам раптово довелося підтримувати сотні чи тисячі віддалених працівників, і командам керування мережею потрібно було адаптуватися. Віддалена робота продовжує залишатися популярним варіантом серед працівників, тому компаніям важливо усвідомлювати, що віддалені працівники потребують іншої підтримки, ніж співробітники в офісі.

Постійною метою мережевих команд є забезпечення оптимальної підтримки, безпеки, надійності та продуктивності як для особистих, так і для віддалених співробітників. У рамках цих зусиль команди керівництва запровадили стратегії модернізації та покращили конфігурацію мережі та керування безпекою.

IT-адміністратори відповідають за сприяння та керування дистанційною роботою. Щоб забезпечити найкращі можливі результати для віддалених працівників, організаціям важливо мати цілеспрямований і проактивний підхід до віддаленої роботи. У цій статті наведено вказівки щодо моніторингу та керування продуктивністю та безпекою мережі для віддалених працівників. Також надається контрольний перелік дій, яких команди мережі можуть дотримуватися, щоб забезпечити мережеву підтримку для цих співробітників.

Правила та процедури віддаленої роботи

Офіційна політика щодо технології віддаленої роботи є важливим компонентом програми. Ця політика відрізняється від загальної корпоративної політики щодо віддаленої роботи. Він зосереджений насамперед на технологіях, необхідних віддаленим працівникам для виконання своїх обов'язків у безпечному середовищі. IT-команди повинні документувати, регулярно оновлювати та поширювати процедури віддаленої роботи. Таким чином віддалені працівники можуть безпечно підключатися до необхідних ресурсів.

Пристрої кінцевого користувача

На початку дистанційної роботи співробітники зазвичай використовували свої персональні ноутбуки або комп'ютери. Однак в ідеалі організації видають віддаленим працівникам налаштовані та налаштовані ноутбуки. За такої домовленості співробітники все ще можуть використовувати особисті пристрої, такі як смартфони, планшети та інші подібні пристрої.

Підприємства повинні налаштувати на кожному пристрої відповідне програмне забезпечення для безпечного доступу до корпоративної VPN або іншої корпоративної мережі. Замість таких домовленостей IT-відділи повинні забезпечити конфігурацію персональних пристроїв віддалених працівників для доступу до ресурсів компанії. Віддаленим користувачам може знадобитися мати обліковий запис компанії на своїх пристроях на додаток до особистого.

Мережеві ресурси для віддаленої роботи

Хоча VPN є безпечним методом віддаленого підключення до корпоративних ресурсів, організаціям може бути складно отримати достатню кількість ліцензій VPN для підтримки кожного співробітника. Додайте до цього витрати на механізми доступу, такі як двофакторна (2FA), багатофакторна автентифікація (MFA) або керування паролями, щоб забезпечити безпечний вхід до ресурсів компанії. У цьому випадку інфраструктура корпоративної мережі компанії може бути кращим засобом для віддалених працівників.

Управління смугою пропускання для роботи віддалених працівників залишається важливою діяльністю. Віддалені користувачі можуть підключатися до VPN своєї компанії через Інтернет, тому необхідну пропускну здатність у центрі обробки даних компанії може знадобитися суттєве збільшення, щоб впоратися з попитом. Це може означати переговори з операторами LAN і WAN щодо додаткової пропускної здатності. Програмно визначені глобальні мережі також можуть оптимізувати пропускну здатність.

Безпека віддаленої роботи

Віддалена робота завжди підвищує занепокоєння щодо безпеки. Хоча VPN мають власні атрибути безпеки, важливо розширити безпеку в додаткових напрямках. Наприклад, 2FA і MFA є ключовими методами доступу. Шифрування даних — у спокої та в русі — є ще

однією важливою діяльністю. Деякі технології забезпечують безпеку майже будь-якої транзакції даних. Моделі безпеки з нульовою довірою додатково підвищують атрибути безпеки.

Окрім основної діяльності, регулярно аналізуйте ризики безпеки, загрози та вразливі місця. Це може допомогти виявити потенційних загроз, які можуть порушити роботу віддалених мереж за допомогою:

- Пошкодження або викрадення даних під час передачі.
- Знайомство з фішинговими шахрайствами.
- DDoS атаки.
- Атаки програм-вимагачів.

Команди можуть допомогти зберегти безпеку мережі, розгорнувши системи безпеки, які контролюють стан віддаленого з'єднання. Ці системи безпеки можуть запускати тести на проникнення, а також симулювати злами та атаки, щоб забезпечити стабільні та справні віддалені з'єднання.

Віддалені працівники повинні мати у своїх системах антивірусні програми, програми-вимагачі, засоби контролю доступу та шифрування, щоб забезпечити безпеку на межі мережі. Підготовлені компанією ноутбуки та інші робочі станції можуть допомогти досягти цього.

Віддалене адміністрування роботи

Компанії з віддаленими працівниками повинні мати групи IT-мереж і безпеки, які займаються їх роботою. Оптимізуйте внутрішні відділи служби підтримки для підтримки віддалених працівників. Це може означати відокремлення віддаленої допомоги від внутрішньої діяльності з підтримки. Якщо це неможливо, переконайтеся, що у команд підтримки є необхідні інструменти для віддаленої діагностики проблем і надання рішень.

Заміна обладнання на місці неможлива для віддалених працівників. Таким чином, працівникам може знадобитися самостійно отримати товари на заміну або чекати на доставку.

Постійний моніторинг усіх віддалених співробітників та їхніх мережевих з'єднань необхідний для швидкого виявлення потенційних проблем. Доступні численні засоби діагностики мережі. Головне – вибрати інструменти, які забезпечують як віддалений моніторинг, так і діагностику. Додаткова адміністративна діяльність включає наступне:

- За потреби підключайте пристрої.
- Перегляньте й оновіть брандмауер і правила системи виявлення вторгнень /системи запобігання вторгненням.
- Оцініть використання та тенденції VPN.
- Керуйте сегментацією мережі, якщо вона використовується.
- Відстежуйте зміни трафіку WAN і реагуйте на них.
- Перевірте підключення віддаленого доступу.
- Аналізуйте ризики, загрози та вразливі місця.
- Відстежуйте використання хмарних технологій, які підтримують віддалену роботу.
- Перегляньте та оновіть плани аварійного відновлення, пов'язані з віддаленою роботою.
- Встановіть резервні механізми на випадок збою мережі.
- Надайте поради та вказівки віддаленим працівникам, зокрема тренінги щодо найкращих практик та ознайомлення з дистанційною роботою.
- Переконайтеся, що ресурси для співпраці, такі як Microsoft Teams і Zoom, доступні та працюють.

Віддалені та офісні працівники

Співробітники в офісі мають доступ до всіх відповідних мережевих ресурсів і ресурсів безпеки. Співробітники в офісі можуть швидко вирішити виниклі проблеми та залучити IT-спеціалістів у разі необхідності.

Навпаки, віддалені працівники мають більший ризик для своєї здатності виконувати свої обов'язки. Вони покладаються на віддалені мережі, такі як Wi-Fi і доступ до Інтернету через місцевого оператора, які можуть бути ненадійними на 100%. Віддаленим співробітникам потрібні заходи безпеки та мереж, такі як 2FA/MFA та VPN.

Віддалена діагностика проблем і усунення несправностей може бути більш складною. Настільні інструменти повинні мати можливість синхронізуватися з системами центру обробки даних. Інструменти для співпраці необхідні для зустрічей і підтримки зв'язку. Повинні діяти процедури надзвичайних ситуацій для усунення незапланованих збоїв.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів віддаленого адміністрування комп'ютера у мережі для організації техпідтримки. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем віддаленого адміністрування комп'ютера у мережі для організації техпідтримки; Досліджена система віддаленого адміністрування комп'ютера у мережі для організації техпідтримки; На основі отриманих результатів досліджень створена програмна реалізація системи віддаленого адміністрування комп'ютера у мережі для організації техпідтримки. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання віддаленого адміністрування комп'ютера у мережі для організації техпідтримки. 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. 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.
2. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. Smirnov A.A., Kuznetsov 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.
19. 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.
20. 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.
21. 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.