УДК 004

А.Мукієнко, магістр гр. КН-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ХМАРНОГО СЕРВІСУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РОЗУМНОГО БУДИНКУ

У статті розроблено програмне забезпечення, яке призначено для системи хмарного сервісу забезпечення безпеки розумного будинку. Метою розробки є дослідження та принципи побудови системи хмарного сервісу забезпечення безпеки розумного будинку. Об'єктом дослідження є процес хмарного сервісу забезпечення безпеки розумного будинку. Предметом дослідження є методи хмарного сервісу забезпечення безпеки розумного будинку. Методи дослідження базуються на методах хмарних технологій, методах інтернету речей, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи хмарного сервісу забезпечення безпеки розумного будинку. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

хмарний сервіс, забезпечення безпеки, розумний будинок

Постановка проблеми. В останні роки хмарні системи домашньої безпеки революціонізували спосіб захисту наших домівок. Ці системи використовують можливості хмарних обчислень, щоб пропонувати розширені функції, віддалений доступ та безперешкодну інтеграцію з пристроями розумного дому.

Хмарні системи домашньої безпеки використовують підключені до Інтернету пристрої та хмарні обчислення для забезпечення моніторингу, оповіщення та керування в режимі реального часу. На відміну від традиційних систем безпеки, які часто потребують тривалої проводки та локального сховища, хмарні системи зберігають дані на безпечних зовнішніх серверах, що забезпечує легший доступ та керування.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи хмарного сервісу забезпечення безпеки розумного будинку.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи хмарного сервісу забезпечення безпеки розумного будинку.

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

– Огляд існуючих систем хмарного сервісу забезпечення безпеки розумного будинку.
– Дослідження системи хмарного сервісу забезпечення безпеки розумного будинку.
– Програмна реалізація системи хмарного сервісу забезпечення безпеки розумного будинку.

Об'єктом дослідження є процес хмарного сервісу забезпечення безпеки розумного будинку.

Предметом дослідження є методи хмарного сервісу забезпечення безпеки розумного будинку.

Методи дослідження базуються на методах хмарних технологій, методах інтернету речей, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Очікується, що світовий ринок систем безпеки житлових приміщень до 2027 року перевищить 13 мільярдів доларів, зростаючи на 24,58%

щорічно. Оскільки загальна кількість систем «розумних будинків» досягла 258,54 мільйона, очевидно, що люди почали усвідомлювати важливість систем безпеки розумних будинків і більше не розглядають безпеку житлових приміщень як розкіш.

Як показують опитування, сучасні клієнти охоче інвестують у розумні системи безпеки, зокрема житлові, та платитимуть вищу орендну плату за розумні будинки.

У цьому розділі ми розповімо, як працює система безпеки розумного дому, перерахуємо її обов'язкові функції та розглянемо приклади популярних програм для домашньої безпеки. Ми почнемо з визначення розумної системи захисту для дому та перейдемо до її переваг.

Інтелектуальна система безпеки для житла – це мережа пристроїв, які працюють синхронно один з одним, забезпечуючи розширений захист та моніторинг будинку.

Основні компоненти такої мережі включають наступне:

1. Інструменти обмеження доступу

Інтелектуальні замки дозволяють домовласникам дистанційно замикати та відмикати свої двері за допомогою смартфона або голосових команд. Найбільш інноваційні замки оснащені сканерами відбитків пальців, які набагато безпечніші, ніж традиційні замки з кодом та паролем.

2. Детектори активності

Сучасні домогосподарства використовують датчики, що фіксують рух, розбиття скла, відкриття дверей та вікон, а також дим або шкідливі речовини та викиди. Ці датчики відстежують незвичайну активність та зміни в навколишньому середовищі та повідомляють про них мешканцям.

3. Спостереження

Відеоспостереження також є невід'ємною частиною потужної мережі безпеки житлового будинку. Внутрішні та/або зовнішні камери контролюють будівлю, записують відео та дозволяють користувачам переглядати відео в реальному часі зі своїх телефонів або комп'ютерів.

4. Звукові сирени

Ще однією традиційною частиною системи безпеки є звукова сигналізація. Сучасні засоби спостереження за будинком використовують звукові сирени або дзвінки для попередження мешканців та стримування зловмисників.

5. Голосові помічники

Деякі інтелектуальні платформи захисту дому інтегрують популярні голосові помічники, що дозволяє власникам керувати ними за допомогою голосових команд.

6. Служба моніторингу

Багато інтелектуальних систем захисту дому мають професійну службу моніторингу, здатну сповістити правоохоронні органи про випадок злому або іншої термінової ситуації.

7. Кнопки екстреного виклику

Це фізичні або віртуальні пристрої, які дозволяють мешканцям миттєво викликати екстрену допомогу у разі кризи чи загрози. Кнопки паніки призначені для швидкого реагування на потенційно небезпечні ситуації, такі як проникнення зі зломом, невідкладна медична допомога чи будь-які інші загрозливі обставини.

8. Панель керування/хаб

Панель керування об’єднує всі інші мережеві компоненти в один центральний вузол та керує ними. Вона діє як централізований вузол для ввімкнення та вимкнення системи, керування розумною домашньою технікою та отримання сповіщень.

Інтеграція цих пристроїв створює рішення, яке можна налаштувати відповідно до вподобань мешканця та забезпечити повний захист.

Безпека розумного дому: ключові принципи роботи

Як працює система безпеки розумного дому? Домашні мережі безпеки включають численні інтелектуальні пристрої, які підключаються до центральної панелі керування.

Остання підключається до Інтернету, що дозволяє власникам відстежувати її через додаток та керувати нею дистанційно за потреби.

Наприклад, якщо у вашій квартирі спрацював датчик, ваш телефон отримає сигнал. Додаток безпеки попросить вас вжити заходів або вимкнути сигналізацію.

Платформи розумного дому використовують інноваційні технології для виявлення та реагування на можливі загрози в режимі реального часу. Вони також можуть синхронно працювати з іншими розумними пристроями, забезпечуючи комплексне рішення для домашньої автоматизації та безпеки.

Переваги системи безпеки житлового будинку

Розумні системи безпеки житлових приміщень перевершують звичайні за кількома показниками. Мешканці можуть бути впевнені, що їхня власність у безпеці, коли її охороняє інтелектуальна мережа захисту. Користувачі також можуть перевіряти її будь-коли дистанційно.

Більш конкретно, переваги включають наступне:

Віддалене відстеження та управління

Сучасні мережі безпеки керуються за допомогою дистанційного керування. Мешканці також можуть спілкуватися з відвідувачами або давати вказівки домашньому персоналу в дистанційному режимі.

Миттєві сповіщення

Якщо щось відхиляється від норми, користувачі отримують миттєві сповіщення через мобільні додатки домашньої безпеки. Наприклад, домовласник отримуватиме своєчасні сповіщення про ввімкнений електроприлад, протікання крана або неочікуваного відвідувача.

Тільки дійсні виклики служби безпеки

Боротьба з хибними тривогами може бути складною. Якщо аварійній бригаді доручено забезпечити безпеку будинку, власникам можуть фактично стягнути чималу суму за хибний виклик охорони. Завдяки інтелектуальним системам розумного дому хибні тривоги більше не є проблемою.

Запобігання вторгненню

Сповіщення про те, що ввімкнено систему захисту розумного дому, слугує ідеальним захистом від грабіжників та зловмисників. Більшість злочинців, які сподіваються на швидкий та легкий доступ, легко зупиняться завдяки інтелектуальній системі захисту дому.

Важко відключити

Зловмисникам також досить важко вивести з ладу житлову мережу безпеки, просто відрізавши шнур. Такі платформи використовують бездротові технології та їх нелегко вивести з ладу.

Фінансово виправдано

Окрім захисту та безпеки вашої власності, хороша система цифрової безпеки може фактично забезпечити кращі страхові пакети для власників нерухомості, що робить її розумною інвестицією.

Комплексний захист, моніторинг у режимі реального часу, фінансові переваги та чудова зручність використання роблять програми та системи безпеки для розумного дому популярним вибором для сучасних технічно підкованих власників житлової нерухомості. У наступному розділі ми розглянемо приклади деяких популярних мобільних програм та систем домашньої безпеки.

Основні характеристики мобільного додатку для домашньої безпеки

Створення мобільного застосунку є невід'ємною частиною побудови системи безпеки для житлових приміщень. Набір функцій відрізнятиметься залежно від функціональності та компонентів рішення, проте деякі функції є абсолютно необхідними.

Також, якщо ви хочете, щоб ваш додаток працював з більшістю доступних розумних побутових пристроїв, подумайте про впровадження базового набору функцій.

8. Дистанційне керування

Ваш мобільний додаток для безпеки повинен дозволяти користувачам дистанційно отримувати доступ до своєї мережі безпеки та керувати нею. Це включає такі функції, як встановлення та зняття системи з охорони, керування інтелектуальними пристроями та налаштування параметрів з будь-якого місця, де є підключення до Інтернету.

9. Своєчасні сповіщення

Додаток має надсилати сповіщення в режимі реального часу на мобільні пристрої користувачів про різні події, такі як порушення безпеки, виявлення руху, відкриття дверей/вікон або спрацьовування сигналізації. Користувачі повинні отримувати сповіщення своєчасно та мати можливість вжити негайних заходів за потреби.

10. Спостереження в реальному часі

Додаток для домашньої безпеки повинен забезпечувати пряму трансляцію відео з камер спостереження, розташованих зовні та всередині будівлі. Власники будинків повинні мати можливість переглядати зображення з камер у режимі реального часу, перемикатися між різними камерами та мати можливість двостороннього аудіозв'язку, якщо камери його підтримують.

11. Історія подій та відтворення відео

Додаток має зберігати журнали історії подій, включаючи позначки часу та деталі минулих подій безпеки. Крім того, він має надавати користувачам доступ до записаних відеоматеріалів з камер для відтворення, що дає їм змогу переглядати конкретні інциденти або події.

12. Геозонування

Геозонування – це корисна функція, яка дозволяє користувачам визначати віртуальні межі або зони. Додаток має підтримувати можливості геозонування, що дозволить користувачам отримувати автоматичні сповіщення або запускати певні дії на основі їхнього місцезнаходження, такі як вхід або вихід із зазначеної зони.

13. Персоналізація та налаштування

Найкращі системи безпеки для розумного дому повинні пропонувати варіанти налаштування відповідно до індивідуальних уподобань. Клієнти повинні мати можливість налаштовувати параметри, розклади та правила відповідно до своїх конкретних потреб. Це може включати налаштування різних режимів (наприклад, «вдома», «не вдома», «сон»), коригування параметрів сповіщень або створення правил автоматизації.

14. Керування користувачами та доступом

Мобільний додаток безпеки повинен дозволяти користувачам додавати та видаляти облікові записи користувачів, призначати різні рівні доступу та дозволів, а також налаштовувати тимчасовий або гостьовий доступ для таких осіб, як члени родини, друзі або постачальники послуг.

15. Інтеграція

Інтеграція з іншими інструментами та платформами покращує загальну функціональність та зручність системи захисту житлових приміщень. Додаток повинен підтримувати інтеграцію із сумісними пристроями, дозволяючи користувачам керувати кількома функціями розумного дому з одного інтерфейсу.

16. Відстеження стану та стану системи

Додаток має надавати інформацію про стан та справність пристроїв системи. Це включає відстеження рівнів заряду батареї, стану підключення та будь-яких потенційних проблем або несправностей. Користувачів слід попереджати про низький рівень заряду батареї або проблеми з підключенням, які можуть вплинути на ефективність платформи.

17. Ресурси підтримки та допомоги

Найкращі програми для систем безпеки розумного дому повинні містити ресурси підтримки та довідки, такі як поширені запитання, навчальні посібники, посібники з усунення несправностей або прямий контакт зі службою підтримки клієнтів. Це гарантує, що

користувачі зможуть легко знайти допомогу, якщо у них виникнуть будь-які проблеми або є запитання щодо програми чи їхньої системи безпеки.

Завдяки поєднанню цих основних функцій, програмне забезпечення для систем домашньої безпеки може забезпечити користувачам зручний та ефективний контроль над їхньою мережею інтелектуального захисту, забезпечуючи безперебійний та зручний користувацький досвід.

У найближчі роки технології розумного дому продовжуватимуть впливати на наше повсякденне життя. Інтелектуальні побутові пристрої, ймовірно, стануть ще більш взаємопов'язаними, що забезпечить безперебійну комунікацію між різними пристроями та платформами.

Асистенти та алгоритми на базі штучного інтелекту продовжуватимуть удосконалювати автоматизацію підключеного дому шляхом персоналізації, вивчення індивідуальних уподобань та адаптації до потреб мешканців.

Попит на автоматизацію розумного дому зростає, і для підприємців все ще існує багато невикористаних можливостей для впровадження нових та унікальних послуг з розробки розумного дому. Створюючи додаток для домашньої безпеки, компанії можуть представити свої інноваційні ідеї, задовольнити потреби конкретних клієнтів та виділитися серед конкурентів.

Ключові характеристики хмарної домашньої безпеки:

1. Віддалений доступ: домовласники можуть контролювати та керувати своїми системами безпеки з будь-якого місця за допомогою смартфонів, планшетів або комп'ютерів.
2. Масштабованість: ці системи можуть легко встановлювати додаткові пристрої та функції без значних змін у апаратному забезпеченні.
3. Інтеграція: Бездоганно інтегрується з іншими пристроями розумного дому, такими як освітлення, термостати та дверні замки.
4. Сповіщення в режимі реального часу: Забезпечує миттєві сповіщення про підозрілу активність, що дозволяє оперативно реагувати.
5. Економічно ефективний: часто доступніший за традиційні системи завдяки нижчим витратам на встановлення та обслуговування.

BIoT

Система хмарного сервісу забезпечення безпеки розумного будинку реалізована з використанням функцій BIoT.

З розвитком технологій концепція розумних будівель виходить на нові висоти завдяки інтеграції Інтернету речей у будівлях (BIoT). Це наступне покоління автоматизації будівель використовує передові датчики, взаємопов'язані пристрої та складну аналітику даних для створення більш ефективних, адаптивних та зручних для користувача середовищ. У цій статті досліджується майбутнє BIoT, його переваги, проблеми та трансформаційний вплив, який він має на те, як ми керуємо будівлями та взаємодіємо з ними.

Інтернет речей у будівництві (BIoT) стосується інтеграції технології IoT саме в контексті управління та автоматизації будівель. На відміну від традиційних систем автоматизації будівель, які працюють ізольовано, BIoT створює цілісну, взаємопов'язану мережу пристроїв і датчиків, які взаємодіють у режимі реального часу. Така інтеграція дозволяє здійснювати комплексний моніторинг, керування та оптимізацію різних систем будівлі, включаючи опалення, вентиляцію та кондиціонування повітря, освітлення, безпеку тощо.

Роль передових датчиків та пристроїв Інтернету речей

Основою BIoT є використання передових датчиків та пристроїв Інтернету речей. Ці датчики збирають величезні обсяги даних про різні аспекти продуктивності будівлі, такі як температура, вологість, заповнюваність та споживання енергії. Потім пристрої Інтернету речей передають ці дані до центральної системи, де їх можна проаналізувати та вжити заходів.

Наприклад, датчики присутності можуть виявляти присутність людей у кімнаті та відповідно регулювати освітлення й системи опалення, вентиляції та кондиціонування повітря для економії енергії. Датчики навколишнього середовища можуть контролювати якість повітря та запускати системи вентиляції для підтримки здорових умов у приміщенні. Завдяки постійному збору та аналізу даних, системи BIoT дозволяють будівлям працювати ефективніше та адаптуватися до потреб своїх мешканців у режимі реального часу.

Переваги BIoT:

1. Підвищена енергоефективність: системи BIoT оптимізують використання енергії, контролюючи та регулюючи системи освітлення, опалення та охолодження на основі заповненості приміщень та умов навколишнього середовища в режимі реального часу. Це призводить до значної економії енергії та зменшення викидів вуглецю.

2. Покращений комфорт та продуктивність мешканців: Створюючи адаптивне середовище, яке відповідає потребам та вподобанням мешканців, BIoT підвищує комфорт та продуктивність. Наприклад, системи освітлення можуть налаштовуватися відповідно до циклів природного освітлення, покращуючи самопочуття мешканців та зменшуючи втому.

3. Прогнозне обслуговування та скорочення часу простою: BIoT дозволяє проводити прогнозне обслуговування, постійно контролюючи стан систем будівлі та виявляючи потенційні проблеми до того, як вони призведуть до збоїв. Такий проактивний підхід мінімізує час простою та подовжує термін служби обладнання будівлі.

4. Комплексна аналітика даних: величезна кількість даних, зібраних системами BIoT, може бути проаналізована для отримання уявлення про продуктивність будівлі та виявлення можливостей для покращення. Розширена аналітика може виявляти закономірності та аномалії, допомагаючи керівникам об'єктів приймати обґрунтовані рішення та оптимізувати експлуатацію будівлі.

Незважаючи на численні переваги, впровадження BIoT не обходиться без труднощів. Однією з основних проблем є інтеграція різноманітних систем і пристроїв. Багато будівель мають застарілі системи, які можуть бути несумісними із сучасними технологіями Інтернету речей. Забезпечення безперебійної комунікації та сумісності між різними системами вимагає ретельного планування та інвестицій.

Безпека даних є ще однією критичною проблемою. Оскільки системи будівель стають більш взаємопов’язаними, вони також стають більш вразливими до кіберзагроз. Захист конфіденційних даних та забезпечення безпеки систем автоматизації будівель мають першочергове значення.

Крім того, початкові витрати на впровадження BIoT можуть бути високими. Хоча довгострокова економія та переваги часто виправдовують інвестиції, забезпечення необхідного фінансування та ресурсів може бути перешкодою для деяких організацій.

Майбутнє BIoT

Майбутнє BIoT виглядає багатообіцяючим, оскільки постійний розвиток технологій стимулює подальші інновації. Новітні технології, такі як 5G, периферійні обчислення та блокчейн, мають розширити можливості систем BIoT, забезпечуючи швидшу обробку даних, покращену безпеку та надійніше з’єднання.

Оскільки будівлі стають більш інтелектуальними та взаємопов'язаними, потенціал біотехнологій, що працюють в Інтернеті речей (BIoT), для трансформації забудованого середовища продовжуватиме зростати. Завдяки BIoT, керівники об'єктів можуть створювати розумніші, ефективніші та адаптивніші будівлі, які відповідають потребам мешканців та зацікавлених сторін, що постійно змінюються.

На завершення, інтеграція BIoT являє собою значний крок вперед в автоматизації будівель. Використовуючи можливості передових датчиків, пристроїв Інтернету речей та аналітики даних, BIoT створює цілісну та інтелектуальну систему управління будівлею, яка підвищує енергоефективність, комфорт мешканців та загальну продуктивність будівлі. Хоча проблеми залишаються, переваги BIoT роблять її переконливою та трансформаційною технологією для майбутнього розумних будівель.

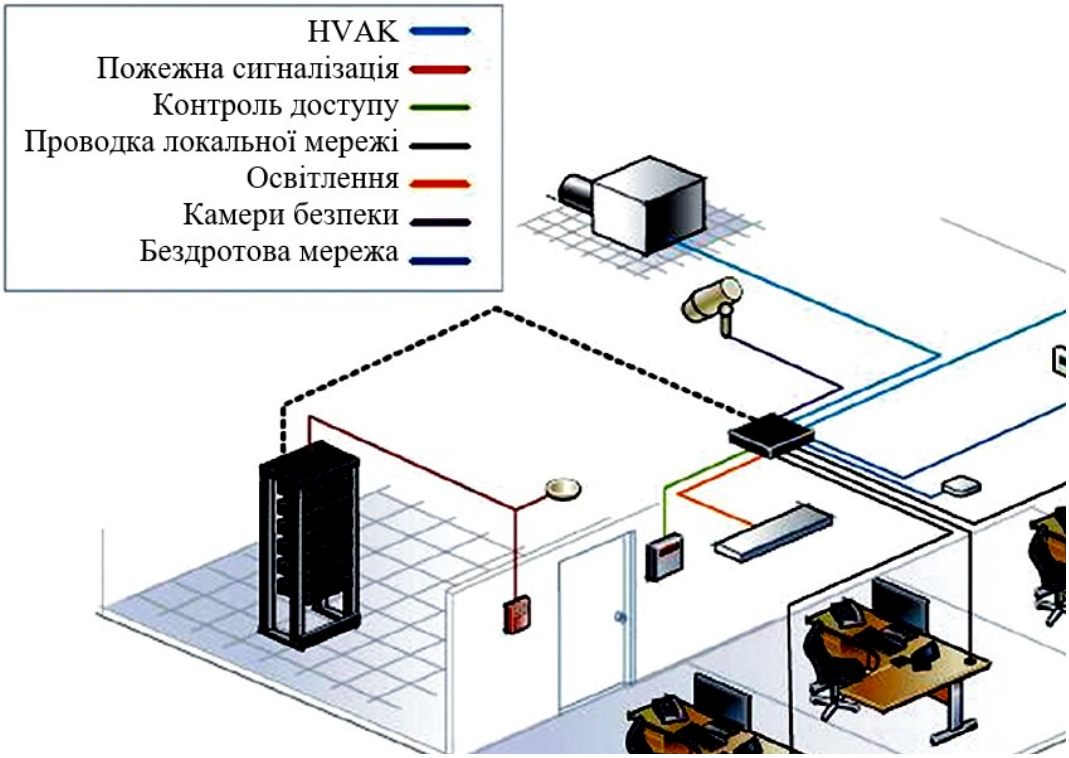

Рисунок 1 – Структурна схема системи

Висновки. У статті освіти наведені теоретичне узагальнення й рішення наукового завдання дослідження методів хмарного сервісу забезпечення безпеки розумного будинку. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем хмарного сервісу забезпечення безпеки розумного будинку.

– Досліджена система хмарного сервісу забезпечення безпеки розумного будинку.

– На основі отриманих результатів досліджень створена програмна реалізація системи хмарного сервісу забезпечення безпеки розумного будинку.

Розроблені алгоритми дозволяють успішно вирішувати завдання хмарного сервісу забезпечення безпеки розумного будинку. 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, 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. Вінтенко, Б., Миронець, І., Смірнов, О., Коваленко, А., Конопліцька-Слободенюк, О., Смірнова, Т., Константинова, Л. «Дослідження застосування систем підтримки оперативного персоналу об'єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 6-26.
9. 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.
10. 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.
11. 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.
12. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the Age of ASIC Resistance». CEUR Workshop Proceedings, 2023, 3628, pp. 93-105.
13. 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.
14. 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.
15. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 3(73), С. 155-166.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
24. 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.
25. 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.
26. 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.
27. 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.
28. 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.
29. 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.
30. 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.
31. 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.
32. 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.
33. 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.