основі: розподілених інтелектуальних агентів; програмного забезпечення автоматизованих систем; SCADA-систем.

Удосконалені інтерфейси та підтримка прийняття рішень спрямовані для ефективного керування енергосистемою за умови зростання кількості змінних. Функціональність: технології візуалізації, які зводять велику кількість даних у візуальні формати; програмні системи; симулятори; системи аналізу сценаріїв.

Згідно з Енергетичною стратегією України створення розумних екологічних систем та розумних енергосистем на основі технології Smart Grid забезпечуватиме: зменшення викидів вуглекислого газу в навколишнє середовище; впровадження відновлювальних джерел альтернативної енергетики: вітроенергетичних станцій та сонячних батарей; запровадження «розумних лічильників», з метою контролю енергопостачання та розподілу електроенергії за цільовими тарифами, прийнятними для споживачів. На період до 2035 року Smart Grid технології будуть запроваджені в розумних енергомережах і забезпечуватимуть безпечне використання електроенергії, енергоефективність цього використання та конкурентоспроможність альтернативних джерел енергії на ринку електроенергії.

Висновок: розглянуто технологічні компоненти та подано характеристики розвитку Smart Grid 1.0\2.0\3.0. Проаналізовано аспекти ефективності застосування концепції Smart Grid.

П. Ерфан
Науковий керівник – д.т.н., проф. Г. В. Микитин

КІБЕРФІЗИЧНІ СИСТЕМИ В ПРОЕКТУВАННІ РОЗУМНИХ БУДИНКІВ

Застосування кіберфізичних систем (КФС) та забезпечення їх інформаційної безпеки є однією з актуальних задач інтелектуалізації суспільства у предметних сферах: медицини, екології, енергетики, логістики, оборонної промисловості т. і. **Актуальною є задача** використання безпечної структури КФС у проектуванні системи “Розумний будинок”. *Функціональність КФС* передбачає: контроль/відбір інформації від об’єктів інфраструктури – у фізичному просторі; зберігання/обробку/управління – у кібернетичному просторі; передавання/приймання – у комунікаційному середовищі. *Проектування системи “Розумний будинок”* (рисунок 1) ґрунтується на структурі КФС, яка виконує цільові функції: розпізнавання ситуацій на об’єкті, порівняння

з встановленими/допустимими параметрами, прийняття рішення на управління з використанням технологій: Інтернет речей, як мережі мереж давачів, сенсорних мереж, автоматизованої системи обробки інформації з обмеженим доступом.

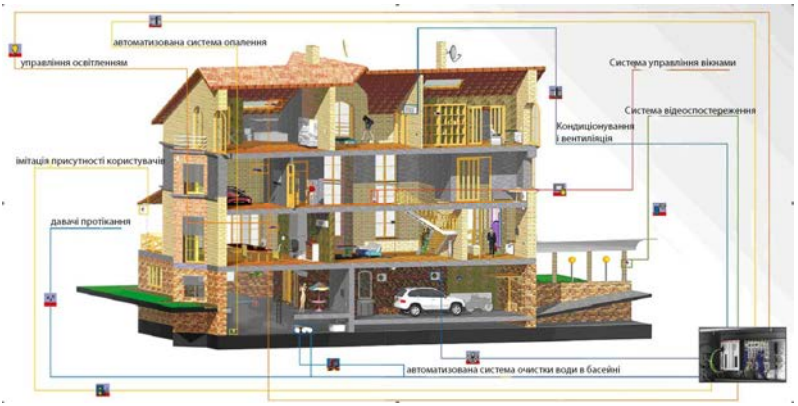

Рис. 1. Система "Розумний будинок"

Узагальнений підхід до проектування КФС ґрунтується на архітектурі 5-ти рівнів: 1) розумного підключення – пристрої призначені для самопідключення та самостійного моніторингу поведінки об'єкта; 2) перетворення – дані з пристроїв і давачів передаються для опрацювання та прогнозування; 3) кібер – кожна машина створює свій власний "двійник", який в кіберпросторі може самостійно виконувати порівняння характеристик для вирішення завдань; 4) пізнання – результати представляються користувачам; 5) конфігурації – система може бути змінена з урахуванням пріоритетних напрямів.

Безпека КФС. На рисунку 2 представлена модель інформаційної безпеки системи «Розумний будинок».

Рис. 2. Модель безпеки системи «Розумний будинок»

На зовнішньому рівні безпеки (відбір/контроль інформації) виникають загрози: відмова та несправності технічних засобів, пошкодження у зв'язку з погодними умовами, установка закладних пристроїв, порушення режиму конфіденційності, режиму охорони і системи захисту, виведення давачів з робочого стану. Зовнішня безпека системи «Розумний будинок» передбачає використання систем: біометрії, відеоспостереження, радіочастотної ідентифікації, контролю доступу т. і.

На внутрішньому рівні (аналіз, автоматизація обробки інформації з обмеженим доступом, прийняття управлінського рішення) виникають загрози: порушення цілісності та достовірності інформації, витік інформації при зберіганні, навмисне викрадання даних, несанкціонований доступ до інформації. Технологіями захисту на внутрішньому рівні безпеки є: підвищення рівня системи безпеки, постійне оновлення системи безпеки, моніторинг доступних користувачів, використання ліцензійного програмного забезпечення, постійне оновлення програмного забезпечення, використання алгоритмів шифрування AES, "Калина".

Висновок. Розглянуто застосування КФС у проектуванні системи "Розумний будинок" на рівні структури контроль – обробка – управління, а також модель інформаційної безпеки відповідно до концепції "загроза – захист."

Х. Руда
Науковий керівник – д.т.н., проф. Г. В. Микитин

ВИКОРИСТАННЯ ПРЕДИКТИВНИХ МОДЕЛЕЙ ДЛЯ ВИЯВЛЕННЯ ШАХРАЙСТВА З КРЕДИТНИМИ КАРТАМИ

Сучасні банківські системи дозволяють клієнтам оперувати коштами, використовуючи численні способи, зокрема платежі через Інтернет, для виконання яких необхідні тільки реквізити, які фізично розташовані на пластиковій картці. Зловмисник, використовуючи засоби соціальної інженерії або технічні засоби, може дізнатись реквізити і спробувати використати їх для власного збагачення. Спеціалізовані структури банку аналізують деталі транзакції і авторизують або не авторизують її. Під час проведення аналізу проблемою є відносно невелика кількість підтверджених шахрайських запитів в порівнянні із загальною кількістю операцій.

Актуальною є задача балансування наборів даних, що використовуються для класифікування транзакцій шахрайськими або не шахрайськими.