

8. Smirnov O., Kuznetsov A., Kiiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58. (Scopus).
9. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256. (Scopus).
10. Smirnov O., Kuznetsov A., Kiiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114. (Scopus).
11. Smirnov O.A., 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. (Scopus).
12. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131. (Scopus).
13. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14. (Scopus).
14. Smirnov O., Lutsenko M., Kuznetsov A., Kiiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84. (Scopus).
15. 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. (Scopus).
16. 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. (Scopus).
17. 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. (Scopus).
18. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43. (Scopus).
19. 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. (Scopus).
20. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660., (Scopus).

УДК 004

І.Завірюха, магістр гр. КІ-21М-1,4,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ SMART HOME З ВИКОРИСТАННЯМ ПРОТОКОЛУ X10

У статті розроблено програмне забезпечення, яке призначено для системи smart home з використанням протоколу X10. Метою розробки є дослідження та програмна реалізація системи smart home з використанням протоколу X10. Об'єктом дослідження є процес smart home з використанням протоколу X10. Предметом дослідження є методи smart home з використанням протоколу X10. Методи дослідження базуються на методах інтернету речей, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи smart home з використанням протоколу X10. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерна інженерія, smart home, X10

Постановка проблеми. У сучасному житті вже звичайними й навіть обов'язковими стають різні пристрої й пристосування, що забезпечують високу якість життя й комфорт мешканців. І якщо раніше каналні кондиціонери, електроуправляемі водопровідні вентиля, індивідуальне управління кліматом і безліч світлових груп були атрибутами великого

заміського будинку, то зараз ці особливості властиві й міській квартирі. Зрозуміло, при повсякденній експлуатації настільки різноманітного встаткування в користувачів виникає безліч повторюваних завдань, наприклад:

- одночасне вимикання множини світлових груп;
- вимикання великої кількості приладів при відході із квартири й включення їх у потрібний режим при поверненні у квартиру;
- управління кліматом у приміщеннях залежно від часу доби й присутності людей;
- контроль цілісності комунікацій і справності встаткування.

У першу чергу, саме для виконання таких рутинних операцій, причому з великим ступенем надійності й точності, призначені системи домашньої автоматики, тобто системи «Smart home».

Але логічно, що саме все не буде включатися й відключатися у smart home (інтелектуальному домі). Для того, щоб smart home запрацював, по-перше необхідно установити відповідне устаткування, по-друге необхідно з'єднати це устаткування у мережу, й відповідно написати якесь програмне забезпечення, яке повинно керувати устаткуванням.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи smart home з використанням протоколу X10.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи smart home з використанням протоколу X10.

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

- Огляд існуючих систем smart home з використанням протоколу X10.
- Дослідження системи smart home з використанням протоколу X10.
- Програмна реалізація системи smart home з використанням протоколу X10.

Об'єктом дослідження є процес smart home з використанням протоколу X10.

Предметом дослідження є методи smart home з використанням протоколу X10.

Методи дослідження базуються на методах інтернету речей, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Огляд технології X10

Технологія домашньої автоматизації X10 призначена для інтелектуального управління освітленням і побутовими електроприладами з використанням силової електропроводки.

Сигнали управління X10 передаються й приймаються безпосередньо по електричній мережі (Power Line Carrier або PLC). Відсутність додаткових дротів робить інсталяцію систем X10 швидкою й легкою.

Для передачі команд управління в системах X10, крім силової проводки, використовується радіоканал із частотою 433Мгц. Так забезпечується комфорт бездротового способу управління.

Одна з головних переваг технології X10 у порівнянні із традиційною електроінсталяцією полягає в тому, що схема управління може багаторазово мінятися простим переналаштуванням окремих компонентів мережі X10 – контролерів, вимикачів, реле й диммерів. У випадку традиційної електроінсталяції зв'язок «орган управління – об'єкт управління» задаються жорстко раз і назавжди структурою кабельної проводки. Системи X10 легко розширювані. У будь-який момент у діючу інсталяцію можна додати нові компоненти навіть якщо опоряджувальні роботи давно закінчені.

Вартість мінімального комплексу встаткування X10 становить 1-2 тис. грн., що робить технологію доступною й популярною.

Технологія X10 веде свою історію з початку 70-х років минулого століття. У той час інженери з англійської компанії PICO Electronics уперше створили пристрої, що використовували електричну проводку як середовище мережної комунікації. З тих пор

технологія безупинно вдосконалювалася й сьогодні автоматикою X10 оснащені мільйони будинків по усьому світі. Особливе поширення й популярність технологія одержала в країнах Північної Америки.

Управління X10

За допомогою технології X10 вирішуються завдання комфортного управління освітленням, компонентами інженерних систем і побутових електроприладів. Технологія X10 забезпечує різноманітні способи управління домашнім устаткуванням у ручному й автоматичному режимах.

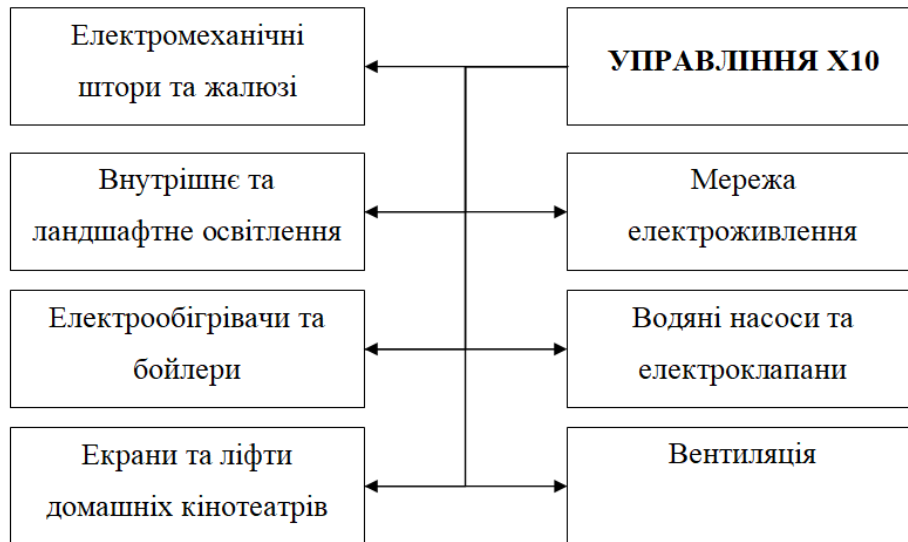


Рисунок 1 – Схема управління технології X10

Додатковий асортименти мультимедійних і охоронних пристроїв розширює функціональні можливості базового комплекту X10 по управлінню освітленням і електроприладами й робить всю лінійку ще більш привабливою для самого широкого кола споживачів.

Функції X10, устаткування X10

Мережа X10 – це сукупність контролерів і виконавчих пристроїв, взаємодіючих один з одним по електричній мережі або радіоканалу. При необхідності додатково використовуються спеціальні системні пристрої, що забезпечують працездатність мережі X10 у цілому. Устаткування X10 може задовольнити найрізноманітнішим вимогам до розміщення.



Рисунок 2 – Застосування устаткування X10



Рисунок 3 – Приклади пристроїв X10

Адреси X10

Кожний виконавчий пристрій X10 настраюється на певну адресу, що складається із двох 16-значних полів – Коду будинку (буквені значення A..P) і Коду пристрою (цифрові значення 1..16). Таким чином, усього можливі 256 адресні комбінації. Це максимально можлива кількість керованих груп пристроїв у мережі X10. Виконавчі пристрої X10 настраюються на певну адресу за допомогою двох механічних адресних селекторів-коліщат. Більшість контролерів X10 також вимагають попереднього налаштування адрес.

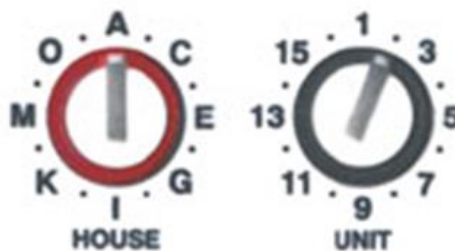


Рисунок 4 – Виконавчий пристрій X10

Для проходження команд контролер і виконавець повинні бути настроєні на однакові адреси.

Команди X10

У протоколі X10 передбачено шість базових команд:

- Включити (On).
- Виключити (Off).
- Яскравіше (Bright).
- Темніше (Dim).
- Включити все світло (ALL Lights ON).
- Виключити всі (ALL Units OFF).

Сигнали X10

Технологія X10 використовує цифрове подання сигналів управління. Інформація кодується двійковим кодом і передається по електричній мережі за допомогою високочастотних імпульсів. Кожний переданий імпульс відповідає одному біту інформації с_i значенням “1”. Передача чергового імпульсу відбувається в момент часу, коли сіткова напруга приймає нульове значення.

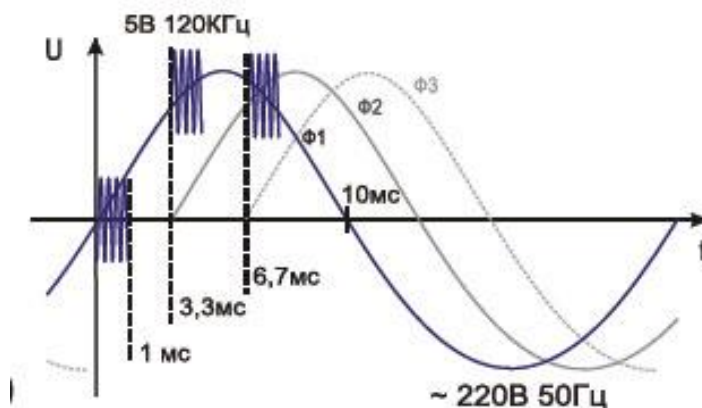
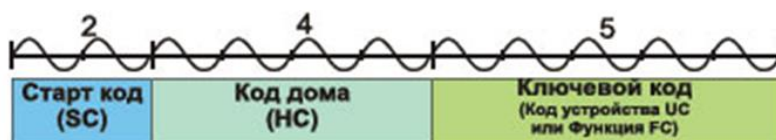


Рисунок 5 – Передача цифрових сигналів

Стандартна команда X10 передається протягом, приблизно, 50 періодів сіткової напруги частоти 50Гц або 1 сек. Більшість переданих по мережі X10 повідомлень містить, принаймні, два інформаційні поля – адреса пристрою, якому ця команда адресована й властиво команду. Підключені до електромережі пристрої X10 приймають передані повідомлення, декодують поле адреси одержувача й, якщо він збігається з їхньою власною адресою, виконують команду.

Періоди силової напруги



Повний цикл команди X10

11 періодів

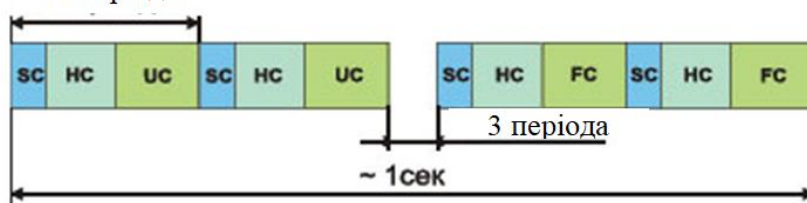


Рисунок 6 – Цикл виконання команди X10

Інтеграція X10

Основним засобом інтеграції мережі X10 із зовнішнім устаткуванням є PLC інтерфейс XM10. Будь-який контролер, що підтримує відкритий протокол обміну з XM10, може відправляти команди X10 в електромережу й, навпаки, одержувати з мережі інформацію про стан пристроїв X10. Так, наприклад, охоронні системи широко відомих у світі брендів – Ademco, DSC, Visonic і деяких інших – підтримують протокол X10 і дозволяють реалізувати інтегровані системи автоматизації й безпеки. Друга можливість апаратної інтеграції – підключення зовнішніх пристроїв по «сухому контакті». У лінійці X10 для цього використовуються модулі UM7206 і SM10.

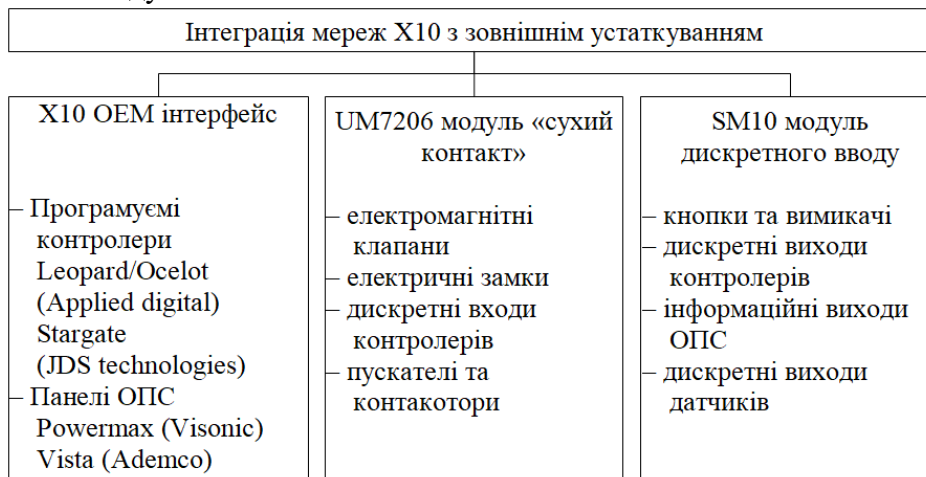


Рисунок 7 – Інтеграція мереж X10

Працездатність мережі X10

При установці автоматики X10 необхідно звертати особливу увагу на:

- перешкодозахищеність системи;
- забезпечення міжфазного проходження сигналу X10 при багатофазній схемі електроживлення;
- захист електричних кіл і пристроїв X10 від перенапруги, перевантаження й струмів короткого замикання.

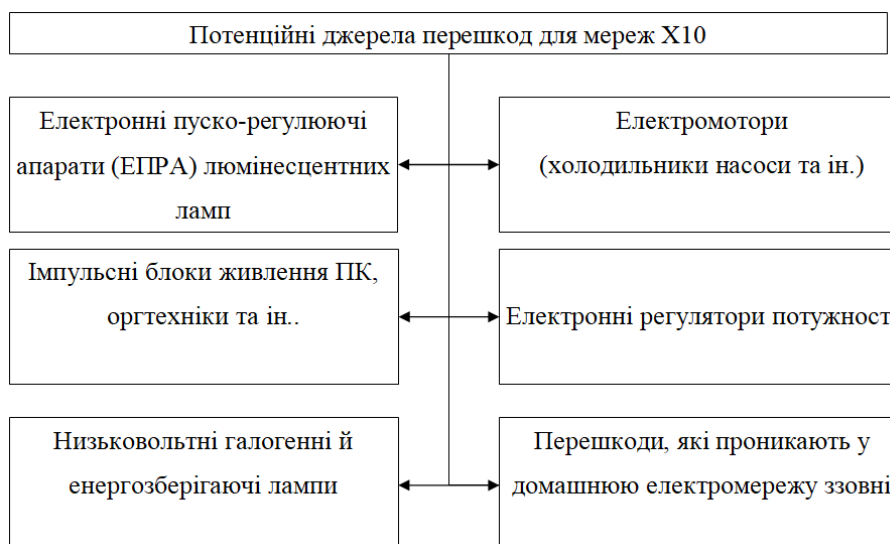


Рисунок 8 – Джерела перешкод для X10

Міри, що рекомендуються, для усунення перешкод у мережах X10:

- використання мережних фільтрів (FM10, FD10, TF678 і ін.) на введенні домашньої електромережі й у місцях підключення до електроживлення приладів-джерел перешкод;

–підключення пристроїв X10 і приладів-джерел перешкод до різних фаз у багатофазній електромережі;

–заміна «шумливих» електроприладів на більш якісні моделі.

У цілому деякі електроприлади стають джерелами перешкод для пристроїв X10, і при дотриманні нескладних правил захисту від високочастотного шуму автоматика X10 працює надійно протягом довгого часу.

Проект X10

Вихідною інформацією для проектів X10, як і для більшості проектів домашньої автоматизації, є:

–плани приміщень

–однолінійна електрична схема

–плани розміщення електроустаткування – світильників, світлових вимикачів, електричних розеток, точок прямого підключення електроустаткування, електричних щитків і шаф, комутаційних вузлів

–перелік автоматизуємих групових і одиночних електричних навантажень, із вказівкою їхніх типів і потужності

–плани існуючої кабельної проводки й кабельний журнал

–відомості про стан об'єкта й можливості проведення кабельних робіт

–вимоги замовника до функціональності проекрованої системи управління

При виконанні проекту X10 рекомендується технологічна послідовність робіт зображена на рисунку 10.

Розробка структурної схеми

На рисунку 11 зображена узагальнена структурна схема інтелектуального дому.

Як було відзначено вище, сучасний smart home – це дуже складне інженерне рішення, що складається з наступного набору систем:

–Система безпеки.

–Система комфорту.

–Інформаційна система.

–Система диспетчеризації.

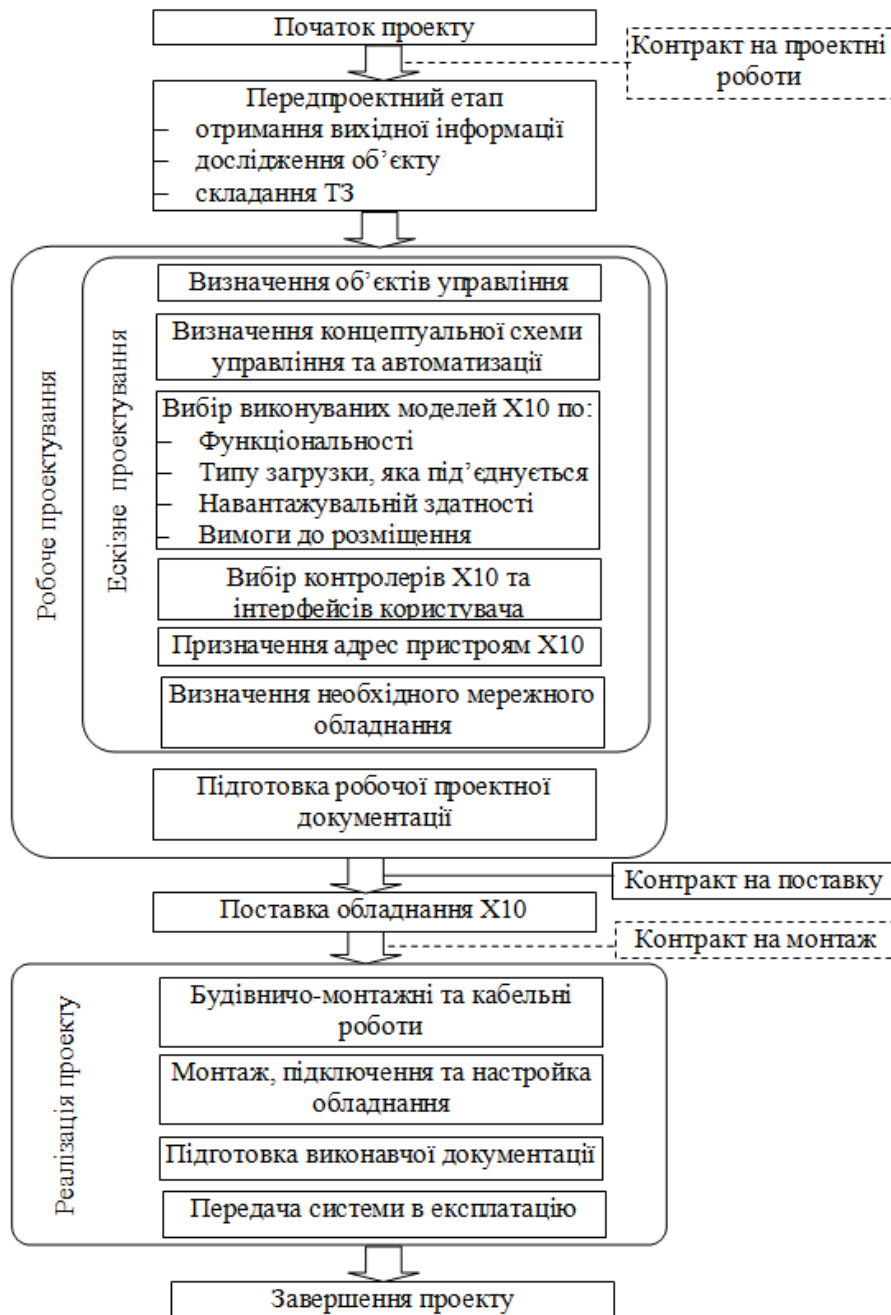


Рисунок 10 – Виконання проекту X10

Розглянемо які підсистеми входять у перераховані вище системи.

Система безпеки:

– Система цифрового відеоспостереження з можливістю одночасного спостереження, перегляду, архівування. Режим віддаленого перегляду й управління через Інтернет.

– Бездротова пожежна й охоронна сигналізація з можливістю обміну інформацією через GSM модуль.

– Система контролю доступу в приміщення (у тому числі віддалене управління гаражними воротами).

Система комфорту:

– Внутрішня телефонна система, голосний зв'язок усередині будинку.

– Система супутникового, ефірного телебачення з можливістю перегляду в будь-якій кімнаті.

– Система "Домашній кінотеатр".

- Система "Мультирум" аудіо– й відео– (система "звук навколо").
- Цифровий розважальний комплекс, оцифровка відео, печать фотографій, створення особистих цифрових фото– і відео– альбомів і т.д.
- Управління світлом у всьому будинку, світлові сцени й сценарії.
- Управління системою вентиляції й кондиціонування.
- Управління системою опалення.
- Управління сауною, басейном.

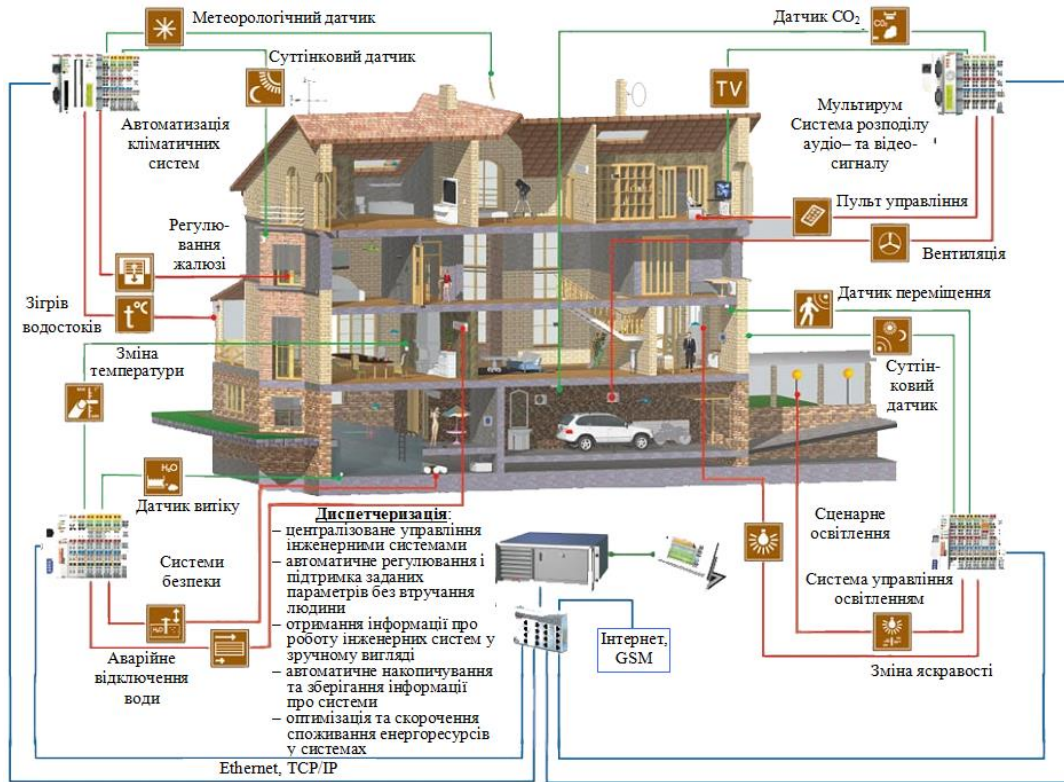


Рисунок 11 – Структурна схема інтелектуального дому

Інформаційна система:

- Установа локальної обчислювальної мережі в будинку, мережна печать, мережні ігри (можлива використання бездротових технологій).
- Вихід в Інтернет з будь-якого комп'ютера в будинку (у тому числі з мобільного).
- Віддалене управління всіма системами будинку через Інтернет.
- "Домашній офіс" з віддаленим підключенням до корпоративної мережі робочого офісу.

Система диспетчеризації:

- Система безперебійного електропостачання
- Управління системою опалення, казаном водонагрівача
- Контроль витоку води, газу.
- Система управління здатна погоджувати роботу інженерних систем, оцінюючи стан сенсорів, датчиків, відпрацьовуючи команди з пультів управління, прив'язуючись до часу доби, пори року й т.п. При цьому виключаються ситуації, коли домашнє устаткування, покликане вирішувати спеціалізовані проблеми, працює в режимах, взаємовиключих один одного.

На рисунку 12 відображено структурну схему взаємодії систем інтелектуального будинку.

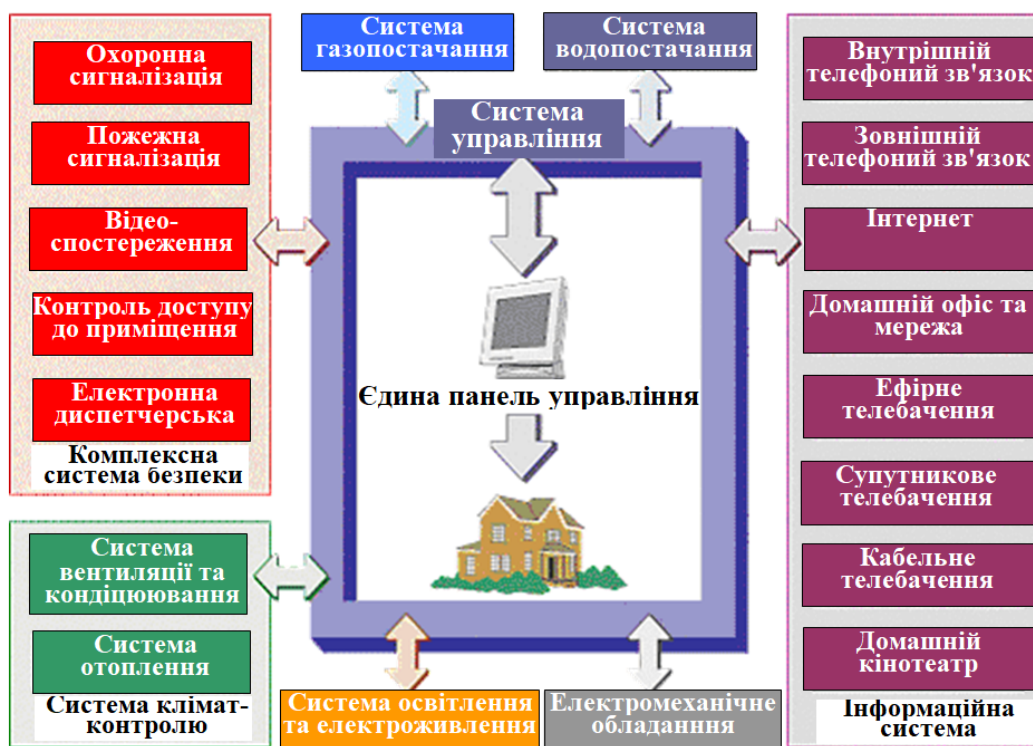


Рисунок 12 – Структурна схема взаємодії систем інтелектуального будинку

Smart home дозволяє замінити всі пульти управління однією або декількома (по кількості зон або кімнат) сенсорними панелями. Вони дозволяють не ламати голову над тим, як підбудувати середовище перебування під необхідні умови.

Використання сучасного устаткування дозволяє створити в будинку єдиний комплекс із систем безпеки (охоронна й пожежна сигналізація, відеоспостереження, контроль доступу), систем зв'язку й комунікації (телефонна й комп'ютерна мережі, оповіщення, екстрений виклик), систем управління опаленням, вентиляцією, освітленням і т.д., що працює по обраному алгоритмі.

Як ілюстрацію можна привести приклад, коли автоматизація й включення в єдиний контур управління освітлювальної системи й систем клімат-контролю (опалення, кондиціювання й вентиляція) будинку (окремої квартири) дозволяють реалізувати автоматичне управління цими системами залежно від пори року й доби, умов навколишнього середовища, присутності людей і інших факторів. У результаті досягається істотне зниження витрат на електроенергію й теплопостачання. Досвід показує, що економія експлуатаційних витрат у цьому випадку може досягати 15-20%.

Основні складові інтелектуального будинку

Зв'язок:

- телефонний зв'язок внутрішня (інтерком) і локальні АТС;
- телефонний зв'язок зовнішня провідна, радіорелейна, супутникова;
- інтернет – телефонія;
- системи відеоконференцій.

Мультимедіа:

- наземне й кабельне телебачення;
- супутникове телебачення;
- домашнє відео;
- домашній кінотеатр;
- мульти– аудіо й відео (multiroom).
- один пульт управління для всіх систем

Інформаційні системи:

- локальна комп'ютерна мережа;
- домашній офіс;
- широкополосний доступ у глобальну мережу (Інтернет).

Безпека:

- пожежна сигналізація й система автоматичного пожежогасіння;
- охоронна сигналізація;
- система контролю доступу;
- система зовнішнього й внутрішнього відео спостереження;
- система управління паркінгом;
- система внутрішнього оповіщення (радіомережа);
- аварійний контроль інженерних систем;
- система екологічного контролю.

Водопостачання й газопостачання:

- автоматичне наповнення ванн, басейнів і накопичувальних резервуарів;
- автономне й резервне нагрівання води;
- запобігання витоку водопроводу й витоку газу;
- управління ландшафтними водними системами (фонтани, водоспади);
- управління температурою води у ваннах і басейнах (термостатування);
- облік витрат й управління споживанням води й/або газу.

Система електроживлення:

- безперебійне й гарантоване електропостачання;
- захист від поразки електричним струмом людей і тварин;
- автоматизація управління електроживленням побутових приладів;
- запобігання перевантажень і короткого замикання в електричній мережі;
- управління якістю електроживлення – моніторинг, стабілізація й фільтрація;
- облік витрат й управління споживанням електроенергії.

Освітлення внутрішнє й зовнішнє:

- аварійне й чергове освітлення;
- автоматизація управління світлом;
- гнучке налаштування світлових груп;
- дистанційне й віддалене управління світлом;
- програмування світлових сцен.

Опалення, вентиляція, кондиціонування:

- автоматизація управління температурою повітря;
- контроль якості повітря;
- узгодження роботи різних кліматичних систем;
- облік витрати й управління споживанням теплової енергії.

Тепер спробуємо створити зі звичайного будинку інтелектуальний. Для цього нам потрібно всі прилади, які виконують перераховані вище функції, об'єднати в одну систему й підключити її до віддаленого сервера. Тим самим буде управління кожним компонентом, та всіма вєдино. І необхідно щоб контроль за станом всіх приладів користувач міг одержати в будь-який момент часу, навіть перебуваючи поза будинком. Для цього треба організувати мережу в будинку, об'єднавши всі прилади й системи над якими треба здійснити контроль, та потім вибрати спосіб підключення до віддаленого сервера.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів smart home з використанням протоколу X10. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем smart home з використанням протоколу X10. Досліджена система smart home з використанням протоколу X10. На основі отриманих результатів досліджень створена програмна реалізація системи smart home з використанням протоколу X10. Розроблені під час виконання випускної

кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання smart home з використанням протоколу X10. 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. Kovalenko A.S. Information model and its element for displaying information on technical condition of objects of integrated information system / A.S. Kovalenko, A.A. Smirnov, A.V. Kovalenko, A.P. Dorensky // International Journal of Computational Engineering Research (IJCER). – India: Delhi, 2016. – Volume 6, Issue 1. – P. 21-27.
2. Кожанова А.С. Обґрунтування необхідності створення систем технічної діагностики інтегрованих інформаційних систем / О.А. Смірнов, А.С. Кожанова, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2013. – Вип. 6(113). – С. 255-257.
3. Коваленко А.С. Задачи распознавания ситуаций в ERP системах / А.В. Коваленко., А.А. Смірнов, А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 4(120). – С. 161-164.
4. Коваленко А.С. Підсистема технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / А.С. Коваленко, О.А.Смірнов, О.В. Коваленко // Системи озброєння і військова техніка.– Х.: ХУПС, 2014. – № 1(37). – С. 126-129.
5. Коваленко А.С. Анализ эффективности использования экспертной системы технической диагностики с традиционной структурой / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 2(38). – С. 106-108.
6. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
7. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
8. Коваленко А.С. Структура системи технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Кіровоградського національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: Вид-во КНТУ, 2014. – Вип. 27. – С. 245-251.
9. Коваленко А.С. Дослідження будови інтегрованої інформаційної системи та її елементів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 4(40). – С. 85-88.
10. Коваленко А.С. Розробка структури бази даних для обліку технічного стану елементів інтегрованої інформаційної системи з урахуванням вимог споживачів інформації / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 75-79.
11. Коваленко А.С. Обґрунтування набору даних для оцінки технічного стану інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2015. – Вип. 1(42). – С.39-41.
12. Коваленко А.С. Експертна система технічного діагностування інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2015. – № 1(41). – С. 106-111.
13. Коваленко А.С. Удосконалення методу технічного обслуговування об'єктів інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко, О.П. Доренський // Системи озброєння і військова техніка. – Х.: ХУПС, 2016. – № 2(46). – С. 109-114.
14. Кожанова А.С. Система технічної діагностики інтегрованих інформаційних систем – обґрунтування необхідності створення, визначення понятійного апарату та напрямів досліджень / А.С. Кожанова, О.А. Смірнов, М.П. Савченко, Д.М. Ізосімов, В.В. Мороз // Створення та модернізація озброєння і військової техніки в сучасних умовах: Тринадцята наук.-техн. конф., 5-6 вер. 2013 р., м. Феодосія: тези доп. – Феодосія: ДНВЦ, 2013. – С. 187-188.
15. Кожанова А.С. Визначення основних напрямків досліджень щодо створення системи технічної діагностики інтегрованих інформаційних систем / А.С. Кожанова, О.А. Смірнов, А.В. Челпанов // Проблемні питання розвитку озброєння та військової техніки Збройних Сил України: IV наук.-техн. конф., 16-20 груд. 2013 р., м. Київ: зб. тез. – Київ: ЦНДІ ОВТ ЗСУ, 2013. – С. 293.
16. Коваленко А.С. Обґрунтування необхідності створення систем технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Інформатика та системні науки : V Всеукр. наук.-практ. конф., 13–15 бер. 2014 р., м. Полтава: зб. тез. – Полтава: ПУЕТ, 2014. – С. 292-294.
17. Коваленко А.С. Створення систем технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Проблеми і перспективи розвитку IT-індустрії: VI між нар. наук.-практ. конф., 17-18 квіт. 2014 р., м. Харків: зб. тез. – Харків: ХНЕУ, 2014. – С. 241.

18. Коваленко А.С. Визначення понятійного апарату та напрямів досліджень для синтезу систем технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Комп'ютерне моделювання у наукоємних технологіях (КМНТ-2014): наук.-техн. конф. з міжнар. участю, 28-31 трав. 2014 р., м. Харків: зб. наук. праць. – Харків: ХНУ, 2014. – С. 190-193.
19. Коваленко А.С. Дослідження елементів інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Комбінаторні конфігурації та їх застосування: XVII між нар. наук.-практ. сем., 17-18 квіт. 2015 р., м. Кіровоград: зб. тез – Кіровоград: КНТУ, 2015. – С. 5.
20. Коваленко А.С. Метод автоматизованої перевірки результатів вимірювання параметрів об'єкти в інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Стратегія якості у промисловості і освіті: XI міжнар. конф., 1 – 5 черв. 2015 р., м. Варна, Болгарія.: зб. матер. – Варна: ТУВ, 2015. – С. 423-426.

УДК 004

В. Коваленко, магістр гр. КІ-21М-1,4,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ З'ЄМНИХ НОСІЇВ

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

комп'ютерна інженерія, захисту доступу, з'ємних носії

Постановка проблеми. Широке застосування комп'ютерних технологій і постійне збільшення обсягу інформаційних потоків викликає постійний ріст інтересу до криптографії. Останнім часом збільшується роль програмних засобів захисту інформації, просто модернізуємих, не потребуючих великих фінансових витрат у порівнянні з апаратними криптосистемами [1-5]. Сучасні методи шифрування гарантують практично абсолютний захист даних, але завжди залишається проблема надійності їхньої реалізації. Іншою важливою проблемою застосування криптографії є протиріччя між бажанням громадян захистити свою інформацію й прагненням державних спецслужб мати можливість доступу до деякої інформації для припинення незаконної діяльності [6]. Надзвичайно важко знайти незаперечно оптимальне рішення цієї проблеми. Як оцінити співвідношення втрат законослухняних громадян і організацій від незаконного використання їхньої інформації й збитків держави від неможливості одержання доступу до захищеної інформації окремих груп, що приховують свою незаконну діяльність? Чи можна гарантовано не допустити незаконне використання криптоалгоритмів особами, які порушують і інші закони? Крім того, завжди існують способи схованого зберігання й передачі інформації. Хоча стримування відкритих досліджень в області криптографії й криптоаналізу є найпростішим шляхом, але це принесе значний негативний ефект. Застосування ненадійних засобів не захистить користувачів, але викличе поширення комп'ютерних злочинів, навпроти, виявлення своєчасне виявлення помилок у системах захисту інформації дозволить запобігти збитку [5-