КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (11), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.11.100109
УДК 004.45

Мошенченко Микита Сергійович
Аспірант
Київський політехнічний інститут ім. Ігоря Сікорського, Київ, Україна
ORCID ID: 0000-0002-0211-2263
nrodan@icloud.com

Жураковський Богдан Юрійович
Доктор технічних наук, професор
Київський політехнічний інститут ім. Ігоря Сікорського, Київ, Україна
ORCID ID: 0000-0003-3990-5205
zhurakovskiybyu@tk.kpi.ua

ЗАХИСТ ІНФОРМАЦІЇ В ТЕХНОЛОГІЯХ “SMART CITY”

Анотація. В даній статті розглянуто проблеми захисту інформації у системах “SmartCity”. Проведено порівняння існуючих рішень та протоколів передачі даних для проводових рішень, таких як IPsec, SSL, TLS та безпроводових систем: ZigBee, Z-Wave, Thread, WeMo. Проаналізовано переваги та недоліки кожної із існуючих систем. Система “SmartCity” повинна вміти розпізнавати конкретну ситуацію, що виникає в будинку, місті, на виробництві, при обробці великої кількості даних, реагувати відповідно: одна із систем може контролювати поведінку інших систем за допомогою заздалегідь розробленого алгоритму. Основним призначенням системи «SmartCity» є економія енергоносіїв, що є все більш актуальним у зв’язку з їх подорожчанням в Україні. Тому інтелектуалізація стає все популярнішою, наздоганяючи світові тенденції до автоматизації побуту. Однак, незважаючи на розвиток та поступову формальну та неформальну стандартизацію технологій розумного міста, та будь-якої домашньої автоматизації, все ще існує проблема вибору протоколів для передачі інформації між керованими пристроями, датчиками та іншими елементами. Ця проблема особливо серйозна, коли це необхідно для забезпечення конфіденційності та цілісності даних, що циркулюють у системі. Метою цього дослідження є пошук захищеного мережевого протоколу, який дозволяє використовувати його в автоматичному сигналізуючому обладнанні, щоб не можна було використовувати спеціальні програмні та апаратні рішення для впливу на конфіденційність та цілісність інформації.В статті не останнє місце займає питання безпеки інформації, адже маючи доступ до такого будинку системи правління містом або виробництвом, можна завдати дуже великої шкоди його власнику. Оскільки в наш час досить поширеним є віддалене управління та доступ до інформації, слід використовувати захищені схеми, схеми шифрування та захисту, щоб знизити відсоток вразливості та не дати можливості зловмисникам завдати шкоди.

Ключові слова:smartcity: протокол; інтернет речей; безпроводові; захист інформації; wi-fi: zigbee; wemo.

ВСТУП

Використання IT-технологій дозволяє створити «Розумний будинок» тобто сукупність програмно-апаратних систем, безпосередньо керуючих інженерно-технічними, енергетичними, комунікаційними та іншими підсистемами житлового приміщення. Однак використання IT-інфраструктури, зокрема інформаційних систем управління нерозривно пов'язане з вирішенням питань забезпечення безпеки такої інфраструктури. Практична значимість проблеми забезпечення безпеки «розумного

будинку» полягає в реалізації заходів щодо захисту ІТ-інфраструктури для забезпечення особистої безпеки проживаючих громадян, забезпечення їх здоров'я і необхідних санітарно-гігієнічних умов, захисту майна. Існує проблема, пов'язана з неповною або недостатнім опрацюванням і дослідженням загроз перш за все інформаційної безпеки «розумного будинку» і відповідно, недостатніми механізмами їм протидії.

Постановка проблеми. Сучасні ІТ-системи «SmartCity» мають вразливості і не захищені від загроз. Так як така система являє собою комп'ютерну мережу, загрози націлені насамперед на вразливості мережевої структури

Аналіз останніх досліджень і публікацій.

Інтернет речей (IoT) складається зпристроїв, які генерують, обробляють та обмінюються величезною кількістю критичноважливих для безпеки даних, а також конфіденційної інформації, і, отже, є привабливимидля різних кібератак [8]. Існують різні дослідження щодо безпеки та конфіденційності IoT та розумногобудинку. Цим питанням присвячені експериментальні дослідження вітчизняних тазакордонних вчених: Л. Монастирського, О. Петришина, A. Chakravorty, T. Wlodarczyk,C. Rong, A. Dorri, R. Jurdak, S. S. Kanhere, P. Gauravaram, S. Fan, L. Song, C. Sang та інші.Вони одностайні в тому, що технологія IoT вимагає легкої, масштабованої тарозподіленої безпеки та захисту конфіденційності. Важливим для таких систем єствореннямереж малого радіуса дії, здатних тримати зв'язок основного процесора збагатьма пристроями і надійно передавати дані, економно витрачаючи живлення IoTпристроїв [4].

Мета статті.

Дослідити надійність технологій обміну інформацією у системі керування "SmartCity" на прикладі «розумного» будинку, узагальнити особливості застосування технологій передавання даних і їх захищеності щодо різних впливів, розробити рекомендації щодо їх використання.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

«Smartcity» або «розумне місто» – сучасне місто, створене із застосуванням технологічних пристроїв для максимально комфортного проживання людей. «Smartcity» це система, що вміщає в собі комфорт, безпечне й економне проживання для усіх жителів міста.

У найпростішому випадку система повинна вміти розпізнавати конкретну ситуацію, що виникає в будинку, і реагувати відповідно: одна із систем може контролювати поведінку інших систем за допомогою заздалегідь розробленого алгоритму. Іншими словами, це будівля, інженерна система якої може адаптуватися до можливих майбутніх змін. В якості об'єкта захисту позначено житлові або нежитлові (не використовуються для проживання) місця, обладнані комп'ютерною технікою та пристроями управління. Це обладнання та засоби управління підтримують інформаційні технології та можуть вживати активних заходів для задоволення потреб людей у комфортному та безпечному житті.Створюючи та підтримуючи стандартні санітарні умови для повсякденної діяльності людини, призначене комп'ютерне обладнання та методи управління (приводні реле, виконавчі механізми) можуть реагувати на зміни в потребах людини таких як: особиста безпека, зменшення ризику загрози здоров'ю та майну громадян [1]. Отже, за допомогою автоматичного управління системою життєзабезпечення в будинку / житловому приміщенні,

включаючи спілкування з навколишнім середовищем за допомогою інформаційного спілкування, може бути досягнута мета управління в «розумному будинку» - забезпечення комфортних та безпечних умов проживання. «Розумний дім» із використанням набору засобів автоматизації та інформаційних технологій може забезпечити ефективну та безпечну експлуатацію та запобігти ризику пошкодження, що може призвести до збоїв у комунальному господарстві, вентиляції, опаленні, електропостачанні, газопостачанні, безпеці, захисті від холоду та морозу, систем гарячого водопостачання, водовідведення, комунікації та інших будівельних та структурних системах [1].

Коли говорять «розумний будинок» - вважається, що мова йде про сукупність приміщень, таких як офіси, що зв'язані єдиною системою (автоматизованою) управління та моніторингу (рис. 1).

Рис. 1. Основні підсистеми «розумного будинку»

Список підсистем «SmartCity» можна розкласти наступним чином [2]:
– освітлення;
– гаряче водопостачання та опалення;
– холодне водопостачання та протікання трубопроводу;
– медична система (за наявності);
– електрична мережа, електроживлення;
– аудіо та відео система;
– телефонія;
– телебачення;
– локальна та глобальна мережа;
– сигналізація (охоронна, пожежна);
– відеоспостереження;
– система запобіжників;
– доступ в приміщення;
– дистанційний контроль жилим приміщенням;
– вентиляція та кондиціювання;
– інфраструктура надворі.

У той же час ви можете зустріти використання терміну "інтелектуальна будівля", який позначає термін, що використовується в інтегрованій системі автоматизації управління нежитловими або житловими будинками. квартира. Отже, термін "розумний будинок" тут і надалі буде в основному використовуватися для житлових (особистих)

ISSN 2663 - 4023

будинків, квартир у багатоквартирних будинках або ізольованих будинків у нежитлових будинках в межах сфери управління не "розумних будинків"[3].

Існує два види організації системи «розумний дім»:

– децентралізований;

– централізований.

Будова розумного будинку являє собою контролер, елементи управління, спеціалізованого обладнання зв’язаного в єдину локальну мережу (рис.2).

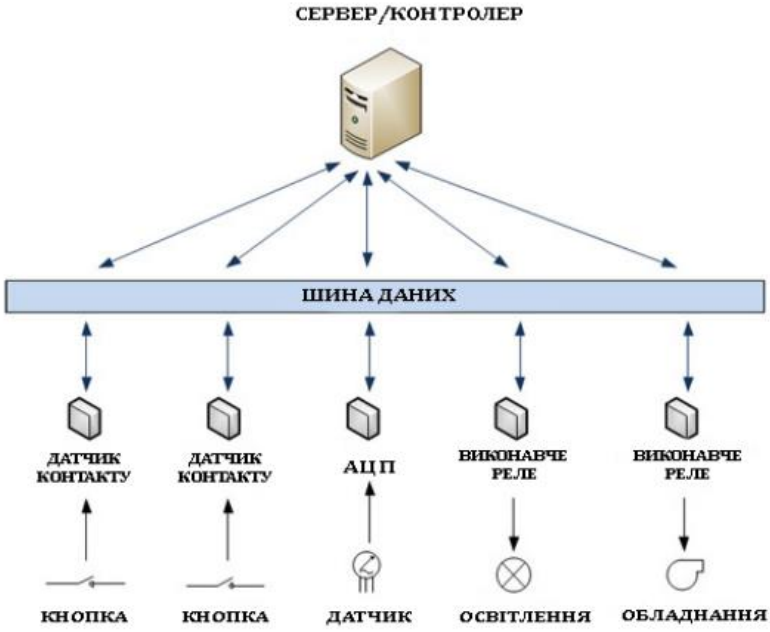

Рис. 2. Схема централізованої системи «розумного будинку» з головним комп’ютером

Елемент управління - це обчислювальний або командний пристрій (пульт дистанційного керування), за допомогою пристрою можна надсилати команди виконання в систему «розумний дім». Управління може бути реалізовано пультом дистанційного керування, сенсорним екраном, смартфоном та різним датчиками (світло, стан, температура, вологість тощо) [4].

Центральний контролер контролює всю систему і кожен окремий елемент. Це обчислювальний пристрій, який зберігає в пам'яті і виконує всі команди від користувачів або виконуваних програм [2, 5]. До керованих пристроїв "Розумний дім" зазвичай включено все обладнання та побутова техніка, від лампочок до складних систем, що використовуються для захисту та контролю складу повітря.

Децентралізований підхід означає розгортання системи з розподіленою логікою для виконання команд [6]. На відміну від централізованого методу, у децентралізованому методі відсутній центральний контролер. за цих обставин система складається з датчиків, датчиків та активаторів (рис. 3). Датчик виявляє будь-які зміни характеристик будинку, переміщення або зміну параметрів, встановлених програмою, і реагує на ці зміни командою на пристрій, який починає роботу за допомогою активатора.

ISSN 2663 - 4023

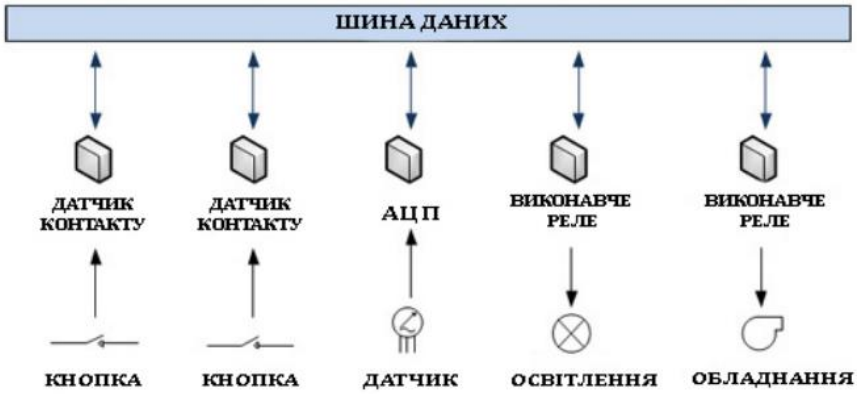

Рис. 3. Схема децентралізованої системи «розумного будинку» без контролера керування

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для цього найважливішого механізму безпеки необхідно знайти протокол передачі інформації, який повинен відповідати стандартам конфіденційності, цілісності та доступності даних. Важливим моментом буде спосіб спілкування з іншими структурними елементами житлової площі: розумні будинки в цьому сегменті ринку можуть використовувати загальну мережеву інфраструктуру [7,8].

Однак, незважаючи на розвиток та поступову формальну та неформальну стандартизацію технологій розумного будинку [9] та будь-якої домашньої автоматизації [10], все ще існує проблема вибору протоколів для передачі інформації між керованими пристроями, датчиками та іншими елементами будинку [11]. Ця проблема особливо серйозна, коли це необхідно для забезпечення конфіденційності та цілісності даних, що циркулюють у системі.

Метою цього дослідження є пошук захищеного мережевого протоколу, який дозволяє використовувати його в автоматичному сигналізуючому обладнанні, щоб не можна було використовувати спеціальні програмні та апаратні рішення для впливу на конфіденційність та цілісність інформації. Доступність цих пристроїв також повинна забезпечуватися завдяки можливості автономної роботи. Основні протоколи безпеки можна розділити на дві категорії: придатні для проводових рішень (таких як IPsec, SSL, TLS); та безпроводових систем (ZigBee, Z-Wave, Thread, WeMo) [13]. У житлових приміщеннях зазвичай використовуються різні пристрої та змішані технології. Ці пристрої та технології, як правило, є додатковими компонентами існуючої інфраструктури. Тому основним напрямком аналізу є безпроводові протоколи, що дозволяють легко реалізовувати мережеві взаємодії.

Провідні рішення слід розглядати лише в контексті впровадження домашньої автоматизації на ранніх етапах будівництва кімнати чи квартири та при проектуванні ключових елементів системи. Коли використовуються безпроводові протоколи та пристрої, виникають питання щодо їх здатності забезпечити належний рівень конфіденційності та цілісності даних [14]. Це пов'язано з впливом на існуючі безпроводові мережі, популяризацією протоколів зв'язку та можливістю перехоплювати сигнали з їх подальшим аналізом та атакою. Є й інші вимоги щодо забезпечення доступності даних у «розумному домі» та можливості автономної роботи.

Беремо до розгляду основні безпроводові технології, що допомагають реалізувати захищену автоматизацію. Порівнювати будемо наступні можливості [15]:

1) Шифрування: технології та засоби утворення захищеної передачі даних

2) Топологія: способи забезпечення доступу пристроїв до мережі.

3) Автономність: правила та рішення для забезпечення автономної роботи та відкату до резервної копії.

4) Широкополосна мережа: швидкий доступ до мережі задля мінімізації затримки між командою та початком її виконання навіть за умови перевантаження каналу зв'язку [7, 16].

Спочатку розглянемо шифрування. Для створення безпечної передачі даних ця функція є важливою. Усі протоколи використовують шифрування, але по різному. Якщо порівняти Zig-Bee та Z-Wave, вони обидва використовують AES-128, та головна відмінність Z-Wave полягає в тому, що ця технологія може використовуватися лише на виділених вузлах системи, а не будь де, як у Zig-Bee [17]. Thread використовує сучасний протокол, заснований на еліптичних кривих, для яких ще не знайдено алгоритму субекспоненційногорішення.WeMob в цьому випадку суперечливий, його можливості шифрування повністю залежать від можливостей маршрутизатора, це шифрування TKIP / AES. З точки зору доступності та можливості в перерахованих алгоритмах, необхідно використовувати Zig-Bee. У майбутньому, доки підтримується швидкість шифрування, протокол Thread матиме можливість замінити Zig-Bee [5]. Крім того, якщо порівняти алгоритм AES (Zig-Bee, WPA2, ZWave) (рис. 4) із підключенням J-PAKE + NISTP-256, ви зможете побачити ефективність алгоритму AES для швидкої передачі даних. Однак на практиці всі алгоритми, як правило, використовують команди короткої довжини, тому стандарт швидкості має сенс лише тоді, коли протокол використовується в нестандартнихситуаціях для обладнання та може працювати автономно.

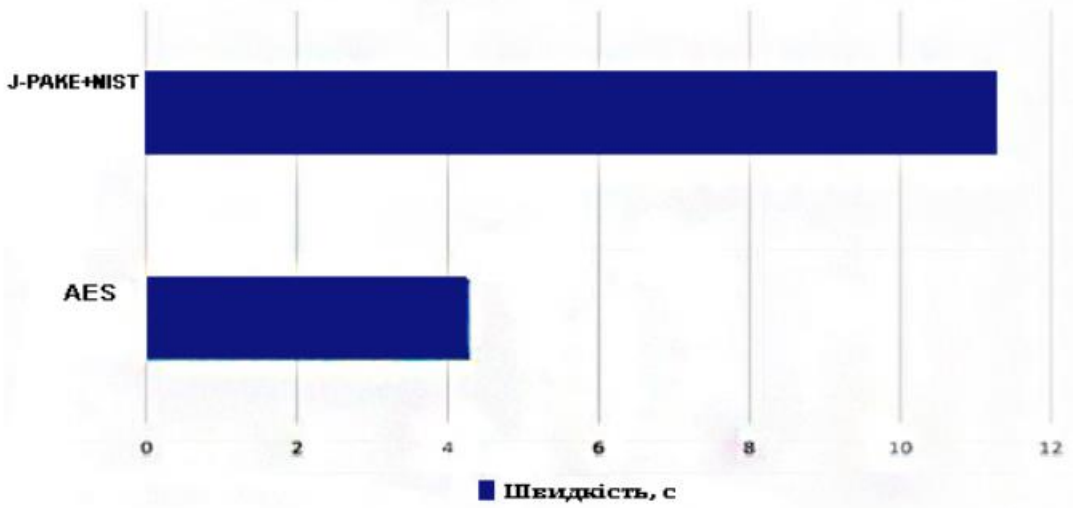

Рис. 4. Порівняння швидкості шифрування протоколів AES і зв'язки NISTP-256 + J-PAKE на прикладі кількох тестів (чим менше, тим краще)

З точки зору створеної топології мережі, у запропонованому протоколі є два основних варіанти. Перший тип - це «зірка», є деяке центральне обладнання, яке виступає в ролі сполучної ланки. Його легко розгорнути, але коли центральний пристрій виходить з ладу, це може мати наслідки у вигляді порушення доступності [10]. Протоколи WeMo та Zig-Bee можуть розгортати такі мережі. Друга категорія -

стільникова децентралізована мережа. Zig-Bee, Z-Wave і Thread підтримують цю технологію, дві останні є єдиними можливими технологіями. Завдяки своїй децентралізації мережа покращує доступність всієї мережі [15].

Доступність - другий важливий критерій безпечного розумного будинку. Якщо дані від датчиків руху, датчиків пожежі та інших датчиків не передаються належним чином, можуть виникнути різні надзвичайні ситуації. Протокол WeMo повністю залежить від маршрутизатора, тому в разі несправності він не може забезпечити автономну роботу пристроїв «розумного дому». Якщо розглянути Z-Wave, протокол все одно може працювати без основного джерела живлення. Окрім джерела живлення від акумулятора, Zig-Bee та Thread також мають алгоритми самоорганізації та самовідновлення мережі, які можуть підтримувати доступність даних про інфраструктуру будинку без єдиного вузла [18].

Швидкість передачі даних на протоколах, що працюють на низьких частотах, не є їх сильною стороною, але їх ресурсів більш ніж достатньо для передачі основних команд. У цьому стандарті виділяється лише WeMo, і його швидкість передачі даних залежить від пропускної здатності маршрутизатора. Питання заміни захищеного бездротового протоколу російським слід згадати окремо. Хоча в АСУ ТП використовуються спеціальні протоколи передачі інформації (наприклад, ОВЕН) або бездротова технологія MeshLogic, технічні функції не дозволяють їх правильно використовувати в системах домашньої автоматизації в їх поточному вигляді.

Отже, з точки зору основних характеристик найбільш підходить технологія Zig-Bee, вона найбільшою мірою вирішує проблему конфіденційності, цілісності та доступності даних у системі з автоматичною сигналізацією [12]. Протокол Thread використовує більш сучасні технології, але нещодавно опубліковані основні технічні характеристики та відсутність іншої інформації про обладнання, що використовується, унеможливлюють назвати його повною заміною Zig-Bee, і це може бути лише найближчим часом. Протокол WeMo не підходить для створення безпечної системи "розумного дому".

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Метою даної роботи є дослідження безпеки IT-системи «розумний дім» шляхом виявлення загроз та вразливостей інформаційної безпеки. Система «розумного дому» базується на телекомунікаційній (комп’ютерній) мережі, тому загрози інформаційній безпеці в основному можуть бути спричинені вразливостями в структурі мережі: кодом операційної системи (наприклад, вразливістю до переповнення пам'яті, управління оновленнями операційної системи); протоколами передачі , такими як TCP, DNS, SMTP або ICMP; дефекти прикладних програм (firmware, такі як Apache); помилки програм користувача; програмним забезпеченням, вбудованим в апаратні пристрої, такі як маршрутизатори, BIOS; перехоплення та управління повідомленнями в бездротових системах.

Для того, щоб зменшити ризики, пов'язані з реалізацією цих загроз, необхідно застосовувати такі заходи: використовувати механізми ідентифікації та аутентифікації користувачів, використовувати шифрування та контроль цілісності переданих даних, використовувати антивірусне програмне забезпечення, контроль доступу, розподіл навантаження механізмів, Регулярно перевіряйте працездатність усіх елементів системи та використовуйте резервне живлення.

Крім того, найбільш підходящою технологією було визначено Zig-Bee, яка максимально вирішує проблему забезпечення конфіденційності, цілісності та доступності даних в системі автоматичної сигналізації. Протокол Thread використовує більш сучасні технології, але нещодавно опубліковані основні технічні характеристики та відсутність іншої інформації про обладнання, що використовується, унеможливлюють назвати його повною заміною Zig-Bee, і це може бути найближчим часом. Протокол WeMo не підходить для створення безпечної системи "розумного дому".

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Тесля, Е. А. (2008). «Умный дом» своими руками. Строим интеллектуальную цифровую систему в своей квартире. *Петербург*.
2. Элсенпитер, Т. Р., & Велт, Дж. (2005). *Умный Дом строим сами* (Т. Р. Элсенпитер & Дж. Велт, Ред.). КУДИЦ–ОБРАЗ.
3. Гололобов, В. Н. (2007). *Умный дом» своими руками* (В.Н. Гололобов, Ред.). НТ Пресс.
4. Харке, В.Н. (2006). *Умныйдом. Объединение в сетьбытовойтехники и систем коммуникаций в жилищномстроительстве*. Техносфера.
5. Adams, C. E. (2002). Homeareanetworktechnologies. *BT TechnologyJournal*, *20*(2), 53–72.
6. Mario, B.B., & Candid, W. (2015). *Insecurityinthe Internet ofThings*. SECURITY RESPONSE.
7. Michael, S., & Ulf, L. (2014). *Smart-Home-Starter-Kits*. AV-TEST-Studie.
8. Лапонина, О.Р. (2005). *Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия*. Интернет–университет информационных технологий – ИНТУИТ.ру.
9. Широков, 9. Ф. (2001). Bluetooth: на пути к миру без проводов. *Открыты есистемы*, (2). http://www.radioscanner.ru/info/article95/
10. Teslyuk, V., Beregovskyi, V., & Pukach, A. (2013). Automation of the smart house system-level design. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska*, *3*(4), 81–84. https://doi.org/10.35784/iapgos.1487
11. Жураковский, Б. Ю. (2018). Объектно-оринтированная модель системы управления телекоммуникационной сетью. *Актуальные научные исследования в современном мире*, (11), 60–65.
12. Жураковський, Б.Ю. (2020). Стандарти SmartCity. *Актуальныенаучныеисследования в современном мире*. (2), 41–44.
13. Жураковский, Б. Ю. (2020). Алгоритм виявлення та усунення несправностей в мультисервісних мережах. *Актуальные научные исследования в современном мире*, (5), 94–101.
14. Druzhynin, V., Toliupa, S., Pliushch, O., Stepanov, M., & Zhurakovskyi, B. (2000). Features of processing signals from stationary radiations ourcesinmulti-position radiomonitoring systems. У *CEUR WorkshopProceedings* (с. 46–65). http://ceur-ws.org/Vol-2746/
15. Zhurakovskiy, B., & Tsopa, N. (2019). Assessment. technique and selection of interconnecting line of information networks. У *3rd International Conference on Advanced Information and Communications Technologies (AICT)* (с. 71–75). https://doi.org/10.1109/AIACT.2019.8847726
16. Zhurakovskyi, B., Boiko, J., Druzhynin, V., Zeniv, I., & Eromenko, O. (2020). Increasing the efficiency of information transmission in communication channels. *Indonesian Journal of Electrical Engineering and Computer Science*, *19*(3), 1306. https://doi.org/10.11591/ijeecs.v19.i3.pp1306-1315
17. Жураковський, Б. Ю., Пархомей, І. Р., & Дружинін, В. А. (2018). Обробка інформації в сенсорних мережах. *Адаптивні системи автоматичного управління*, *1*(32), 42–57. https://doi.org/10.20535/1560-8956.32.2018.145610
18. Овсієнко, К. (б. д.). *Захист інформації в технологіях "розумного будинку"*. https://cutt.ly/DzBpWhA

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (11), 2021
ISSN 2663 - 4023

Mykyta Moshenchenko
Graduate
NationalTechnicalUniversityofUkraine “IgorSikorskyKyivPolytechnicInstitute”, Kyiv, Ukraine
0000-0002-0211-2263
nrodan@icloud.com

Bohdan Zhurakovskyi
DoctorofTechnicalSciences, Professor
NationalTechnicalUniversityofUkraine “IgorSikorskyKyivPolytechnicInstitute”, Kyiv, Ukraine
0000-0003-3990-5205
zhurakovskiybyu@tk.kpi.ua

INFORMATION PROTECTION IN “SMART CITY” TECHNOLOGIES

Abstract. This article discusses the problems of information security in "SmartCity" systems. The comparison of existing solutions and data protocols for wired solutions, such as IPsec, SSL, TLS and wireless systems: ZigBee, Z-Wave, Thread, WeMo. The advantages and disadvantages of each of the existing systems are analyzed. The SmartCity system must be able to recognize a specific situation that arises in the house, city, workplace, when processing large amounts of data, to respond accordingly: one of the systems can control the behavior of other systems using a pre-designed algorithm. The main purpose of the "SmartCity" system is to save energy, which is becoming increasingly important due to their rise in price in Ukraine. Therefore, intellectualization is becoming increasingly popular, catching up with global trends in home automation. However, despite the development and gradual formal and informal standardization of smart city technologies, and any home automation, there is still the problem of choosing protocols for the transfer of information between controlled devices, sensors and other elements. This problem is especially serious when it is necessary to ensure the confidentiality and integrity of data circulating in the system. The purpose of this study is to find a secure network protocol that allows you to use it in automatic signaling equipment, so you can not use special software and hardware solutions to affect the confidentiality and integrity of information.In the article is not the last issue of information security such a house of the city government system or production, can cause very great damage to its owner. As remote management and access to information are quite common nowadays, secure schemes, encryption and protection schemes should be used to reduce the percentage of vulnerabilities and prevent intruders from causing harm.

Keywords: smartcity: protocol; IoT; wireless; informationprotection; wi-fi: zigbee; wemo..

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Teslya, E.A. (2008). Do-it-yourself smart home. We are building an intelligent digital system in our apartment. Petersburg.
2 Elsenpeter, T.R., & Welt, J. (2005). We build the Smart Home ourselves (T.R. Elsenpeter & J. Welt, Ed.). KUDITS-IMAGE.
3 Gololobov, V.N. (2007). Do-it-yourself smart home (VN Gololobov, Ed.). NT Press.
4 Harke, V.N. (2006). Smart House. Networking of household appliances and communication systems in housing construction. Technosphere.
5 Adams, C. E. (2002). Homeareanetworktechnologies. BT TechnologyJournal, 20 (2), 53–72.
6 Mario, B.B., & Candid, W. (2015). Insecurityinthe Internet ofThings. SECURITY RESPONSE.
7 Michael, S., & Ulf, L. (2014). Smart-Home-Starter-Kits. AV-TEST-Studie.
8 Laponina, O.R. (2005). Fundamentals of network security: cryptographic algorithms and communication protocols. Internet University of Information Technologies - INTUIT.ru.
9 Shirokov, 9. F. (2001). Bluetooth: Towards a wireless world. The systems are open, (2). http://www.radioscanner.ru/info/article95/
10 Teslyuk, V., Beregovskyi, V., & Pukach, A. (2013). Automation of the smart house system-level design. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 3 (4), 81–84. https://doi.org/10.35784/iapgos.1487

11 Zhurakovsky, B. Yu. (2018). Object-oriented model of a telecommunication network management system. Actual scientific research in the modern world, (11), 60–65.
12 Zhurakovskiy, B.Yu. (2020). SmartCity standards. Relevant scientific research in the modern world. (2), 41–44.
13 Zhurakovsky, B. Yu. (2020). Algorithm for detecting that faults in multi-service framing. Actual scientific research in the modern world, (5), 94-101.
14 Druzhynin, V., Toliupa, S., Pliushch, O., Stepanov, M., & Zhurakovskyi, B. (2000). Features of processing signals from stationary radiations ourcesinmulti-position radiomonitoring systems. From CEUR Workshop Proceedings (pp. 46–65). http://ceur-ws.org/Vol-2746/
15 Zhurakovskiy, B., & Tsopa, N. (2019). Assessment. technique and selection of interconnecting line of information networks. At the 3rd International Conference on Advanced Information and Communications Technologies (AICT) (pp. 71–75). https://doi.org/10.1109/AIACT.2019.8847726
16 Zhurakovskyi, B., Boiko, J., Druzhynin, V., Zeniv, I., & Eromenko, O. (2020). Increasing the efficiency of information transmission in communication channels. Indonesian Journal of Electrical Engineering and Computer Science, 19 (3), 1306. https://doi.org/10.11591/ijeecs.v19.i3.pp1306-1315
17 Zhurakovsky, B. Yu., Parkhomey, I. R., & Druzhinin, V.A. (2018). Processing of information in sensory framing. Adaptive systems of automatic control, 1 (32), 42–57. https://doi.org/10.20535/1560-8956.32.2018.145610
18 Ovsinko, K. (b. D.). Zakhist information in technologies of the "smart house". https://cutt.ly/DzBpWhA