УДК 004

Д.Іщенко, магістр гр. КІ-22М-2
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПЛАТФОРМИ УПРАВЛІННЯ МЕРЕЖНИМИ ПРИСТРОЯМИ ІНТЕЛЕКТУАЛЬНОГО БУДИНКУ ЗА ТЕХНОЛОГІЄЮ CWMP

У статті розроблено програмне забезпечення, яке призначено для системи платформи управління мережними пристроями інтелектуального будинку за технологією CWMP. Метою розробки є дослідження та програмна реалізація системи платформи управління мережними пристроями інтелектуального будинку за технологією CWMP. Об’єктом дослідження є процес платформи управління мережними пристроями інтелектуального будинку за технологією CWMP. Предметом дослідження є методи платформи управління мережними пристроями інтелектуального будинку за технологією CWMP. Методи дослідження базуються на методах Інтернету речей, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи платформи управління мережними пристроями інтелектуального будинку за технологією CWMP. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. «Розумний будинок» або «інтелектуальний будинок» – це централізована автоматизована система управління всіма електричними навантаженнями, інженерними системами й мультимедійним устаткуванням у будинку, що дозволяє досягти нового рівня комфорту, безпеки й енергозбереження.

Можливості системи «розумний будинок» обмежуються тільки Вашою уявою. Ви можете створювати різні сценарії, поєднуючи між собою систему освітлення, опалення, кондиціювання, систему безпеки й відеоспостереження, домашній кінотеатр, систему управління воротами, вікнами, жалюзями. У теж час інженерією легко управляти за допомогою сенсорних панелей і вимикачів, універсального пульта, мобільного телефону.

Система «інтелектуальний будинок» надає наступні послуги:

– Управління освітленням. Ви можете управляти освітленням у будинку й на вулиці, при наявності/відсутності руху, створювати світлові сценарії, ефект присутності під час Вашої відсутності, виключати все освітлення, ідучи з будинку.

– Управління мікрокліматом. Система забезпечує загальне управління приточно-витяжною вентиляцією, кондиціонерами, казанами, системою обігріву, теплими підлогами, теплою покрівлею. Ви можете централізовано регулювати мікроклімат у всьому будинку або індивідуально кожної кімнати.

– Мультирум. Медіацентр. Це система розподілу звуку й відео, що охоплює велику кількість окремих приміщень, від віталень і спалень до кухні, ванною й навіть комори. Мультирум також може забезпечити «ландшафтне озвучування присадибної ділянки під час літньої вечірки.

– Відеоспостереження. Детальний звіт подій, що відбуваються під час вашої відсутності. Особи й дії фіксуються в системі й зберігаються в її пам'яті. Ви одержуєте можливість оперативного перегляду ситуації на будь-якому моніторі або комп'ютері в будь-якій точці миру, використовуючи Інтернет.

– Захист від затоплення й витоку газу. Відключення газу або води (залежно від типу аварійної ситуації), повідомлення у відповідні служби, а також на мобільний телефон замовника.

– Охоронна й пожежна сигналізація. Визначення факту несанкціонованого проникнення на охоронюваний об'єкт або появи ознак пожежі, видачі сигналу тривоги й включення виконавчих пристроїв (світлових і звукових оповіщувачів, реле й т.п.).

– Засоби управління Розумним будинком. Система підтримує всі сучасні доступні засоби управління, починаючи від звичайного вимикача, або пульта дистанційного управління, закінчуючи сенсорною панеллю із графічним інтерфейсом, кишеньковим комп'ютером або мобільним телефоном.

Завдяки системі «розумний будинок» різні підсистеми починають працювати погоджені, інженерне устаткування – самостійно, з'являється поняття «сценарій», коли по натисканню однієї кнопки, відбувається будь-який набір дій.

У результаті Ви одержуєте – комфорт, безпеку й економію електроенергії.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-20] було виявлено певні прогалини у забезпеченні системи платформи управління мережними пристроями інтелектуального будинку за технологією cwmp**.**

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи платформи управління мережними пристроями інтелектуального будинку за технологією CWMP.

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

– Огляд існуючих систем платформи управління мережними пристроями інтелектуального будинку за технологією CWMP.

– Дослідження системи платформи управління мережними пристроями інтелектуального будинку за технологією CWMP.

– Програмна реалізація системи платформи управління мережними пристроями інтелектуального будинку за технологією CWMP.

Об'єктом дослідження є процес платформи управління мережними пристроями інтелектуального будинку за технологією CWMP.

Предметом дослідження є методи платформи управління мережними пристроями інтелектуального будинку за технологією CWMP.

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

Виклад основного матеріалу. TR-069 (скорочення від Technical Report 069) – технічна специфікація, що описує протокол управління абонентським устаткуванням через глобальну мережу – CWMP (CPE WAN Management Protocol). Стандарт був опублікований в 2004 році консорціумом DSL Forum, перейменованим пізніше в Broadband Forum. Ціль – стандартизація й уніфікація принципів і підходів до управління абонентським устаткуванням різних виробників.

CWMP є протоколом прикладного рівня, що використовує як інструмент передачі інформації SOAP (Simple Object Access Protocol) – надбудову над HTTP. Всі дані передаються у форматі XML.

Відповідно до специфікації на території провайдеру повинен бути розташований сервер автоконфігурації (ACS – Auto Configuration Server), що організує взаємодію з абонентським устаткуванням, що здійснює обробку запитів від пристроїв і здатного підключати додаткові сервіси. Сесія може бути ініційована як з боку CPE, так і з боку ACS.

Для того, щоб було можливо управління пристроєм, він повинен мати IP-адресу незалежно від типу цього пристрою (Bridge, Router, IP-Phone). Для забезпечення захищеного з'єднання в TR-069 використовується SSL і TLS.

TR-069 підтримує наступні функції:

- Конфігурація. Мова йде як про початкову конфігурацію, так і автоконфігурації вже працюючого пристрою або внесенні змін у налаштування.
- Управління версіями ПЗ і його відновлення.
- Аналіз log-файлів, продуктивності й діагностика пристрою.
- Виконання збережених процедур
- Вибір CPE для обслуговування може здійснюватися по різних умовах. Наприклад, конкретний пристрій, по виробнику, моделі або версії ПЗ.

Використовувати автоконфігурацію можливо при будь-якому способі придбання пристроїв:

- Устаткування надається під час підписання договору.
- Устаткування купується абонентом у вигляді комплекту підключення до мережі оператора.
- Устаткування купується абонентом самостійно й не має попередніх налаштувань на мережу оператора.

Протокол CWMP визначає принципи взаємодії між абонентськими пристроями (CPE) і сервером Auto-Configuration Server (ACS). ACS, згідно TR-069, є мережним пристроєм і являє собою сервер додатків, що автоматизує реалізацію основних методів управління абонентськими пристроями (CPE):

- Автоматичне налаштування й динамічне реконфігурування сервісів (послуг, надаваних абонентам оператором, таких як доступ в Інтернет, VoIP, IPTV).
- Управління програмним забезпеченням (firmware) CPE.
- Моніторинг стану й параметрів продуктивності CPE.
- Діагностика.

Состав специфікації TR-069

Під формулюванням TR-069 звичайно розуміють весь комплекс специфікацій, розроблених Broadband Forum в області управління CPE. Прикладена таблиця визначає состав зазначених специфікацій. Актуальні версії відповідних документів наведені на сайті www.broadband-forum.org.

TR-046 – Auto-Config: Architecture & Framework – Визначає основні принципи автоматизованого конфігурування кінцевих пристроїв, підключених за технологією DSL.

TR-069 – CPE WAN Management Protocol v1.1 – Специфікація протоколу CWMP.

TR-098 – Internet Gateway Device Data Model for TR-069 – Описує модель даних CWMP для шлюзів доступу в Інтернет.

TR-104 – DSLHomeTM Provisioning Parameters for VoIP CPE – Описує модель даних CWMP для пристроїв VoIP.

TR-106 – Data Model Template for TR-069- Enabled Devices – Визначає об'єктну структуру й вимоги до моделі даних CWMP.

TR-111 – DSLHomeTMApplying TR-069 to Remote Management of Home Networking Devices – Визначає функції управління пристроями локальних мереж, у тому числі за NAT.

TR-135 – Enabling Network Throughput Performance Tests and Statistical Monitoring – Визначає об'єкти CWMP, що забезпечують рішення завдання моніторингу продуктивності й контролю доступності CPE.

TR-140 – TR-069 Data Model for Storage Service Enabled Devices – Описує модель даних CWMP для пристроїв зберігання.

TR-142 – Framework for TR-069 enabled PON Devices – Описує модель даних CWMP для пристроїв PON і підключених до них оптичних пристроїв.

TR-143 – Enabling Network Throughput Performance Tests and Statistical Monitoring – Визначає об'єкти CWMP, що забезпечують рішення завдання моніторингу продуктивності й контролю доступності CPE.

TR-157 – Component Objects for CWMP – Розширення об'єктної моделі CWMP відповідно до нових технологій і можливостями домашніх мереж.

TR-181 – Device Data Model for TR-069 – Визначає єдину модель даних для всіх пристроїв, що підтримують TR-069.

TR-196 – Femto Access Point Service Data Model – Описує модель даних CWMP для пристроїв femto-cell.

«Південний» інтерфейс (southbond) забезпечує реалізацію перерахованих вище функцій управління стосовно CPE. Спочатку передбачалося управління CPE з використанням технології DSL. У цей час зусиллями як самого Broadband Forum, так і інших організацій (Home Gateway Initiative, Digital Video Broadcasting), до складу керованих по TR-069 CPE увійшли інтегровані пристрої доступу (IAD), PON і пов'язані з ними оптичні пристрої, VoIP-пристрої, приставки IPTV, інші пристрої домашніх мереж.

«Північний» (northbound) інтерфейс забезпечує взаємодію ACS з іншими системами OSS/BSS провайдеру в рамках реалізації єдиних наскрізних процесів управління послугами.

Функції управління

Ключова й одна з найбільш затребуваним бізнесом функцій управління CPE, обумовлених TR-069 – автоматичне налаштування й динамічне реконфігурування сервісів. Специфікація визначає можливість як первинного, так і повторного конфігурування CPE, наприклад, по запиті абонента або при зміні тих або інших параметрів послуги.

TR-069 визначає можливість виконання операцій конфігурування як стосовно одному конкретного CPE, так і до групи, об'єднаних одним або декількома загальними ознаками, такими як виробник CPE, модель, версія firmware і т.д. Підтримується можливість роботи з опціональними наборами параметрів послуг (наприклад, з параметрами, що визначають платежі, функції Батьківського контролю), включення яких вимагає щодо більше високого рівня доступу, у тому числі з використанням механізму цифрового підпису. Функція управління програмним забезпеченням CPE забезпечує виконання завантаження ПЗ на пристрій. Протокол визначає механізми ідентифікації версій керованого ПЗ, ініціації (з ініціативи ACS або по запиті CPE), виконання й завершення завантаження файлів образів, логування й оповіщення служби експлуатації про результативність виконання завантаження. Крім функцій безпосереднього управління конфігурацією CPE, протокол CWMP визначає методи надання доступу до інформації, що може бути використана сервером ACS для моніторингу статусу й продуктивності CPE. Протокол CWMP також визначає набір механізмів, які дозволяють CPE самостійно сповіщати ACS про зміни свого стану. Крім можливостей моніторингу CPE, CWMP надає також механізми діагностики, у тому числі состав параметрів, які можуть містити діагностичну інформацію, методи надання діагностичної інформації. Істотною відмінністю від SNMP-протоколу є можливість для ACS (виконуючого роль менеджера) не тільки запросити діагностичну інформацію з CPE, але й одержати неї в необхідному обсязі від самого CPE (у випадку SNMP можливе одержання тільки SNMP- трапа, всю іншу інформацію менеджер повинен самостійно запитувати в агента). На додаток до перерахованим вище функцій CWMP надає механізми автоматичної автентифікації й авторизації на веб-сайтах оператора залежно від ідентифікатора й типу використовуваного для доступу CPE (докладніше відповідний механізм описаний у додатку D до специфікації TR-069).

Архітектура CWMP

Архітектура протоколу CWMP містить у собі:

- Стек протоколів CWMP, використовуваний для організації взаємодії між ACS і CPE.
- Параметри CWMP.
- Процедури CWMP.

Стек протоколів

Протокол CWMP реалізований як комплекс стандартних і спеціально розроблених протоколів. Структура стеку:

- CPE/ACS Management Applicatioin.
- RPC.

- SOAP 1.1.
- HTTP.
- SSL/TLS.
- TCP/IP.

Параметри CWMP

Параметри CWMP являють собою модель даних, структура якої визначена іншим документом Broadband Forum – «TR-106: Data Model Template for TR-069-Enabled Device». Основне призначення параметрів – надання даних ACS про характеристики й стан CPE, управління їхньою конфігурацією. Параметри можуть бути визначені як read-only або read-write. Параметри read-only можуть використовуватися сервером ACS для визначення специфічних характеристик CPE, поточного стану CPE або одержання накопиченої статистики. Параметри read-write дозволяють серверу ACS змінювати конфігурацію CPE. В CWMP всі параметри об'єднані в ієрархічну структуру. Ця структура даних в CWMP представлена у вигляді об'єкта. Кожний об'єкт містить один параметр або набір параметрів. Кожний CPE має тільки один головний об'єкт (root), залежно від типу пристрою приймаюче значення Device або InternetGatewayDevice.

У більшості випадків, головний об'єкт містить у собі три елементи:

- Common Objects.
- Components.
- Service Objects.

Об'єкт Components містить параметри, що забезпечують різні функції TR-069. Їхня специфікація наведена в окремих документах BroadBand Forum.

CPE/ACS Management Application – додаток, що запускається на CPE або ACS, що реалізує функції CWMP. Додаток не специфікується CWMP і може являти собою сервіси, GUI додатка й т.п. RPC – набір методів RPC, використовуваних при взаємодії між ACS і CPE, описаний у специфікації CWMP.

SOAP – всі повідомлення, передані між ACS і CPE, конвертуються у формат XML. Використання SOAP дозволяє забезпечити платформонезалежність рішення, піти від специфіки реалізації конкретних додатків.

HTTP – обраний як транспортний протокол для запитів SOAP за його поширеність. Передбачається, що в більшості випадків налаштування міжмережних екранів припускають пропуск трафіку по портах http, відповідно, при впровадженні CWMP не буде потрібно істотного перегляду корпоративних політик інформаційної безпеки SSL/TLS – при передачі даних між CPE і ACS використовуються відповідні методи шифрування трафіку, що забезпечують конфіденційність і цілісність переданих даних. Використовується автентифікація взаємодіючих по протоколі CWMP сторін з використанням сертифікатів.

TCP/IP – всі повідомлення, передані між ACS і CPE, відповідно до TR-069 повинні віддаватися з використанням протоколу TCP для забезпечення їхньої гарантованої доставки.

Використання TCP також визначається необхідністю роботи в умовах використання NAT.

ServiceObjects містить об'єкти для кожного типу послуг, забезпечуваних конкретною моделлю CPE. Відповідно, для мультисервісних CPE визначається кілька об'єктів відповідного типу. Для основних типів послуг параметри формалізовані й оформлені у вигляді відповідних рекомендацій BroadBand Forum.

Для спрощення операцій масового управління CPE, відповідно до TR-069, для ACS визначається поняття профілю. Під профілем розуміється набір вимог, яким повинні задовольняти значення параметрів одного або декількох CPE. Параметри конфігурації сервісу, його підключення або відключення можуть бути зібрані в єдиний профіль. Кожний CPE може мати більше одного профілю – залежно від кількості й типу надаваних абонентові сервісів. Звичайно для кожного типу CPE виділяється один базовий профіль, що визначає основні параметри його роботи, а також трохи додаткових, отриманих на основі базового й специфічні для типів, що включають у себе, сервісів параметри.

CommonObjects містить параметри, які визначають тип CPE. Параметри вітки CommonObject використовуються для ідентифікації CPE на ACS і містять у собі:

- DeviceInfo.
- ManagementServer.
- GatewayInfo.
- Time.
- Config.
- UserInterface.
- LAN.

Завершуючи короткий огляд параметрів, необхідно відзначити, що CWMP не регулює число параметрів, підтримуваних конкретною реалізацією CPE. Кожний виробник може додати свої, специфічні параметри, що щонайкраще реалізують функції управління конкретним типом і моделлю устаткування. Протокол CWMP у свою чергу визначає лише набір основних параметрів, що дозволяють реалізувати функції уніфікованого управління гетерогенною мережею оператора.

Розробка структурної схеми

Домашні мережі стають усе більше масштабними й складними. Вони зв'язують різноманітні взаємодіючі між собою пристрою: ігрові консолі, телеприставки, телефони VoIP і ПК. Зважаючи на те, що щодня в системі безпеки виявляється безліч уразливостей, наявність яких може вплинути на потоки переданого в домашній мережі трафіку, цими пристроями необхідно управляти, щоб забезпечити належна якість сервісу й підвищити надійність мережі. Це завдання спрощується за рахунок надання за допомогою TR-069 єдиної платформи для ефективного управління всіма мережними пристроями.

Зростаюче сімейство розширюваних і керованих модульних «моделей даних» TR-069 визначає широкий спектр функцій пристроїв і програмних модулів. Ці моделі, по-перше, указують, що пристрій ставиться до категорії підключених і повинне розпізнаватися мережею, а по-друге, надають відомості про тип пристрою – VoIP, телеприставка, шлюз або фемтостільникова точка доступу.

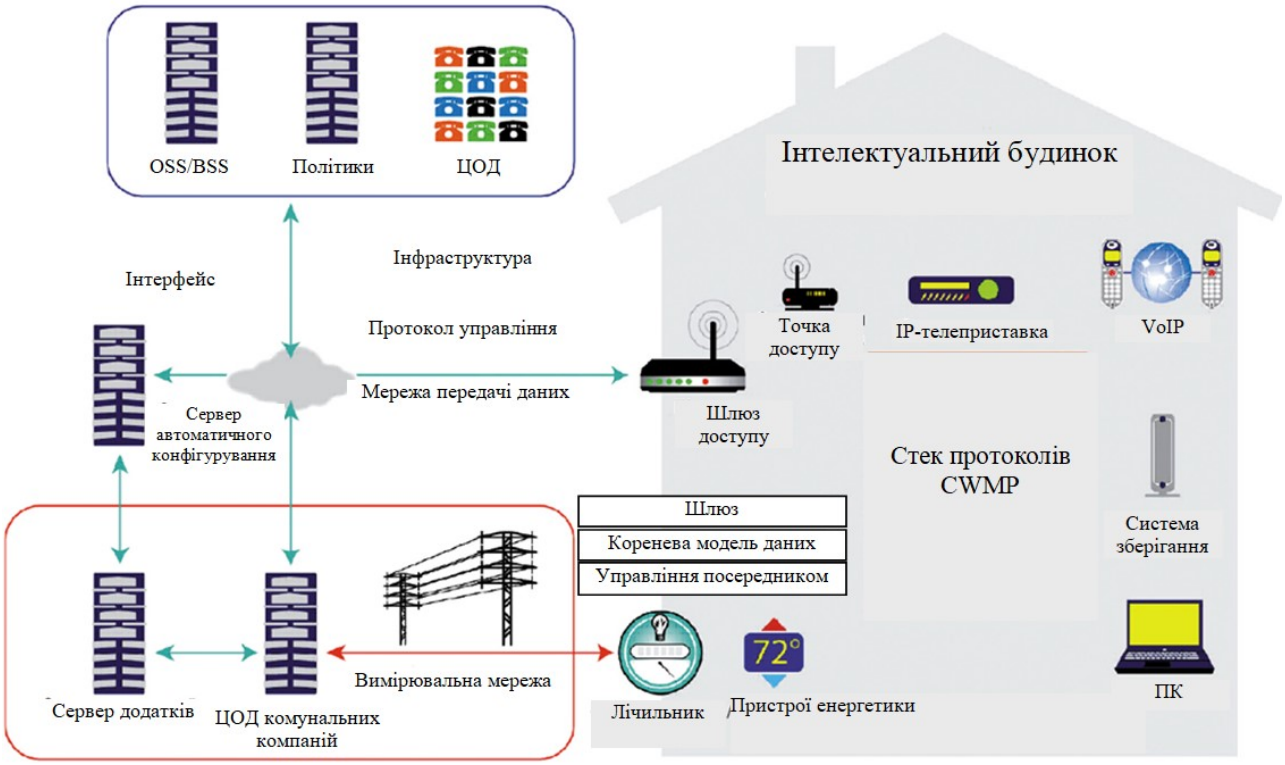

Рисунок 1 – Структурна схема системи

Своя модель даних передбачена й для управління посередниками – завдяки їй, мережа може підтримувати такі об'єкти, як лічильники електроенергії, пристрої для забезпечення безпеки й домашнього моніторингу. Список пристроїв продовжує поповнюватися, і TR-069 регулярно обновляється для підтримки всі нових їхніх типів. Його ефективність не залежить від локального методу доступу (DSL, кабельна, бездротова мережа й т.д.), він може працювати з будь-якими з'єднаннями й протоколами в домашній мережі (G.hn, HomePlug, OAM, і ін.). Виводячи на ринок новий мережний пристрій, потрібно навчити його «розмовляти» на одній мові з мережею, щоб остання могла ідентифікувати новий пристрій, що підключається, підтвердити його тип і забезпечити швидкість і стабільність роботи, необхідні для виконуваних на ньому додатків. Відповідність пристрою стандарту TR-069 і вимогам моделі даних гарантує ефективне виділення ресурсів і одержання замовником підтримуваних можливостей. Мова йде не тільки про управління шлюзом широкополосного доступу, але й про забезпечення взаємодії з іншими пристроями, такими як телеприставки, IP-телефони й мережні системи зберігання (NAS). Важливі переваги одержують і провайдери: вони можуть віддалено набудовувати конфігурацію, управляти різними новими пристроями, що підключаються, і здійснювати діагностику. А для клієнтів це означає, що вони не будуть зіштовхуватися з якими-небудь проблемами при виділенні ресурсів, усуненні несправностей і модернізації устаткування. Одержання клієнтським устаткуванням (CPE) сертифікації Broadband Forum BBF.069 ясно й недвозначно говорить про те, що галузь підтверджує його готовність до виходу на ринок. Тепер постачальники устаткування й систем зможуть знизити витрати на тестування, спростити просування продуктів і скористатися новими можливостями, що дозволяють значно розширити охват ринку.

Дана програма націлена на рішення наступних завдань:

- перевірка відповідності пристроїв протоколу TR-069 і їхньої готовності до виходу на ринок;
- спрощення інтеграції домашніх мережних систем і устаткування з мережами провайдерів;
- поліпшення керованості пристроїв, підвищення їхньої економічності й простоти управління для провайдерів, яким доводиться мати справа з більшим числом пристроїв, що підключаються до мережі.

Програма сертифікації Broadband Forum дає істотні вигоди всім учасникам ланцюжка поставок. Введення сертифікації по TR-069 полегшує операторам і сервісам-провайдерам прийняття інвестиційних рішень. Ця програма гарантує сумісність із мережею і якість, а оператори й сервіспровайдери можуть бути впевнені в тому, що сертифіковані пристрої CPE будуть краще взаємодіяти з їхніми системами віддаленого управління й конфігурування (ACS). Виконаний ABI Research аналіз дозволяє припустити, що до 2016 року обсяг поставок базового устаткування для домашніх мереж (шлюзів/маршрутизаторів, мостів, мережних плат (NIC), що вбудовуються мережних адаптерів (LAN) і мережних систем зберігання (NAS)), а мультимедійних пристроїв, що підключаються також до мережі, (клієнтських пристроїв з мережними інтерфейсами, включаючи комп'ютери й мобільні пристрої) перевищить мільярд одиниць. По оцінках IHS iSuppli, в 2014 році в усьому світі число проданих шлюзів і тонких клієнтів досягло 4,2 млн штук, у той час як роком раніше цей показник становив 345 тис. Згідно із прогнозами, у наступні два роки обсяг продажів буде стрімко збільшуватися – до 6,7 млн штук в 2015 році, до 10,4 млн штук в 2023-м і до 12,6 млн штук до 2024 року. Виробники побутової електроніки, клієнтського устаткування, «розумних» лічильників і пристроїв можуть продавати більше продуктів, якщо вони сертифіковані на відповідність TR-069, оскільки це гарантує, що устаткування легко інтегрується в домашню мережу і їм можна ефективно управляти віддалено.

Контент-провайдери одержують аналогічну можливість для збільшення продажів – споживання «мультиекраного» контенту (для екранів різного типу) росте з розвитком екосистеми пристроїв.

Сервіси-провайдери можуть продавати більше керованих пристроїв і послуг, дістаючи прибуток не тільки від базового сервісу широкополосного доступу. А завдяки забезпечуваному TR-069 віддаленому управлінню знижуються витрати на підтримку мережі й устаткування, підвищується лояльність клієнтів. Комунальні компанії можуть розширити спектр своїх послуг, запропонувавши на основі TR-069 функції управління будинком і моніторингу. Тим часом, завдяки різним ініціативам, використання стандарту TR-069 для побудови в будинках мереж «розумних» лічильників поліпшить управління енергоресурсами й потенційно знизить, що виставляються в рахунках суми. Таким чином, TR-069 надає провайдерам можливості моніторингу, управління й контролю за зростаючим числом усе більше складних підключених пристроїв, терміналів і устаткування. Він дозволяє сервіспровайдерам підтримувати високий рівень якості, пропонувати привабливі для користувачів можливості, надає їм інструменти для поліпшення обслуговування клієнтів і створює передумови для успішної комерціалізації мультиекраних систем і комбінованих послуг.

За останні роки Україна стала одним із ринків широкополосного доступу, які швидко розвиваються, уступаючи лише Китаєві й Індії. Так, наприклад, в 2014 році його ріст склав 28,3% по числу абонентів, а широкополосний доступ охоплює приблизно 15% населення. Більшість користується DSL, але одночасно збільшується кількість підключень по оптичному волокну й через кабельні модеми. Користувачі широкополосних мереж всі частіше хочуть одержувати мультисервісні можливості й підключають до таких мереж безліч нових пристроїв. У цей час росте популярність додатків IPTV, і хоча поки в Україні ними користуються менш 2% населення, за останні чотири роки число передплатників IPTV різко збільшилося й тепер наближається до 3 млн чоловік.

Для сервісів-провайдерів, що працюють в Україні, критично важливим є впровадження світових стандартів мережної архітектури й управління, а TR-069 з різноманітними моделями даних гарантує експонентний ріст українського ринку й ефективне обслуговування населення.

З появою сертифікації Broadband Forum BBF.069 Certification стандарт TR-069 стає ключовим інструментом для подальшого розширення потенціалу й збільшення кількості підключених домашніх пристроїв в усьому світі й особливо в Україні. Сервіси-провайдери можуть внести свою лепту в цей процес, дотримуючись стандарту TR-069 у своїх платформах управління мережами й вимагаючи в запитах RFP сертифікації по BBF.069 CPE.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів платформи управління мережними пристроями інтелектуального будинку за технологією CWMP. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем платформи управління мережними пристроями інтелектуального будинку за технологією CWMP; Досліджена система платформи управління мережними пристроями інтелектуального будинку за технологією CWMP; На основі отриманих результатів досліджень створена програмна реалізація системи платформи управління мережними пристроями інтелектуального будинку за технологією CWMP. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання платформи управління мережними пристроями інтелектуального будинку за технологією CWMP. 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. 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.
2. 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.
3. 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.
4. 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.
5. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
17. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
18. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
19. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
20. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
21. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.