УДК 004.7
DOI: 10.25140/2411-5363-2020-2(20)-218-228

Володимир Базилевич, Марина Мальцева, Тарас Петренко, Леся Черниш

ЗАХИЩЕНА СИСТЕМА РОЗУМНОГО БУДИНКУ З ВИКОРИСТАННЯМ INTERNET OF THINGS

Актуальність теми дослідження. *Сьогодні Internet of Things (Інтернет речей, IoT) щільно увійшов у життя мільярдів людей по всьому світу. IoT використовується в багатьох сферах людської діяльності – промисловості, побуті, медицині, освіті, управлінні містами та ін. Однак зростання кількості підключених пристроїв веде до збільшення ризиків безпеки - від заподіяння фізичної шкоди людині за допомогою цих пристроїв до пошкодження надскладного технологічного обладнання. Саме тому питання забезпечення захисту систем IoT є актуальними.*

Постановка проблеми. *Комплексний захист систем IoT можливий лише при забезпеченні надійного мережевого, програмного та технічного захисту пристроїв, обладнання та комунікацій з яких складаються ці системи. Враховуючи те, що вищезазначені об'єкти та методи їх захисту можна об'єднати в окрему захищену систему розумного дому, її розробка є актуальною теоретичною та практичною задачею кібербезпеки.*

Аналіз досліджень і публікацій. *Сьогодні існує багато публікацій, в яких аналізуються проблеми безпеки IoT, та пропонуються шляхи їх вирішення, проте роботи, в яких була б розроблена окрема захищена система IoT на прикладі розумного будинку, відсутні.*

Виділення недосліджених частин загальної проблеми. *Аналізуючи багаторівневу архітектуру IoT-систем і особливості хмарних платформ Інтернету речей, виділяючи потенційно вразливі компоненти цих комплексних рішень (система управління доступом до IoT-пристрою і хмарної платформи;хмари, мобільні додатки та веб-інтерфейси пристроїв; оновлення програмного забезпечення; пам'ять пристроїв; локальні сховища даних; апаратні та програмні інтерфейси пристроїв; мережеві сервіси пристроїв;екосистема комунікацій, зокрема мережевий трафік) можна стверджувати що побудова захищеної системи розумного дому з використанням IoT дозволить підвищити рівень захищеності цих систем. .*

Метою статті – *побудова захищеної системи з використанням IoT на прикладі розумного будинку.*

Виклад основного матеріалу. *Визначено основні поняття IoT, досліджено основні сфери використання IoT, розроблено захищену систему розумного будинку з використанням IoT в якій використано основні способи захисту інформації що доцільно впроваджувати в мережах розумного будинку - VPN, брандмауер, ACL та паролі для надійного захисту. Проаналізовані основні вразливості IoT та шляхи їх усунення. Розглянуті різні архітектури систем IoT. Запропоновано алгоритм налагодження захищеної системи розумного будинку з використанням IoT*

Висновки відповідно до статті. *В роботі було розроблено захищену систему з використанням Internet of Things на прикладі розумного будинку. Визначено переваги та недоліки використання Інтернет речей. Досліджено, що популярність Інтернет речей зростає щосекунди, тому необхідно більше уваги приділяти їх захисту. Основними уразливостями IoT можна вважати відсутність стандартизації, шифрування трафіку, встановлення дефолтних паролів за замовчуванням. Було запропоновано схему захищеної системи розумного будинку з використанням Internet of Things побудовану в Cisco Packet Tracer та покроковий алгоритм налагодження системи її захисту з використанням фаєрволу ASA5505 для фільтрації вхідного трафіку. Було створено складні паролі для облікових записів пристроїв IoT. Протоколи бездротової передачі WPA2/3-PSK з використанням алгоритму AES забезпечує безпеку бездротової передачі даних. На домашньому контролері встановлено унікальний SSID. Створену систему можна впроваджувати та безпечно використовувати в будинках та офісах.*

Ключові слова: *IoT; мережа; розумний будинок; VPN; WPA2-PSK; ASA5505; ACL.*
Рис.: 10. Табл.: 1. Бібл.: 12.

Актуальність теми дослідження. Сьогодні Internet of Things (Інтернет речей, IoT) щільно увійшов в життя мільярдів людей по всьому світу. IoT використовується в багатьох сферах людської діяльності – промисловості, побуті, медицині, освіті, управлінні містами та ін. Однак зростання кількості підключених пристроїв веде до збільшення ризиків безпеки – від заподіяння фізичної шкоди людині за допомогою цих пристроїв до пошкодження надскладного технологічного обладнання. Саме тому питання забезпечення захисту систем IoT є актуальними.

Постановка проблеми. Комплексний захист систем IoT можливий лише при забезпеченні надійного мережевого, програмного та технічного захисту пристроїв, обладнання та комунікацій з яких складаються ці системи. Враховуючи те, що вищезазначені об'єкти та методи їх захисту можна об'єднати в окрему захищену систему розумного дому, її розробка є актуальною теоретичною та практичною задачею кібербезпеки.

Аналіз досліджень і публікацій. Сьогодні існує багато публікацій, в яких аналізуються проблеми безпеки IoT та пропонуються шляхи їх вирішення, проте робіт, в яких була б розроблена окрема модель захисту IoT на прикладі розумного будинку, немає.

Виділення недосліджених частин загальної проблеми. Аналізуючи багаторівневу архітектуру IoT-систем і особливості хмарних платформ Інтернету речей, виділяючи потенційно вразливі компоненти цих комплексних рішень (система управління доступом до IoT-пристрою і хмарної платформи;хмари, мобільні додатки та вебінтерфейси пристроїв; оновлення програмного забезпечення; пам'ять пристроїв; локальні сховища даних; апаратні та програмні інтерфейси пристроїв; мережеві сервіси пристроїв;екосистема комунікацій, зокрнма мережевий трафік) можна стверджувати що побудова захищеної системи розумного дому з використанням IoT дозволить підвищити рівень захищеності цих систем.

Метою статті є побудова захищеної системи з використанням IoT на прикладі розумного будинку.

Виклад основного матеріалу. Сьогодні до IoT належить понад десять мільярдів пристроїв, що мають підключення до Інтернету. Вони можуть збирати дані та взаємодіяти один з одним, передаючи дані. Завдяки появі дешевих рішень IoT і поширенню бездротових мереж можна перетворити що-небудь від дуже маленького, такого як таблетки, до дуже великого, такого як літак, у частину IoT. IoT складається з розумних приладів із доступом до Інтернету, що використовують вбудовані системи, такі як процесори, датчики та комунікаційне обладнання, щоб збирати, надсилати та діяти на основі даних, які вони отримують зі свого середовища. Пристрої IoT взаємодіють з іншими та можуть ділитися даними, що вони збирають, підключившись до шлюзу IoT або іншого кінцевого пристрою, в якому дані надсилаються в хмару для аналізу. Іноді пристрої можуть бути з'єднанні один з одним, взаємодіяти та на основі отриманих результатів виконувати певні, запрограмовані дії. Здебільшого «розумні речі» працюють без втручання людини, проте в разі потреби, можлива їх взаємодія. Як приклад, людина може налаштувати їх, дати їм інструкції або отримати доступ до даних.

У зв'язку з багаторівневою архітектурою IoT-систем і особливостями хмарних платформ Інтернету речей на базі технологій Big Data, можна виділити наступні потенційно вразливі компоненти цих комплексних рішень:

- система управління доступом до IoT-пристрою і хмарної платформі;
- хмари, мобільні додатків та веб-інтерфейси пристроїв;
- оновлення програмного забезпечення;
- пам'ять пристроїв;
- встановлення програмного забезпечення від вендора;
- локальні сховища даних;
- апаратні та програмні інтерфейси пристроїв;
- мережеві сервіси пристроїв;
- екосистема комунікацій, зокрема мережевий трафік [1].

Вперше термін «Інтернет речей» вжив Кевін Ештон у 1999 році, піонер британських технологій. За словами Ештона IoT є системою фізичних об'єктів у світі, підключених до Інтернету за допомогою датчика [2]. Найпростіше визначення – Інтернет речей – це мережа фізичних пристроїв, які поєднують у собі IP-зв'язок із програмним забезпеченням, датчиками, виконуючими механізмами та іншою електронікою, щоб безпосередньо інтегрувати фізичний світ у наші комп'ютерні системи, що призводить до підвищення ефективності та економічної вигоди [2].

Протоколи підключення, мережевих зв'язків та комунікацій, що використовуються з цими веб-пристроями, значною мірою залежать від конкретних застосованих програм IoT. IoT також може використовувати штучний інтелект (AI) та машинне навчання для полегшення та динаміки процесів збору даних.

Майже будь-який фізичний пристрій можна перетворити на Інтернет речей, якщо має підключення до Інтернету для контролю та передачі інформації.

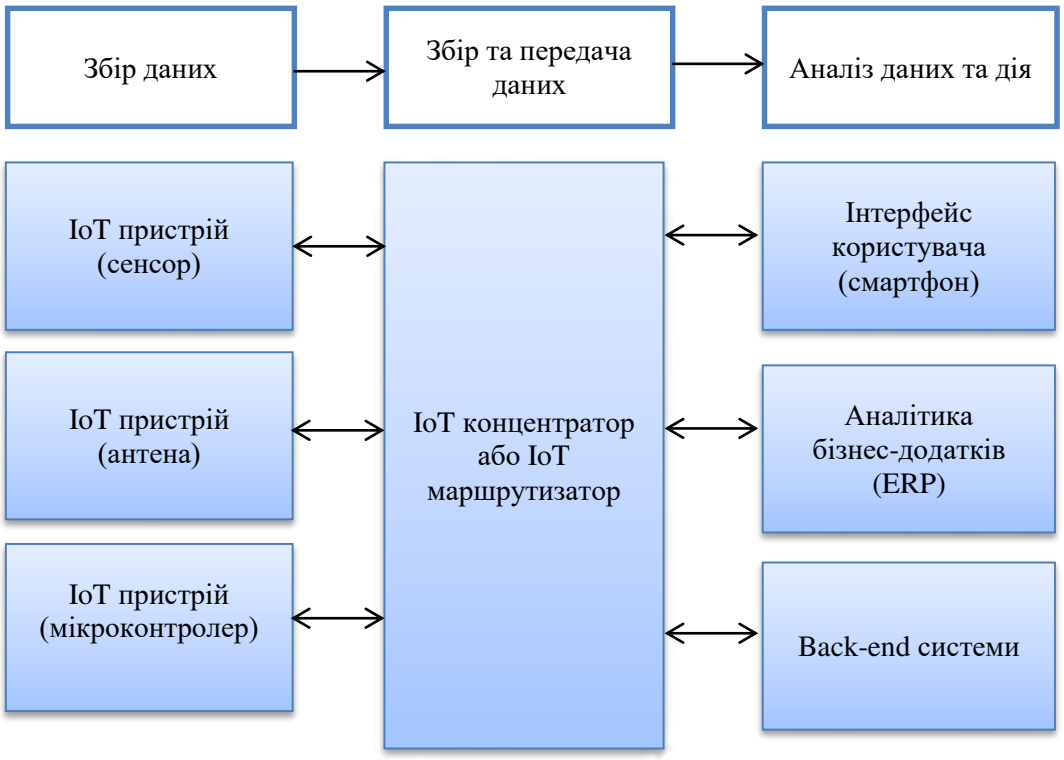

Рис. 1. Приклад IoT системи

Джерело: [3].

Експерти почали називати IoT промисловою революцією 4.0. Звіти статистики IoT показують, як технологічні інновації матимуть вирішальну роль в організації економіки, охорони здоров'я, маркетингу, банківської справи та фінансів, а також уряду. IoT збирається розпочати високий ступінь автоматизації, налаштування та підключення.

Ось деякі факти щодо статистики IoT:

- 127 нових пристроїв IoT підключаються до Інтернету щосекунди;
- побутова електроніка становить 63 % усіх встановлених блоків IoT;
- до кінця 2020 року кількість пристроїв IoT в будинках зросте майже до 13 млрд;
- 23 % поточних масштабних проектів IoT – це розумні міста;
- 40 % пристроїв IoT використовуються в галузі охорони здоров'я;
- глобальні витрати на IoT становитимуть 15 трильйонів доларів за шість років між 2019 та 2025 роками;
- кількість активних пристроїв IoT в 2020 році перевищить 30 млрд [4].

Не існує загальної єдності в поглядах на архітектуру IoT, з якою б погодилися всі науковці. На думку деяких дослідників, архітектура IoT має три шари, але деякі дослідники підтримують чотиришарову архітектуру. Вони вважають, що завдяки удосконаленню, IoT архітектура трьох шарів не може відповідати вимогам додатків. Через проблеми в IoT щодо безпеки та конфіденційності також була запропонована архітектура п'яти шарів. Вважається, що нещодавно запропонована архітектура може відповідати вимогам IoT щодо безпеки та конфіденційності. Ієрархія всієї запропонованої шаруватої архітектури Internet of Things (IoT) показана на рис. 2, де показані шарові архітектури IoT, що складаються відповідно з трьох, чотирьох та п'яти рівнів.

Рис. 2. Ієрархія архітектур IoT

Джерело: [5].

Трирівнева архітектура – це базова архітектура й відповідає основній концепції IoT. Вона була запропонована на ранніх стадіях розвитку IoT. І має три рівні (сприйняття, мережевий та прикладний), як показано на рис. 3.

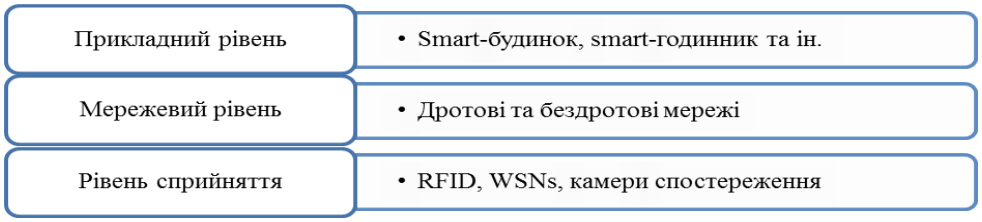

Рис. 3. Трирівнева архітектура IoT

Джерело: [5].

Чотирьохрівнева архітектура. Тришарова архітектура була базовою архітектурою. Через постійний розвиток в IoT, вона не могла виконати всіх вимог до IoT. Тому дослідники представили архітектуру з чотирма рівнями. Вона має три рівня, як попередня архітектура, та ще один рівень, який називається рівнем підтримки. На рис. 4 представлені рівні цієї архітектури з механізмами безпеки, що використовуються для забезпечення захисту від зловмисників.

П’ятирівнева архітектура. Чотирьохрівнева архітектура відіграла важливу роль у розвитку IoT. Були також деякі проблемні питання щодо безпеки та зберігання даних в чотирьохрівневій архітектурі. Внаслідок чого дослідники запропонували п’ятишарову архітектуру, щоб зробити IoT більш надійним. Вона має три основні рівні (рівень сприйняття, транспортний та прикладний), бізнес-рівень та рівень обробки. Вважається, що запропонована архітектура має можливість максимально виконувати вимоги IoT. Вона також має можливість захищати програми IoT [5].

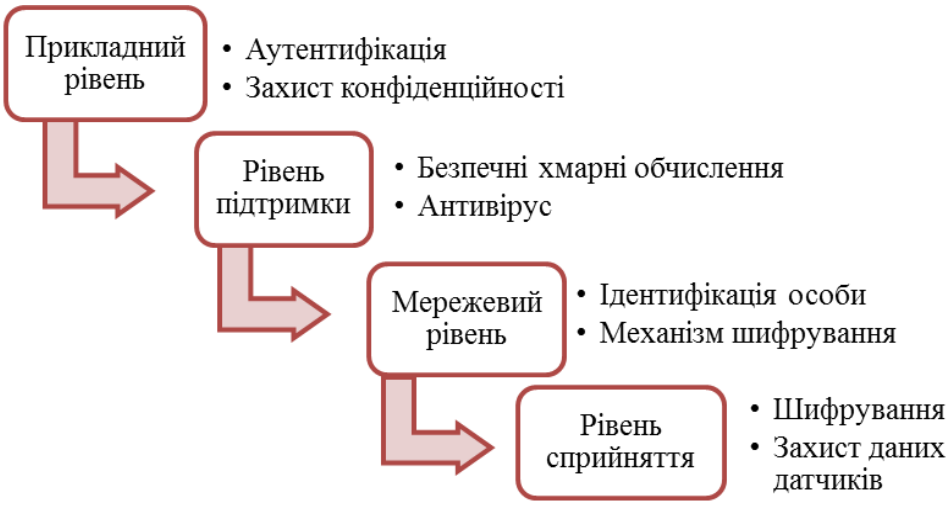

Рис. 4. Чотирьохрівнева архітектура IoT

Джерело: [5].

Інтернет речей переймає сучасні технології і застосовується в різних галузях. Нині ми маємо змогу збирати, обробляти та надсилати дані до інших об'єктів, додатків чи серверів. Протоколи IoT дозволяють цим об'єктам спілкуватися та обмінюватися даними. Протоколи IoT можна класифікувати на дві категорії: мережеві та протоколи даних (рис. 5). Мережеві протоколи використовуються для підключення різних пристроїв, що використовуються в мережі, і зазвичай використовуються Інтернет. З іншого боку, протоколи даних використовуються для підключення IoT низької потужності та підключаються без використання Інтернету.

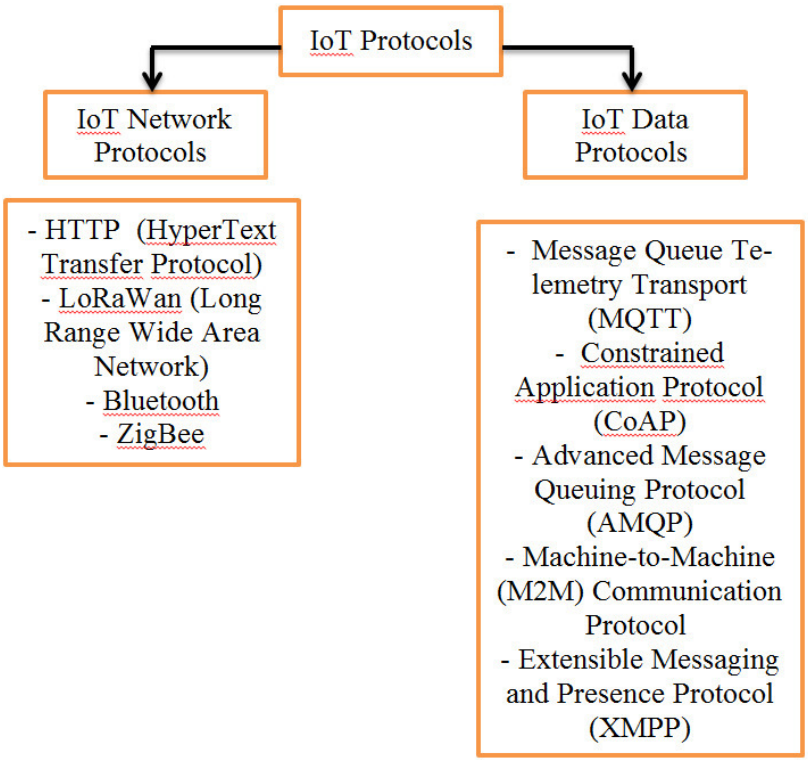

Рис. 5. Протоколи IoT

Найслабшим місцем IoT є безпека. Нажаль майже всі пристрої мають багато уразливостей, що дозволяє хакерам легко їх зламувати. У таблиці наведені найбільші уразливості IoT та шляхи їх усунення [6].

Таблиця

Найбільші уразливості IoT та шляхи їх усунення

Уразливість	**Шляхи подолання**
Недостатня (або відсутня) стандартизація архітектури і протоколів, сертифікація пристроїв	Створення єдиного міжнародного стандарту з єдиним переліком вимог до Інтернет речей
Відсутність шифрування бездротового трафіку	Використання протоколів шифрування WPA2/WPA3-PSK з алгоритмом шифрування AES
Робоче використання типових облікових записів, встановлених виробником за замовчуванням	Можливість створення облікових записів для кожної Інтернет речей та створення виробником різних „Нетипових" паролів за замовчуванням для кожного пристрою
Слабка аутентифікація і системи управління доступом	Створення складного пароля та логіну для кожного облікового запису Інтернет речей
Відсутність підтримки з боку виробника для усунення вразливостей	Використання виробником стандарту безпеки Інтернет речей, створення різних паролів для пристроїв за замовчуванням, наявність технічної підтримки
Складність або неможливість установки оновлень операційної системи	Наявність веб-інтерфейсу домашнього контролера та можливість конфігурування кожної Інтернет речей та наявність можливості встановлення оновлення операційної системи
Використання незахищених мобільних технологій і хмарної інфраструктури	Використання незахищених мобільних технологій і хмарної інфраструктури
взаємна інтеграція різних пристроїв між собою дозволяє зловмисникові оволодіти всією мережею, зламавши лише 1 річ	Шифрування трафіку, що передається від одного пристрою до іншого. Облікові записи для пристроїв.
Відсутність брандмауерів і антивірусів	Використання фаерволів з налаштованими списками доступу для захисту вхідного трафіку та антивірусного програмного забезпечення для внутрішнього захисту
Використання небезпечного ПЗ	Використання ліцензійного програмного забезпечення надійного виробника

Для розробки захищеної системи розумного будинку з використанням IoT була використана багатофункціональна програма моделювання мереж Cisco Packet Tracer. Далі наводимо алгоритм побудови та налагодження захищеної системи розумного будинку з використанням IoT:

1. Побудова мережі, додавання всіх необхідних мережевих та кінцевих пристроїв. (смартфон - девайс з якого буде відбуватися керування та спостереження за Інтернет речей, wireless router - який в свою чергу підключений до Інтернет, далі йде хмара (як імітація Інтернету), до якої було підключено маршрутизатор іншого провайдера(R2). Нижче ISP маршрутизатора був розміщений комутатор та два сервери (DNS–сервер, який містить базу даних загальнодоступних IP-адрес та пов'язаних з ними імен хостів і в більшості випадків служить для вирішення або перекладу цих імен на IP-адреси за потребою та IoT Server – сервер Інтернет речей). До R2 підключено домашній контроллер, який є точкою з'єднання всіх Інтернет речей. Смартфон підключено до точки доступу бездротово, в свою чергу, остання було підключено кросоверним кабелем. ISP1 та ISP2 – за допомогою Serial кабеля. Сервери та домашній контроллер – прямим кабелем (рис. 6).

2. Налаштування мережі. Проведено налаштування домашнього шлюзу. Для початку було змінено дефолтний SSID (ідентифікатор, являє собою унікальний 32-значний буквено-цифровий код, який використовується для ідентифікації WLAN. Необхідний для запобігання випадкового або навмисного підключення до мережі іншого бездротового обладнання). Далі підключили вебкамеру до шлюзу. Для цього перейшли до налаштувань об'єкта та вибрали мережевий адаптер PT-IOE-MN-W та вказали SSID, який налаштували шлюзі.

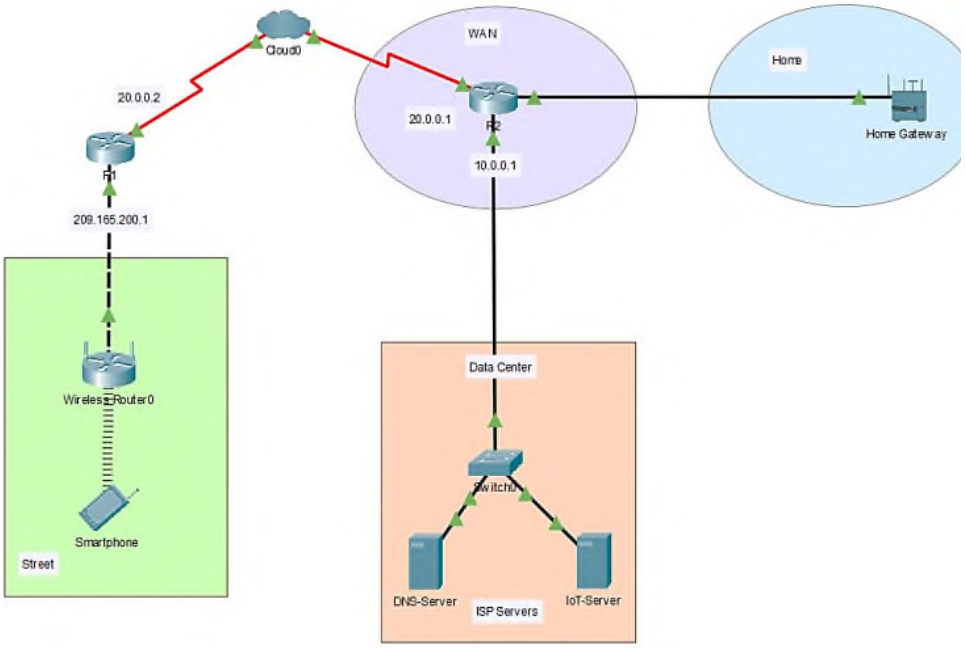

Рис. 6. Побудова мережі

3. Налаштування маршрутизатора R2, налаштування ip-адрес на інтерфейси та налаштування його як dhcp-сервер.

4. Налаштування хмари. Для кожного Serial інтерфейсу задали унікальний DLCI. S0/0 -100 (A), S1/0 (B). На вкладниці frame relay (це ретрансляція кадрів (frame relay, FR) – це метод доставки повідомлень у мережах передачі даних із комутацією пакетів) налаштували таким чином S1 (B) – S0 (A).

5. Налаштування DNS та IoT серверів. Для цього перевірили чи роздав R2 ip-адресу та вкладниці Services — DNS натиснули on. Також додали запис про IoT та DNS сервер. Name — www.iot.com, ip — 10.0.0.253 . Name — www.dns.com, ip — 10.0.0.2533

6. Для захисту моделі розумного дому спочатку було змінено стандартний SSID на домашньому контролері та обрано тип аутентифікації WPA2-PSK (рис. 7).

7. На IoT – сервері було створено обліковий запис зі складним паролем та логіном для підключення розумних речей. Нажаль, програма packet tracer не підтримує можливості створення окремих облікових записів для кожної розумної речі, проте це потрібно зробити обов’язково.

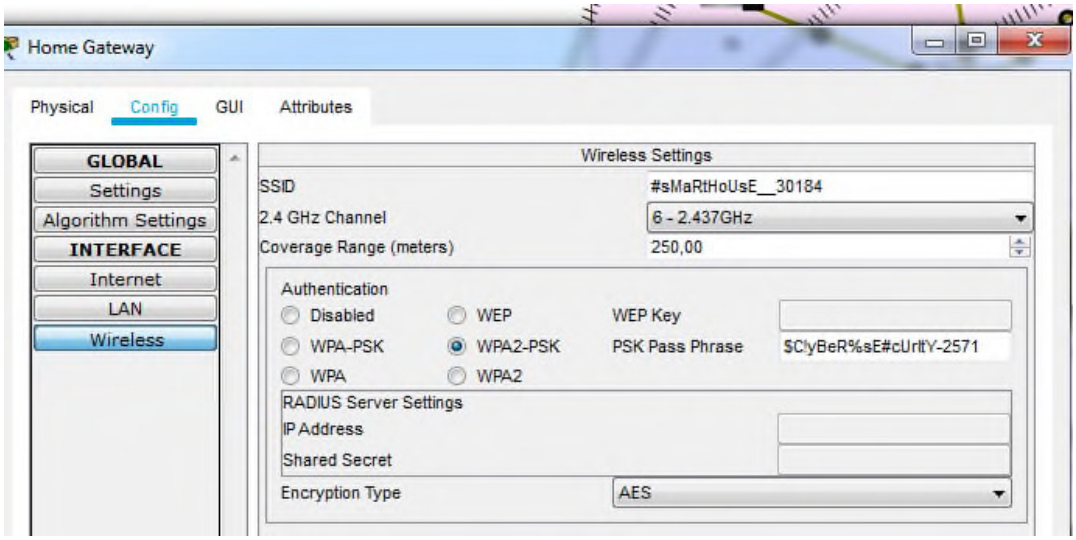

Рис. 7. Налаштування основних параметрів безпеки на домашньому контролері

8. Одним із найкращих способів захистити розумний дім є використання фаерволу. Для роботи було використано файєрвол Cisco ASA 5505. Серія Cisco ASA 5500 – це продовження брандмауера Cisco PIX 500 серії Cisco. Однак ASA - це не просто чистий апаратний брандмауер. Cisco ASA – це захисний пристрій, який поєднує в собі брандмауер, антивірус, запобігання вторгнень та віртуальну приватну мережу (VPN). Він забезпечує активну захист від загрози, яка зупиняє атаки, перш ніж вони поширюються по мережі. Тому брандмауер Cisco ASA – це весь пакет, так би мовити. Він поєднує:

- антивіруса;
- антиспам;
- IDS / IPS систему;
- VPN-пристрій;
- SSL пристрій;
- перевірка вмісту [7].

9. Налаштування основних параметрів брандмауеру. Спершу встановлено пароль на привілейований режим роботи. Потім налаштовано WLAN-и, а саме, надання їм ip-адрес, імен та рівенів захищеності. Внутрішній WLAN завжди має мати найвищий рівень. Налаштовано dhcp на внутрішній порт. Також була прописана маршрутизація для працездатності мережі. Щоб була можливість виходити в Інтернет, необхідно перетворити локальні ip-адреси на глобальні. Для цього налаштували nat.

Далі було створено списки доступу, в яких вказано, які мережі або хости матимуть доступ до внутрішньої мережі (рис. 8).

```
route outside 0.0.0.0 0.0.0.0 209.165.200.1 1
!
access-list FROM-VPN extended permit tcp 192.168.2.0 255.255.255.0 host 10.0.0.253
access-list FROM-VPN extended permit tcp 192.168.2.0 255.255.255.0 host 10.0.0.253 eq www
access-list FROM-VPN extended permit tcp 192.168.2.0 255.255.255.0 host 10.0.0.254 eq domain
access-list FROM-VPN extended permit tcp 192.168.2.0 255.255.255.0 host 10.0.0.254 eq www
access-list FOR-VPN extended permit tcp host 10.0.0.254 192.168.2.0 255.255.255.0 eq domain
access-list FOR-VPN extended permit tcp host 10.0.0.254 192.168.2.0 255.255.255.0 eq www
access-list FOR-VPN extended permit tcp host 10.0.0.253 192.168.2.0 255.255.255.0 eq www
access-list FOR-VPN extended permit tcp host 10.0.0.253 192.168.2.0 255.255.255.0
!
```

Рис. 8. Налаштування списків доступу

Наступним кроком захисту мережі було створення VPN-tunnel між фаерволами. Для цього налаштували першу фазу, а саме, на зовнішньому інтерфейсі увімкнули протокол ike командою crypto ikev1 enable outside.

Далі створили політику crypto ikev1 policy 1, де вказали алгоритм шифрування 3des (це параметри для побудови міні тунелю ISAKMP-тунелю, через який будуть передаватися параметри основного Ipsec-тунелю): encryption 3des алгоритм хешування md5: «hash md5», тип аунтентифікакції Pre-Shared Key: «authentication pre-share» та алгоритм Діффи — Хеллмана: «group 2», «exit».

Наступним кроком було налаштування ключа автентифікації та адреси піра, тобто зовнішньої ip-адреси між мережевого екрану з яким буде побудовано VPN за допомогою команди: tunnel-group 210.210.2.2 type ipsec-l2l. Задамо атрибути ipsec: tunnel-group 210.210.2.2 ipsec-attributes, ikev1 pre-shared-key cisco, exit.

Далі вказали параметри для побудови ipsec-тунелю з ім'ям TS і вказали алгоритм хешування: crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac. Створити списки доступу з ім'ям FOR-VPN, тобто визначили, який трафік буде направлено в VPN-тунель: access-list FOR-VPN extended permit icmp 192.168.2.0 255.255.255.0 10.0.0.0 255.255.255.0. Створили крипто карту з ім'ям TO-SITE2 під номером: crypto map TO-SITE2 1 match address FOR-VPN, де вказали пір, тобто зовнішню ip-адресу між мережевого екрану: crypto map TO-SITE2 1 set peer 210.210.2.2, та вказали lifetime тунелю в секундах: crypto map TO-SITE2 1 set security-association lifetime seconds 86400.

Після цього прив'язали transform-set TS: crypto map TO-SITE2 1 set ikev1 transform-set TS. Також прив'язали цю крипто карту до зовнішнього інтерфейсу: crypto map TO-SITE2 interface outside, end, wr mem.

Аналогічні команди прописали на іншому фаерволі.

Після налаштувань необхідно переконатися, що тунель побудований, для цього зайшли на ASA та подивилися, чи будується тунель: show crypto isakmp sa (рис. 9).

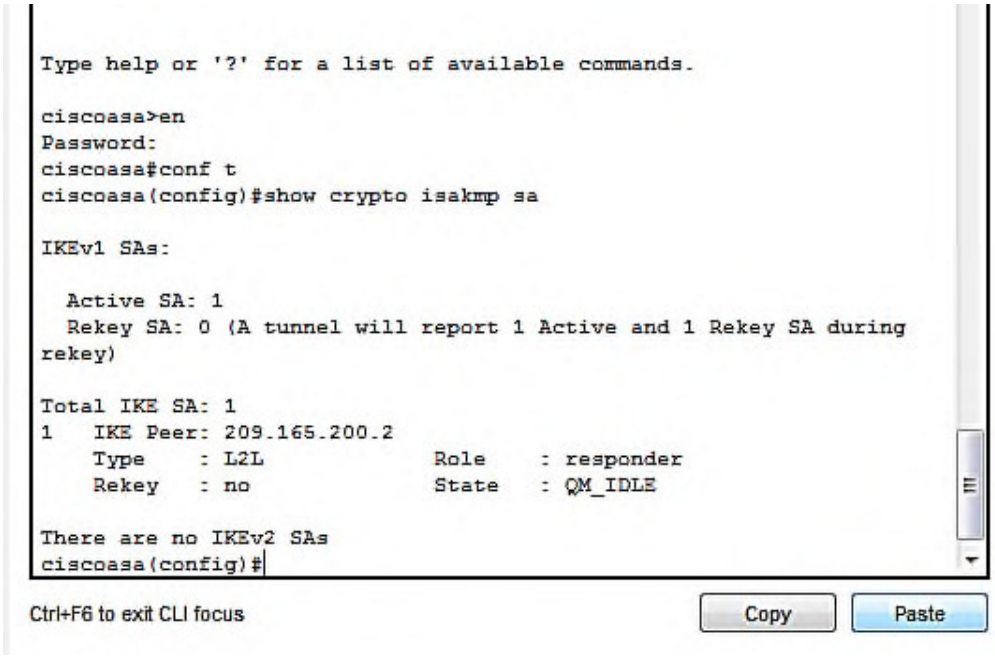

Рис. 9. Перевірка побудови тунелю

Переконавшись, що тунель побудований та далі перевіривши ipsec за допомогою команди show crypto ipsec sa, впевнились, що тунель побудований та при цьому ASA шифрує всі пакети, але вхідні пакети не розшифровує. На цьому налаштування фаерволу ASA5505 та системи захисту в цілому можна вважати закінченим.

В процесі розробки захищеної системи розумного будинку з використанням IoT нами була розроблена схема цієї системи, що складається з датчиків, пристроїв керування, мережевої частини та пристроїв захисту. Зазначена схема наведена на рис. 10.

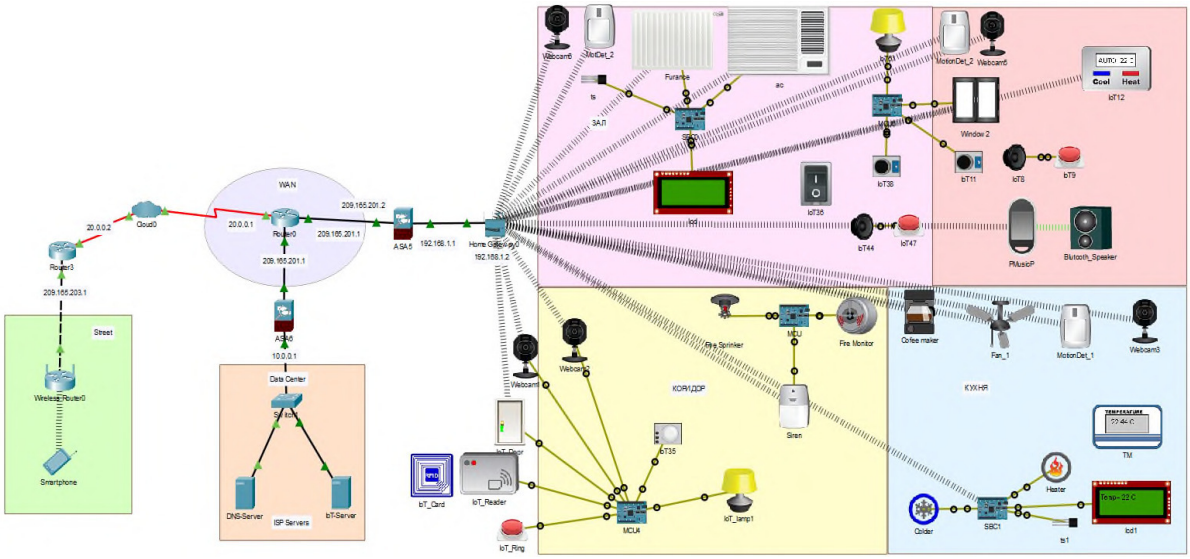

Рис. 10. Загальна схема технічного захисту розумного будинку

Висновки відповідноь до статті. У роботі було розроблено захищену систему з використанням Internet of Things на прикладі розумного будинку. Визначено переваги та недоліки використання Інтернет речей. Досліджено, що популярність Інтернет речей зростає щосекунди, тому необхідно більше уваги приділяти їх захисту. Основними уразливостями IoT можна вважати відсутність стандартизації, шифрування трафіку, встановлення дефолтних паролів за замовчуванням.

Було запропоновано схему захищеної системи розумного будинку з використанням Internet of Things побудовану в Cisco Packet Tracer та покроковий алгоритм налагодження системи її захисту з використанням фаерволу ASA5505 для фільтрації вхідного трафіку. Було створено складні паролі для облікових записів пристроїв IoT. Протоколи бездротової передачі WPA2/3-PSK з використанням алгоритму AES забезпечує безпеку бездротової передачі даних. На домашньому контролері встановлено унікальний SSID. Створену систему можна впроваджувати та безпечно використовувати в будинках та офісах.

Список використаних джерел

1. Coetzee and J. Eksteen. The Internet of Things-promise for the future? An introduction. *IST-Africa Conference Proceesing*, 2011. P. 1-9.

2. What is Internet of Things (IOT)? URL: https://www.informopedia.com/have-you-heard-the-word-internet-of-things-iot-lets-explore.

3. Internet of things (IoT). URL: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT#.

4. В мире подсчитано количество IoT-устройств. URL: http://www.dailycomm.ru/m/47373.

5. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6165453.

6. Internet of Things: information security challenges and solutions. URL: https://www.researchgate.net/publication/326559393_Internet_of_Things_information_security_challenges_and_solutions.

7. Cisco ASA Series CLI Configuration. URL: https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/interface_start_5505.html.

References

1. Coetzee and J. Eksteen (2011). The Internet of Things-promise for the future? An introduction. *IST-Africa Conference Proceesing* (pp. 1-9).

2. What is Internet of Things (IOT)? Retrieved from https://www.informopedia.com/have-you-heard-the-word-internet-of-things-iot-lets-explore.

3. Internet of things (IoT) Retrieved from https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT#.

4. The number of IoT devices is counted in the world Retrieved from http://www.dailycomm.ru/m/47373.

5. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6165453.

6. Internet of Things: information security challenges and solutions Retrieved from https://www.researchgate.net/publication/326559393_Internet_of_Things_information_security_challenges_and_solutions.

7. Cisco ASA Series CLI Configuration Retrieved from https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/interface_start_5505.html.

UDC 004.7

Volodymyr Bazylevych, Marina Maltseva, Taras Petrenko, Lesia Chernysh

PROTECTED INTELLIGENT HOUSE SYSTEM USING INTERNET OF THINGS

Urgency of the research. *Today, the Internet of Things (IoT) is firmly entrenched in the lives of billions of people around the world. IoT is used in many areas of human activity - industry, everyday life, medicine, education, urban management and others. However, the increase in the number of connected devices leads to an increase in safety risks - from causing physical harm to humans with these devices to damage to complex technological equipment. That is why the issues of ensuring the protection of IoT systems are relevant.*

Target setting. *Comprehensive protection of IoT systems is possible only with reliable network, software and technical protection of devices, equipment and communications of which these systems consist. Given that the above objects and methods of their protection can be combined into a separate secure system of a smart home, its development is an important theoretical and practical task of cybersecurity.*

Actual scientific researches and issues analysis. *Today, there are many publications that analyze IoT security issues and suggest ways to solve them, but there is no work that would develop a separate model of IoT protection on the example of a smart home.*

Uninvestigated parts of general matters defining. *Analyzing the multilevel architecture of IoT systems and features of cloud platforms of the Internet of Things, highlighting potentially vulnerable components of these complex solutions (access control system to IoT device and cloud platform; clouds, mobile applications and web interfaces of devices; software updates; device memory ; local data warehouses; hardware and software interfaces of devices; network services of devices; ecosystem of communications, including network traffic) it can be argued that building a secure system of a smart home using IoT will increase the level of security of these systems. .*

The research objective *of this article is to build a secure system using IoT on the example of a smart home.*

The statement of basic materials. *The basic concepts of IoT are defined, the main spheres of IoT use are investigated, the secure system of smart house with use of IoT in which the basic ways of protection of the information which is expedient to implement in networks of smart house - VPN, firewall, ACL and passwords for reliable protection is developed. The main IoT vulnerabilities and ways to eliminate them are analyzed. Different architectures of IoT systems are considered. An algorithm for setting up a secure smart home system using IoT is proposed*

Conclusions. *The work developed a secure system using the Internet of Things on the example of a smart home. The advantages and disadvantages of using the Internet of Things are identified. It has been studied that the popularity of the Internet of Things is growing every second, so it is necessary to pay more attention to their protection. The main vulnerabilities of IoT can be considered the lack of standardization, traffic encryption, default passwords. The scheme of a secure system of a smart home using the Internet of Things built in Cisco Packet Tracer and a step-by-step algorithm for debugging its protection system using the ASA5505 firewall to filter incoming traffic were proposed. Strong passwords have been created for IoT device accounts. WPA2 / 3-PSK wireless protocols using the AES algorithm ensure the security of wireless data transmission. The home controller has a unique SSID. The created system can be implemented and safely used in homes and offices.*

Keywords: *IoT, network, smart home, VPN, WPA2-PSK, ASA5505, ACL.*

Fig .: 10. Table: 1. Bibl .: 12

Базилевич Володимир Маркович – кандидат економічних наук, доцент, завідувач кафедри інформаційних та комп'ютерних систем, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна)
Bazylevych Volodymyr – PhD in Economic science, Associate Professor, Head of Information and Computer Department, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: bazvlamar@gmail.com
ORCID: https://orcid.org/0000-0001-8935-446X

Мальцева Марина Віталіївна – студентка групи КБ-161, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Maltseva Marina – student of the KB-161 group, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: maryna_maltseva@ukr.net

Петренко Тарас Анатолійович – кандидат технічних наук, доцент кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Petrenko Taras – PhD in Technical Science, Associate Professor of Cybersecurity and Mathematical Simulation Department Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: mail_taras@ukr.net
ORCID: https://orcid.org/0000-0001-5571-3815
ResearcherID: G-5801-2014
SCOPUS Author ID: 57193026484

Черниш Леся Григоріївна – кандидат технічних наук, доцент, доцент кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Chernysh Lesia – PhD in Technical Science, Associate Professor, Associate Professor of Department of Cybersecurity and Mathematical Simulation, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: lg4@ukr.net
ORCID: http://orcid.org/0000-0001-7446-1684

Базилевич В., Мальцева М., Петренко Т., Черниш Л. Захищена система розумного будинку з використанням Internet of Things. *Технічні науки та технології.* 2020. № 2 (20). С. 218-228.