УДК 004.942 **Овчиннік С.О., Лаптєв О.А., Зозуля С.А., Правдивий А.М.**
DOI: 10.31673/2409-7292.2020.031421

МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ СИСТЕМИ «РОЗУМНИЙ ДІМ» НА БАЗІ НОВОГО ПРОТОКОЛУ ОБМІНУ ДАНИХ

Проведено аналіз проблем безпеки обміну інформації між клієнтом та системою «Розумний дім». Визначені пріоритети захисту інформації на етапі передачі інформації. Проведений аналіз запропонованого нового бездротового мережевого стандарту Thread. Thread використовує IPv6 і побудований на стандарті IEEE 802.15.4, а його головна перевага - безпека. Одночасно в мережі можуть знаходитися до 250 пристроїв, які захищаються шифруванням рівня банківської системи. Але цього недостатньо для забезпечення цілісності інформації.

Запропоновано використання нового алгоритму шифрування на основі поточного алгоритму шифрування, заснованого на алгоритмі блокчейну, завдяки використанню динамічно змінюваного нелінійного бієктивного перетворення (S-блоки) дозволяє уникнути значних проблем інформаційної безпеки.

Цей алгоритм використовуються для забезпечення конфіденційності (безпеки під час передачі), цілісності (безпеки при зберіганні та модифікації лише для авторизованих користувачів) та автентичності (достовірність джерела повідомлення). Та забезпечує надійний захист інформації.

Ключові слова: «розумний дім», інформація, методика, безпека протоколів, обмін даними.

Вступ

Сьогодні, завдяки нестримному розвитку мікроелектроніки, каналів зв'язку, Інтернет-технологій і штучного інтелекту, тема «розумних будинків» стає все більш актуальною. Людське житло зазнало істотних змін з часів кам'яного віку і в епоху Промислової Революції і Інтернету Речей, стало зручним, функціональним і безпечним. Розумний будинок включає в себе величезну кількість IoT-пристроїв, які збирають і обробляють дані. Вони дають користувачам певні можливості по контролю за апартаментами як в ручному, так і автоматичному режимі. У «розумному середовищі» пристрої періодично обмінюються даними по мережі. Це відбувається або безпосередньо від пристрою до пристрою, або через хмару. Тому захист передачі інформації клієнт - «розумний будинок» є дуже актуальним на сьогоднішній день [1].

Особливістю роботи – системи «розумного будинку» є те, що більшість команд на пристрої проходять через мережі передачі даних. В цілому всі елементи ланцюжка мають доступ в Інтернет. Це робить їх уразливими до атак ззовні і наражає на небезпеку не тільки інформацію користувача, але також його здоров'я. Все це змінює парадигму мислення, в якій мовиться: «Мій будинок – моя фортеця».

Однак безпека, особливо безпека протоколів обміну даними між клієнтом та «розумний будинок» - це необхідна вимога для розумного будинку. До складу системи безпеки можуть входити системи спостереження, системи моніторингу (в тому числі здоров'я) і системи безпеки, до яких можна отримати віддалений доступ. Тому розробка методики захисту інформаційного протоколу обміну між клієнтом та системою «розумний будинок» є дуже важливим питанням [2].

Аналіз останніх досліджень і публікацій.

Компанія HP провела дослідження ринку інтелектуальних систем в ході якого з'ясувала, що практично всі системи мають проблеми з безпекою [3].

Перша проблема - недостатньо надійна перевірка аутентифікації. Системи, незважаючи на те, що володіли хмарними і мобільними інтерфейсами, не вимагали установки паролів достатньої довжини і складності. Жодна з систем не блокувала обліковий запис після певного числа невдалих спроб введення пароля [1, 2].

Ще одна проблема виявилася пов'язана з конфіденційністю. Всі системи збирали будь-які види персональної інформації: імена, адреси, номери телефонів і кредитних карт. Це викликає певну стурбованість, оскільки створює загрозу крадіжки облікових даних.

Варто також відзначити, що ключовою особливістю багатьох домашніх систем безпеки є використання відео, перегляд якого доступний через різні інтерфейси. Конфіденційність подібних даних теж знаходиться під питанням [4].

Нарешті, останньою проблемою експерти назвали відсутність шифрування при передачі даних. Хоча у всіх системах реалізовані механізми шифрування на транспортному рівні, такі як SSL / TLS, багато хмарні підключення залишаються уразливими для атак.

Дуже важливий момент: щоб виключити несанкціоноване втручання в роботу пристрою, обмін між контролером і сервером повинен відбуватися в зашифрованому вигляді. Для забезпечення безпеки протоколів обміну даних потрібно відволіктися від основної функції техніки і почати сприймати її як комп'ютерну мережу, щоб помітити дірки в інформаційній безпеці.

Таким чином, компанії Google, Samsung Electronics, Silicon Labs і деякі інші об'єдналися з метою розробити новий бездротовий мережевий стандарт спеціально для розумних будинків. Він отримав назву Thread. Thread використовує IPv6 і побудований на стандарті IEEE 802.15.4, а головною його перевагою є саме безпека. Одночасно в мережі можуть знаходитися до 250 пристроїв, які захищаються шифруванням на рівні банківської системи [3, 4].

Ще одна особливість Thread - це прозорість. Користувач бачить список всіх підключених пристроїв, завдяки якому йому легко визначити, що з чим пов'язано. На даний момент є ряд рішень для розумних будинків (ZigBee і 6LowPAN), які легко можуть почати підтримувати запропонований стандарт без апаратних змін - в їхньому випадку потрібно просто оновити програмне забезпечення [3].

Цей сценарій показує, наскільки глибоко IoT став інтегруватися в життя людей. Це очевидно з того, як існує застосований пристрій IoT для кожної частини будинку, від вітальні і кухні до ванної кімнати і горища. Ця глибока участь в житті людей робить атаки Інтернету речей життєздатними для хакерів і ефективними для користувачів. Можливо, ніде кіберзагрози більш не були потенційно агресивними і особистими, ніж в розумних будинках.

З аналізу сучасної літератури можна зробити висновок, що універсальних протоколів обміну даними між клієнтом та системою «розумний дім», зараз практично немає. Тому розробка метода підвищення надійності передачі інформації та кодів керування у каналах зв'язку між оператором та системою «розумний дім» –є дуже актуальною.

Постановка проблеми

Найбільш вагомою є загроза пошкодження або втручання у канал зв'язку між клієнтом та системою «Системи розумний дім». Ця загроза включає в себе моніторинг і перехоплення повідомлень під час сеансу зв'язку. Через обсяг і чутливості даних, що проходять через екосистеми IoT, атаки з метою націлювання на канал зв'язку особливо небезпечні, оскільки повідомлення і дані можуть бути перехоплені, захоплені або ними можна маніпулювати під час передачі. Виходячи з вищевикладеного, а розробка метода підвищення надійності передачі інформації та кодів керування у каналах зв'язку між оператором та системою «розумний дім» є вкрай актуальною.

Виклад основного матеріалу.

Зарубіжні компанії провели дослідження ринку інтелектуальних систем в ході якого з'ясували, що практично всі системи мають проблеми з безпекою. Все більше підключених пристроїв приєднується до екосистемі Інтернету речей, дослідники проводять ряд тестів безпеки, щоб виявити уразливості Інтернету речей і розповісти світу про потенційні проблеми безпеки при підключенні пристроїв без належних заходів безпеки. Існують такі ключові вектори загроз:

Загроза, що виходить від зламаних пристроїв. Оскільки багато пристроїв мають власні цінності в силу їх конструкції і характеру функцій, підключений пристрій являє собою потенційну ціль для використання зловмисником. Підключена камера відеоспостереження може розкрити особисту інформацію, наприклад місцезнаходження користувача, при зломі. Це може бути щось настільки ж просте, як управління освітленням в будинку або

службовому приміщенні, або щось настільки ж зловмисне, як керування автомобілем або медичним пристроєм, який може заподіяти фізичну шкоду [5].

Загроза по каналу зв'язку.

Загроза по каналу зв'язку включає в себе моніторинг і перехоплення повідомлень під час сеансу зв'язку. Через обсяг і чутливості даних, що проходять через екосистеми IoT, атаки з метою націлювання на канал зв'язку особливо небезпечні, оскільки повідомлення і дані можуть бути перехоплені, захоплені або ними можна маніпулювати під час передачі. Наприклад, зловмисник може відслідковувати споживання енергії, щоб дізнатися час простою або час безвідмовної роботи системи (наприклад, службових приміщень), щоб спланувати атаку на всі основні системи управління і контролю розумних міст; інший зловмисник може маніпулювати даними, переданими комунальною компанією, і змінювати інформацію. Успішні порушення, такі як ці приклади, можуть поставити під загрозу довіру до інформації та даних, що передаються через інфраструктуру IoT [6].

Основні загрози для виробників пристроїв Інтернету речей і постачальників хмарних послуг можуть поставити під загрозу всю екосистему Інтернету речей, оскільки виробникові і хмари Інтернету речей довірено розміщувати трильйони даних, деякі з яких є дуже конфіденційними за своєю природою. Ці дані важливі, тому що вони являють собою аналітику, яка є основним стратегічним активом, це значний обсяг конкурентної інформації в очах підпільної APT-групи, якщо вона розкрита. Якщо майстер скомпрометований, це дасть зловмисникові можливість маніпулювати безліччю пристроїв одночасно, деякі з яких, можливо, вже були розгорнуті в польових умовах. Наприклад, якщо у постачальника, який часто випускає вбудоване програмне забезпечення / програмне забезпечення, механізм скомпрометований, на пристрої може бути впроваджений шкідливий код.

Тому пропонується метод захисту передачі інформації між клієнтом та системою «розумний дім» на базі нового протоколу обміну даних. Він заснований на модифікації відомого алгоритму (OFM) S-box ГОСТ 34.12-2015, що забезпечує "усунення" можливих криптографічних закладок та підвищення криптостійкості в постквантовий період (поява повномасштабного квантового комп'ютер, що дозволяє зламати на основі алгоритмів Гровера та Шора сучасні симетричні та асиметричні криптосистеми). Крім того, комерційне впровадження забезпечить "протидію" можливих криптодепозитів спецслужбами, що зменшить ризик злому шляхом виявлення "слабких" (вразливих) місць на основі криптографічних закладок.

В алгоритмі блок, що шифрується (довжина 64 біта), розділений на дві рівні частини (32 біти) - праву та ліву. Далі тридцять дві ітерації виконуються з використанням ітераційних ключів, отриманих з вихідного 256-бітного ключа шифрування. Під час кожної ітерації здійснюється одне перетворення на основі мережі Фейстела з правою та лівою половиною зашифрованого блоку. Спочатку права частина складається в модуль 232 з поточним ітераційним ключем, потім отримане 32-бітове число ділиться на вісім 4-бітових і кожен з них, використовуючи таблицю перестановок, перетворюється в інший 4-бітний номер. Після цього перетворення отримане число крутиться вліво на одинадцять розрядів. Далі XOR трансформується з лівою половиною блоку. Отримане 32-бітове число записується в правій половині блоку, а старий вміст правої половини переноситься в ліву половину блоку. Діаграма основного кроку крипто-перетворення алгоритму показана на рис. 1.

Основний крок криптотрансформації алгоритму складається з наступних етапів:

Крок1. Введення вихідних даних для основного кроку криптоперетворення N - 64-розрядний блок введення перетворюється на два 32-розрядних цілих числа (молодшу (N_1) і найстаршу (N_2) частини);

Крок 2. Додавання до ключа. Молодша частина перетвореного блоку складається в модуль із ключовим елементом, що використовується на кроці.

Крок3. Заміна блоку. Отримане на попередньому кроці 32-бітове значення інтерпретується як масив із чотирьох 4-бітових блоків коду: $S_m = (S_0, S_1, S_2, \ldots S_{15})$.

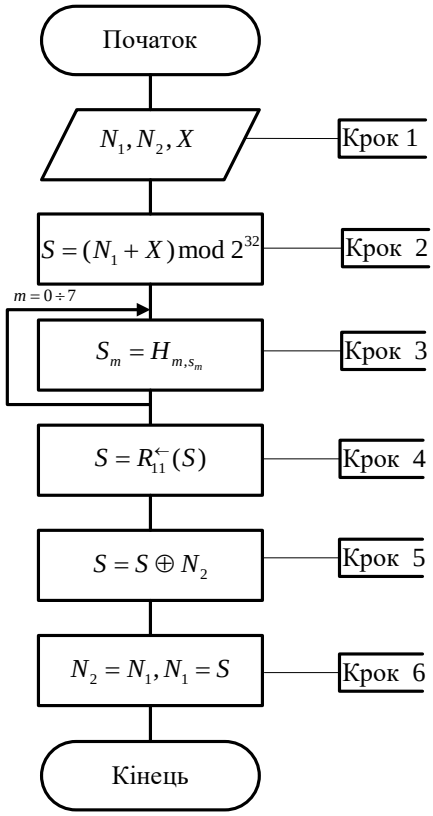

Рис. 1. Схема основного кроку криптоперетворення алгоритму ГОСТ 34.12-2015

Крок4. Циклічний зсув на 11 біт вліво.

Крок5. Додане побиття: значення, отримане на кроці 3, порушується модулем 2 із старшою половиною перетвореного блоку.

Крок6. Зсув по ланцюжку: Молодша частина перетвореного блоку зміщується на місце старшого, а на його місце розміщується результат попереднього кроку.

Тоді структура алгоритму може описати діаграму, представлену на рис. 2.

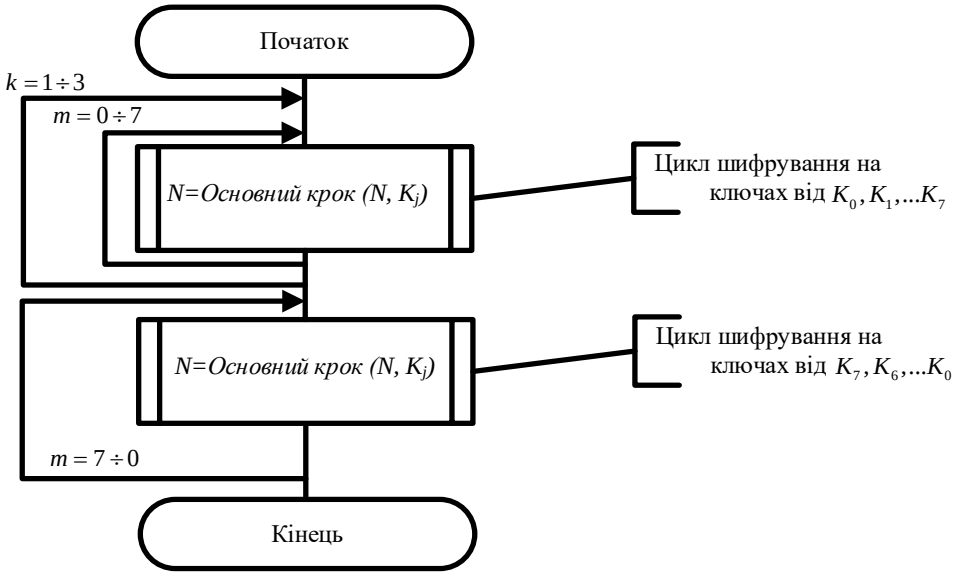

Рис. 2. Цикл шифрування ГОСТ 34.12-2015

Щоб створити вдосконалення алгоритму ГОСТ 34.12-2015, ми змінимо основний крок криптоперетворення алгоритму (рис. 3) в режимі OFM [7].

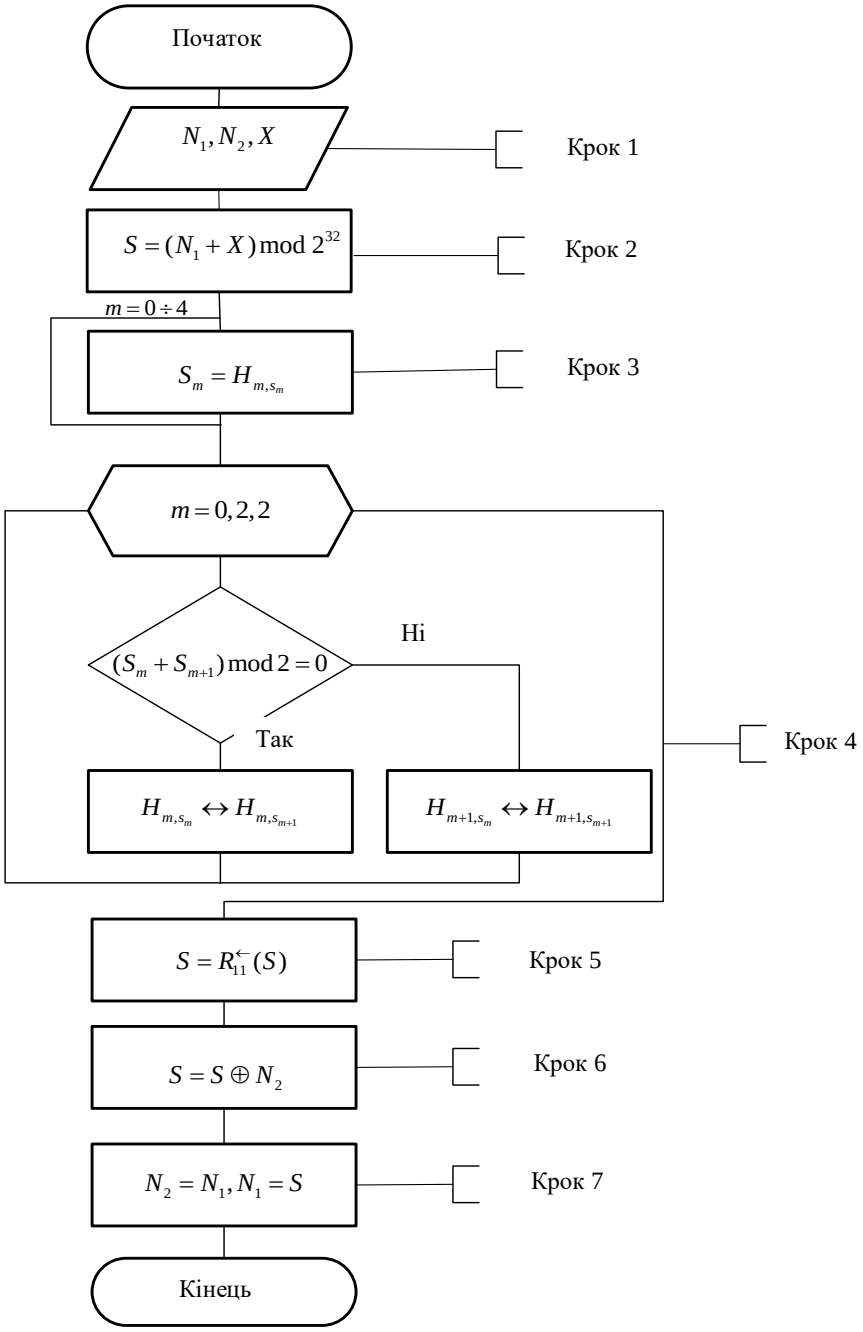

Рис. 3. Схема вдосконаленого основного кроку криптоперетворення алгоритму ГОСТ 34.12-2015

Візьміть за основу порядок змін значень у блоці S алгоритму потокового шифрування RC 4. RC4, алгоритм потокового шифрування, був запропонований в 1987 році Рональдом Лінном Рівестом, відомим американським фахівцем з криптографії. З 1994 року він широко використовується в ряді криптографічних додатків, включаючи відомі, такі як SSL та TLS, для шифрування даних, переданих через мережі передачі даних, які не забезпечують захист даних користувачів, WPA та WEP для захисту бездротових з'єднань. В алгоритмі шифрування потокового передавання два значення S-блоку міняються місцями, коли формується псевдо-ключова послідовність [8].

Основний крок криптоперетворення алгоритму складається з наступних етапів:

Крок1. Введення вихідних даних для основного кроку криптоперетворення N - 64-розрядний блок введення перетворюється на два 32-розрядних цілих числа (молодшу (N_1)) та найстаршу (N_2)) частини);

Крок 2. Додавання до ключа. Молодша частина перетвореного блоку складається в модуль з ключовим елементом, що використовується на сходинці.

Крок3. Заміна блоку. 32-бітове значення, отримане на попередньому кроці, інтерпретується як масив із чотирьох 8-бітових блоків коду: $S_m = (S_0, S_1, S_2, ... S_{255})$.

Потім значення кожного з чотирьох блоків замінюється новим, яке вибирається таблицею заміщення наступним чином: значення блоку S_i змінюється на елемент порядку S_i (нумерація від нуля) і вузол підстановок (тобто і рядок таблиці заміщення, нумерація також від нуля). Іншими словами, як заміна значення блоку, елемент вибирається із таблиці замін із числом, рівним номеру блоку, що замінюється, і номером стовпця, рівним 8-бітовому значенню цілого невід'ємного номер.

Крок 4. Динамічна зміна таблиці заміщення виглядає наступним чином: якщо сума $S_0 + S_1$ парне число, то міняються місцями значення $S_0 \leftrightarrow S_1$ таблиць H_0, інакше $S_0 \leftrightarrow S_1$ таблиць H_1. Якщо сума $S_2 + S_3$ парне число, то поміняйте місцями значення $S_2 \leftrightarrow S_3$ таблиць H_2, інакше $S_0 \leftrightarrow S_1$ таблиць H_3.

Крок5. Циклічний зсув на 11 біт вліво.

Крок6. Додане побиття: значення, отримане на кроці 3, порушується модулем 2 зі старшою половиною перетвореного блоку.

Крок7. Зсув по ланцюжку: Молодша частина перетвореного блоку зміщується на місце старшого, а на його місце розміщується результат попереднього кроку.

Крок6. Отримане значення перетвореного блоку повертається в результаті виконання алгоритму основного кроку крипто-перетворення.

Використання цього перетворення дозволяє динамічно (на основі простого генератора послідовностей псевдо-ключів) формувати режим OFM та забезпечувати необхідний рівень криптостійкості.

Розрахунки та практичні рекомендації:

Підсумовуючи етапи захищеності, знайдемо «Підвищення ймовірності захищеності»:

У звітах зарубіжних компаніях наведені наступні дані: P1=0,4 – це стандартний захист системи «розумного дому». Але, як виявилося, алгоритми шифрування і конфіденційність даних була на проблематичному рівні. Постає питання покращити безпеку, розробивши бездротовий мережевий стандарт, ймовірність якого P2=0,25. Тепер існує ймовірність захищеності P1+P2=0,4+0,25=0.65. Згадавши, що в системах «Розумний дім» відсутнє шифрування, запропонуємо модифікацію відомого алгоритму (OFM) S-box ГОСТ 34.12-2015, що забезпечує "усунення" можливих криптографічних закладок та підвищення криптостійкості в постквантовий період, ймовірність захищеності якого P3=0.3. У зв'язку з тим, що у нас система послідовна, ми отримаємо P1+P2+P3=0,95=P. Розрахуємо наскільки наша нова система має більшу захищеності:

(P-(P1+P2))/(P1+P2)×100%=(0,95-0,65)/(0,65)×100%≈46%

Отже, наша нова система на 46% має більшу захищеність, ніж існуючий до цього метод.

Окрім математично технічних засобів розроблені практичні рекомендації щодо захисту пристроїв IoT у своїх розумних будинках. Заходи безпеки, які користувачі можуть прийняти для захисту своїх розумних будинків від атак на пристрої Інтернету речей [9, 10]:

1) Зрівняйте всі підключені пристрої. Всі пристрої, підключені до мережі, наприклад, вдома чи на рівні підприємства, повинні бути добре враховані. Слід зазначити їх налаштування, облікові дані, версії прошивки і останні виправлення. Цей крок може допомогти оцінити, які заходи безпеки слід вжити користувачам, і визначити, які пристрої, можливо, доведеться замінити або оновити.

2) Змініть паролі та налаштування за замовчуванням. Переконайтеся, що установки, що використовуються кожним пристроєм, відповідають більш високої безпеки, і поміняйте налаштування, якщо це не так. Змініть паролі за замовчуванням і слабкі паролі, щоб уникнути атак, таких як груба сила і небажаний доступ.

3) Патч вразливостей. Установка виправлень може виявитися складним завданням, особливо для підприємств. Але обов'язково застосовувати виправлення відразу після їх випуску. Для деяких користувачів виправлення можуть порушити їх звичайні процеси, для чого можна використовувати віртуальне виправлення.

4) Застосовуйте сегментацію мережі. Використовуйте сегментацію мережі, щоб запобігти поширенню атак і ізолювати потенційно проблемні пристрої, які не можна відразу відключити.

Загальні рекомендації з безпеки Інтернету речей

1) Традиційні параметри, такі як справжність, конфіденційність, цілісність і доступність, можуть використовуватися для захисту екосистеми Інтернету речей.

2) Для управління безпекою взаємопов'язаних пристроїв нам потрібна дійсно відкрита екосистема зі стандартизованими інтерфейсами прикладного програмування, які забезпечують взаємодію з надійною і автоматичною системою виправлень. Криптографічні механізми - більш надійний спосіб захисту зв'язку від підробки, підробки прошивки і незаконного доступу.

3) Багаторівнева безпека з високим рівнем захисту для захисту даних від атак шкідливих програм, вразливостей в мережах і програмних додатках.

4) Апаратна безпека може бути реалізована шляхом впровадження захисту мікросхеми у вигляді TPM (Trusted Perception Module), довіреного термінального модуля і довіреного мережевого модуля. Безпечне завантаження можна використовувати, щоб гарантувати, що на пристрої буде працювати тільки перевірене програмне забезпечення.

5) Мережева безпека може бути досягнута за допомогою рішень безпеки, орієнтованих на дані, які забезпечують безпеку шифрування даних при передачі або зберіганні. Для виявлення небажаних вторгнень і запобігання зловмисних дій можуть використовуватися брандмауери і системи запобігання вторгнень.

6) Безпека на рівні додатків відноситься до методів захисту веб-додатків від зловмисних атак, які можуть розкрити конфіденційну інформацію. Це можна зробити за допомогою брандмауера веб-додатків, контролера доставки додатків безпечного веб-шлюзу і т.д.

7) Повинні бути національні сертифікати або політики, що засвідчують безпеку електронної ланцюга поставок.

Напрямки подальших досліджень.

Подальші дослідження доцільно спрямувати на удосконалення програмних засобів для ліквідування загроз, що виходять від зламаних пристроїв. Оскільки багато пристроїв мають власні цінності в силу їх конструкції і характеру функцій, підключений пристрій являє собою потенційну ціль для використання зловмисником. Підключена камера відеоспостереження може розкрити особисту інформацію, наприклад місцезнаходження користувача, при зломі. Це може бути щось настільки ж просте, як управління освітленням в будинку або службовому приміщенні, або щось настільки ж зловмисне, як керування автомобілем або медичним пристроєм, який може заподіяти фізичну шкоду.

Висновки

Проведений аналіз проблем безпеки обміну даними між клієнт - «розумний будинок». Визначені пріоритети захисту інформації на етапі передачі інформації. Проведений аналіз запропонованого нового бездротового мережевого стандарту Thread. Thread використовує IPv6 і побудований на стандарті IEEE 802.15.4, а основним його достоїнством є безпека. Одночасно в мережі можуть знаходитися до 250 пристроїв, які захищаються шифруванням рівня банківської системи. Але цього недостатньо для забезпечення цілісності інформації.

Запропоновано використання нового алгоритму шифрування на основі поточного алгоритму шифрування, заснованого на алгоритмі блокчейну, завдяки використанню динамічно змінюваного нелінійного бієктивного перетворення (S-блоки) дозволяє уникнути значних проблем інформаційної безпеки.

Цей алгоритм використовуються для забезпечення конфіденційності (безпеки під час передачі), цілісності (безпеки при зберіганні та модифікації лише для авторизованих користувачів) та автентичності (достовірність джерела повідомлення). Та забезпечує надійний захист інформації. Дозволяє підвищити захист протоколу передачі даних та інформації системи «Розумний дім» на 46 %.

Перелік посилань

1. Inside the Smart Home: IoT Device Threats and Attack Scenarios. URL: https://www.trendmicro.com/vinfo/gb/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios (дата звернення: 10.06.2020)
2. Security and privacy issues for an IoT based smart home. URL: https://ieeexplore.ieee.org/document/7973622 (дата звернення: 10.06.2020)
3. How safe are smart homes?URL: https://www.kaspersky.com/resource-center/threats/how-safe-is-your-smart-home (дата звернення: 10.06.2020)
4. IEEE Standard for Information technology – Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 11: Wireless LAN Medium Access Control and Physical Layer (PHY) Specifications.
5. Serhii Yevseiev, Roman Korolyov, Andrii Tkachov, Oleksandr Laptiev, Ivan Opirskyy, Olha Soloviova. Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE). Scopus. Volume 9. No. 5, September-Oktober 2020, pp 8725-8729
6. Лаптєв О.А.,Барабаш А.О. Методика розрахунку ймовірності негласного отримання інформації на основі існуючих методів виявлення сигналів.Тези доповідей: 52 Міжнародна конференція «Розвіток науки в XXI столітті» м.Харків, 14 вересня 2019 р. С.62 – 74.
7. Лаптєв О.А. Актуальні проблеми кібербезпеки та захисту інформації. Тези доповідей: «Вразливість інформаційної системи як основний елемент моделювання схем інформаційної безпеки». Кафедри систем інформаційного та кібернетичного захисту від 07 травня 2019 р.м.Київ. ДУТ, С. 37 – 40.
8. Бабенко Р.В., Лаптєв О.А., Правдивий А.М., Зозуля С.А., Стефурак О.Р. Удосконалена методика вибору послідовності пріоритетів обслуговання потоків інформації. Науково-практичний журнал «Зв'язок». К. : ДУТ, 2020. №4 (146), С.45 – 49.
9. Стефурак О.Р., Тихонов Ю.О., Лаптєв О.А., Зозуля С.А. Удосконалення стохастичної моделі з метою визначення загроз пошкодження або несанкціонованого витоку інформації. Сучасний захист інформації: науково-технічний журнал. К.: ДУТ, 2020. № 2(42)., С 19 – 26.
10. Savchenko Vitalii, Syrotenko Anatolii, Shchypanskyi Pavlo, Matsko Oleksander, Laptiev Oleksander, The Model of Localization Precision for Detection of Hidden Transmitters. International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-9 Issue-4, February 2020. ISSN: 2278–3075. P2114 – 2119.

Надійшла: 15.06.2020 Рецензент: д.т.н., професор Кожухівський А.Д.