Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Колодія Єгора Сергійовича*

академічної групи *125м-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методи оцінки ризиків кібербезпеки в системах "Розумний будинок"*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		Рейтинговою	**Інституційною**	
кваліфікаційної роботи	к.т.н. доц. Сафаров О.О.			
розділів:				
Спеціальний	доц. Сафаров О.О.			
Економічний	к.т.н. к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту ***Колодію Єгору Сергійовичу*** **академічної групи** ***125м-20-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Методи оцінки ризиків кібербезпеки в системах "Розумний будинок"***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _10.12.2021_____ № _1036-с___

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз розумного будинку, його підсистем, систем автоматизації розумного будинку, основних вразливостей та існуючих методів забезпечення кібербезпеки в системі Розумний будинок.	01.12.2021
Розділ 2	Аналіз вразливостей та загроз. Розроблено метод забезпечення забезпечення ІБ.	04.01.2022
Розділ 3	Обґрунтувана економічна доцільності розроблених методів.	10.01.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 02.09.2021

Дата подання до екзаменаційної комісії: 14.01.2022

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 73 с., 7 рис., 3 табл., 4 додатка, 10 джерел.

Об’єкт дослідження: захист інформації в розумному домі.

Мета роботи (проекту): дослідити вразливості, провести аналіз загроз та запронувати методи підвищення інформаційної безпеки у системі розумного будинку. Запропонувати метод підвищення захисту даних, що цикулюють у системі.

Методи розробки: порівняння, аналіз, опис.

У першому розділі було розглянуто застосування Інтернету речей та розумного дому, наведені його основні підсистеми розумного дому. Також були проаналізовані системи автоматизації розумного будинку, наведені переваги та недоліки кожної з них. Були описані основні вразливості кібербезпеки в розумних пристроях, причини їх виникнення. Також були проаналізовані існуючі методи забезпечення інформаційної безпеки в системі розумного будинку.

У другому розділі (спеціальній частині) був проведений аналіз основних вразливостей та загроз у системі розумного будинку. Були проаналізовані рівні загроз та методи підвищення кібербезпеки у системі розумного будинку. Також було розглянуто та реалізувано масштабовану систему, що розрахована на багато користувачів системи розумний будинок, а також знайдено прийнятний варіант для забезпечення конфіденційності даних як на стороні клієнта, так і на стороні сервера.

В третьому розділі було обґрунтувана економічна доцільності розроблених методів.

РОЗУМНИЙ БУДИНОК, ПРОТОКОЛ, ІНТЕРЕНЕТ РЕЧЕЙ, БЕЗПРОВОДОВІ, ЗАХИСТ ІНФОРМАЦІЇ, СТАНДАРТ, ТЕХНОЛОГІЯ, ПЕРЕВАГИ, НЕДОЛІКИ

РЕФЕРАТ

Пояснительная записка: 73 с., 7 рис., 3 табл., 4 приложения, 10 источников.

Объект исследования: защита информации в умном доме.

Цель работы (проекта): исследовать уязвимости, провести анализ угроз и предотвратить методы повышения информационной безопасности в системе умного дома. Предложить метод повышения защиты данных, цикулирующих в системе.

Методы разработки: сравнение, анализ, описание.

В первом разделе было рассмотрено применение Интернета вещей и умного дома, приведены его основные подсистемы умного дома. Также были проанализированы системы автоматизации умного дома, приведены преимущества и недостатки каждой из них. Были описаны главные уязвимости кибербезопасности в разумных устройствах, предпосылки их возникновения. Также проанализированы существующие методы обеспечения информационной безопасности в системе умного дома.

Во втором разделе (специальной части) был проведен анализ основных уязвимостей и угроз в системе умного дома. Были проанализированы уровни угроз и методы повышения кибербезопасности в системе умного дома. Также была рассмотрена и реализована масштабируемая система, рассчитанная на многопользовательскую систему умного дома, а также найден приемлемый вариант для обеспечения конфиденциальности данных как на стороне клиента, так и на стороне сервера.

В третьем разделе была обоснована экономическая целесообразность разработанных методов.

УМНЫЙ ДОМ, ПРОТОКОЛ, ИНТЕРЕНЕТ ВЕЩЕЙ, БЕСПРОВОДНЫЕ, ЗАЩИТА ИНФОРМАЦИИ, СТАНДАРТ, ТЕХНОЛОГИЯ, ПРЕИМУЩЕСТВА, НЕДОСТАТКИ

ABSTRACT

Explanatory note: 73 pp., 7 fig., 3 tab., 4 applications, 10 sources.

Object of research: information protection in a smart home.

Purpose of the work (project): investigate vulnerabilities, conduct threat analysis and prevent methods of improving information security in the smart home system. Propose a method for improving the protection of data circulating in the system.

Development methods: comparison, analysis, description.

In the first section, the application of the Internet of things and smart home was considered, its main subsystems of smart home are given. Smart home automation systems were also analyzed, the advantages and disadvantages of each of them were given. The main cybersecurity vulnerabilities in intelligent devices, the prerequisites for their occurrence were described. The existing methods of ensuring information security in the smart home system are also analyzed.

In the second section (special part), an analysis of the main vulnerabilities and threats in the smart home system was carried out. Threat levels and methods for improving cybersecurity in the smart home system were analyzed. A scalable system designed for a multi-user smart home system was also considered and implemented, and an acceptable option was found to ensure data confidentiality both on the client side and on the server side.

In the third section, the economic feasibility of the developed methods was substantiated.

SMART HOUSE, PROTOCOL, INTERNET OF THINGS, WIRELESS, PROTECTION OF INFORMATION, STANDARD, TECHNOLOGY, ADVANTAGES, DISADVANTAGES

СПИСОК УМОВНИХ СКОРОЧЕНЬ

AES – Advanced Encryption Standard;

AS – Authentication Server;

DES – Data Encryption Standard;

DDoS – Distributed Denial of Service;

CBC – Cipher Block Chaining;

HAKDP – Hashed Key Distribution Patterns;

IoT – Internet of Things;

KDP – Key Distribution Pattern;

NAS – Network Attached Storage;

OTPS – One-Time Password Service;

TGS – Ticket Granting Server;

TGT – Ticket Granting Ticket;

ІБ – інформаційна безпека;

ПЗ – програмне забезпечення

ЗМІСТ

ВСТУП

Оскільки технології продовжують проникати в сучасне суспільство, безпека та довіра, які ми покладаємо на ці системи стають все більш серйозною проблемою. Особливо враховуючи велику кількість атак, спрямованих на організації, уряди та суспільство.

Традиційний підхід у вирішенні таких проблем полягає у проведенні оцінки ризиків кібербезпеки з метою виявлення критичних вразливостей, загроз, ймовірність успішної атаки та шкоду, яка може бути завдана.

Одне з найголовніших досягнень за останні роки – це Інтернет речей (IoT): підключення повсякденних об'єктів – «речей» – до інтернету. Ці розумні пристрої збирають інформацію про своє оточення, полегшують аналіз даних, спілкуються з користувачем та іншими розумними об'єктами, і здатні приймати розумні рішення на основі аналізованих даних. Різні прогнози передбачають величезне зростання IoT. Це означає, що кількість підключених пристроїв буде зростати, тим самим створюючи всюдисущий зв'язок і потенційно перетворюючи життя на краще – суцільно спрощуючи його.

Але методи забезпечення захисту даних користувачів у розумних системах не є надійними. Тож, у даній роботі був проведений аналіз над основними ризиками та вразливостями, що є у розумному будинку та запропоновано методи підвищення кібербезпеки.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Інтернет речей

Головною метою IoT є надання користі суспільству за допомогою ряду розумних платформ і повсюдного поєднання цифрових, кіберфізичних і соціальних систем. Це з'єднання забезпечує взаємозв'язки між системами, які можуть сильно відрізнятися за щільністю, часом та автоматизацією. Проте проблема з IoT з точки зору безпеки та управління довірою полягає в тому, що існуючі методології оцінки ризиків були дуже давно і не є актуальними. Таким чином, ці методології можуть не врахувати складність або поширеність цих автоматизованих систем. Зрештою, застосування цих методів для IoT може зробити нас сліпими до нових ризиків, що виникають у екосистемах. Вони можуть стосуватися кібератак та нових соціальних процесів, які виникають у масштабах населення в режимі реального часу (наприклад, вірусні ефекти в соціальних мережах), і до «стихійних лих», притаманних випадковому збою IT системи.

За своєю природою IoT є складною технологічною парадигмою.

Перше, на що слід звернути увагу – це варіативність масштабування пристроїв і систем. Однією з головних переваг IoT є здатність розширюватися (або зменшуватися) у масштабі та вміщувати широкий спектр нових систем і «речей».

Інший аспект IoT – його динамізм та тимчасовість з'єднань між пристроями Інтернет речей. Пристрої можуть бути слабко пов'язані для виконання деякої задачі та розривати з'єднання після її завершення, або з'єднання можуть бути незмінними. Важливо розуміти рівень темпоральності, необхідний конкретний контекст IoT з урахуванням результуючого впливу на ризик (наприклад, сталість зв'язку з несанкціонованими пристроїв). Останнім рушійним фактором у характері взаємин будуть ресурси, необхідні для підтримувати управління та контроль таких відносин.

Обмежені ресурси означатимуть, що пристрої IoT можуть бути змушені прийняти режими, що допускають невелику різноманітність взаємин через ресурс, необхідний їх обслуговування; або вони можуть бути поєднані з хмарними системами, що також необхідно буде оцінити ризик.

Неоднорідність суб'єктів, здатних взаємодіяти в екосистемах Інтернету речей, також є важливим фактором.

1.2 Стан питання

Одна з найвідоміших частин IoT – це розумний будинок, орієнтований на споживача, який включає в себе розумні пристрої, які можна використовувати в домашніх умовах. Приклади включають розумні термостати, замки та дитячі монітори тощо.

Усі технології розумного дому спрямовані на те, щоб зробити будинок комфортнішим, керованим, безпечним і екологічним.

Потенціал ринку «розумного будинку» великий. У 2016 році Європейська комісія визначила розумний дім як один із секторів ринку IoT з найбільш реальними можливостями для бізнесу зараз і протягом п’яти років, поряд із розумним виробництвом, розумним особистим здоров’ям та здоров’ям, розумними містами тощо. У період з 2020 по 2024 роки обсяг світового ринку технологій для розумного будинку виросте на 65,95 мільярдів долларів, а середньорічні темпи зростання витрат на такі продукти складуть 17%. При ринковій вартості 26,7 мільярдів у 2020 році найбільший дохід було отримано в США. У Європі дохід становив майже 13 мільярдів доларів США. Підйом даного ринку аналітики пояснюють розвитком технологій зв'язку і зростаючим інтересом споживачів до домашньої автоматизації.

За останні кілька років також стрімко зросла пропозиція пристроїв для розумного дому. Швидкий пошук у поточній онлайн-пропозиції пристроїв для розумного дому повертає розумні термостати, замки, детектори диму, камери

спостереження, освітлення, вимикачі, будильники, телевізори, іграшки, радіоняні тощо. Кілька постачальників пропонують повні платформи розумного дому, наприклад Samsung (SmartThings), Apple (HomeKit) і Amazon (Echo). Усі ці технологічні гіганти сподіваються отримати монополію на розумний будинок і мають тенденцію створювати ефекти блокування за допомогою прямих і непрямих мережевих ефектів, що є невигідним для нових конкурентів.

Потенціал та переваги розумного дому можуть бути компенсовані занепокоєнням щодо кібербезпеки та конфіденційності. Проблеми кібербезпеки також стосуються конфіденційності, оскільки відсутність безпеки може призвести до різного роду шкоди конфіденційності. Загалом, (персональні) дані є основою будь-якого розумного пристрою. Це викликає занепокоєння щодо конфіденційності, зокрема щодо захисту персональних даних. Розумний дім викликає додаткові проблеми з конфіденційністю.

Коли хтось використовує технологію розумного дому у своєму будинку, він ділиться особистою та конфіденційною інформацією з приватними компаніями. Це може бути проблематичним саме по собі з точки зору конфіденційності. У нещодавньому опитуванні споживачів щодо мобільних технологій понад 40% респондентів виявили, що технології розумного дому розкривають занадто багато про їхнє особисте життя. Крім того, майже 40% респондентів стурбовані тим, що вони відстежують використання пристроїв розумного будинку. Це свідчить про те, що споживачі відчувають неспокій, згадуючи розумні технології у своїх домівках, де вони бояться, що за ними спостерігають, слухають або відстежують. Ці проблеми споживачів можуть зашкодити подальшому зростанню ринку технологій розумного будинку.

Різні інциденти з пристроями розумного дому демонструють загальну відсутність кібербезпеки в розумних пристроях, включаючи пристрої розумного дому.

Хвилювання щодо IoT та пристроїв розумного дому супроводжуються попередженнями про конфіденційність та кібербезпеку. Останнім часом ми стикаємося з різними інцидентами, пов'язаними з погано захищеними пристроями IoT. У ЗМІ було багато уваги до атак DDoS, в яких розумні пристрої використовувалися для виконання атаки. Повідомлялося, що в 2017 році DDoS-атаки зросли на 91% через IoT.

Примітно, що ботнет Mirai використовував розумні пристрої для атаки DNS-провайдера Dyn та інших веб-сайтів у жовтні 2016 року. атака була здійснена завдяки взлому пристроїв IoT, включаючи маршрутизатори, IP-камери та цифрові відеозаписи, залишивши таким чином своїх користувачів в холоді.

Успішна атака на розумний будинок може призвести до неабияких наслідків, включаючи особисту шкоду, майновий збиток і чистий економічний збиток. Зовсім недавно з'явилося повідомлення про хакера, який віддалено підняв температуру в будинку з 12 градусами на розумному термостаті. Такий інцидент може призвести до тих же типів збитків, що перераховані вище, наприклад, до надмірного рахунку за опалення. У різних інцидентах брали участь дитячі монітори. Кілька разів повідомлялося, що розумний дитячий монітор був зламаний і використовувався для розмови з дитиною в її ліжечку. Також широко повідомлялося про російський сайт, який транслював в прямому ефірі кадри веб-камер, включаючи дитячі монітори. Інший недавній приклад включає в себе розумний динамік, який прослуховувався на користувачів без активації і завантаження звукових файлів на servers.виробника Ці типи інцидентів явно включають в себе шкоду конфіденційності і цілосності.

Різні демонстрації білих хакерів і компаній, які спеціалізуються на кібербезпеці показують, що в пристроях розумного дому на даний час відсутня базова кібербезпека. Очікується, що найближчими роками споживчий ринок

IoT зросте, тому ймовірність зловживань також зростатиме. Тому цілком імовірно, що ми зіштовхнемося з великою кількістю інцидентів, пов'язаних із приватною шкодою.

1.3 Система розумний будинок

Розумний будинок є частиною IoT. Тому всі пристрої розумного дому є пристроями IoT; вони є підвидом. Розумний дім можна визначити як «житло, що включає в себе ряд сенсорних систем і пристроїв, до яких можна віддалено отримати доступ, керувати та відстежувати через комунікаційну мережу». Або, простіше кажучи, будинок стає «розумним», коли його власник або мешканець використовує в ньому пристрої IoT. Сфери застосування розумного дому зазвичай класифікуються як такі, що належать до сфери енергетики, безпеки, розваг та охорони здоров'я. До нього входять підключені до Інтернету прилади, освітлення, вимикачі, дверні замки, термостати та інші предмети, призначені для домашнього середовища. Розумний дім – це автоматизована система з управління і моніторингу всіх підсистем життєзабезпечення і безпеки (Рисунок 1.1).

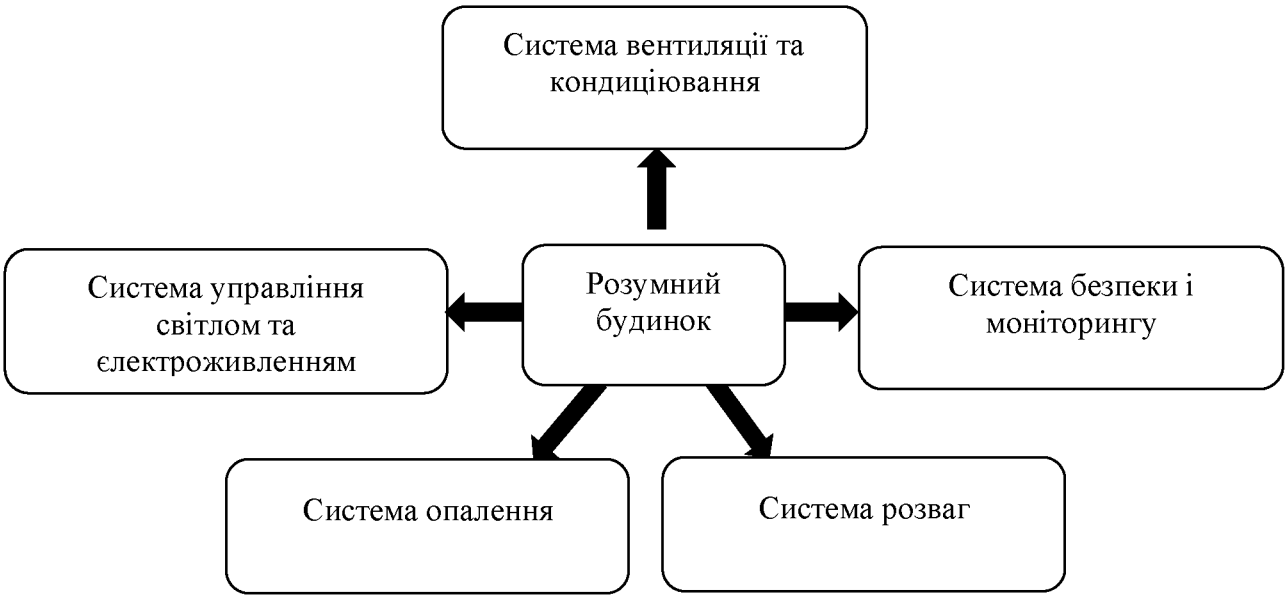


Рисунок. 1.1 – Підсистеми розумного будинку

1.4 Аналіз систем автоматизації розумного будинку

Системи автоматизації розумного дому класифікуються за такими ознаками:

– Централізовані, децентралізовані або комбіновані;
– З відкритим протоколом або з закритим протоколом;
– Дротові або бездротові технології

Ці три параметри можуть утворювати комбінації між собою. Наприклад, «бездротовий централізований розумний будинок з закритим протоколом» або «дротовий децентралізований розумний будинок з відкритим протоколом» тощо.

1.4.1 Централізовані системи автоматизації

Централізована автоматична система має програмований логічний модуль. Пристрій обладнано великою кількістю датчиків, з яких надходить інформація. Модуль аналізує отримані дані та надсилає команди елементам управління. До кожного підключеного об'єкта пишеться конкретна програма. При необхідності у встановлений софт можна вносити коригування.

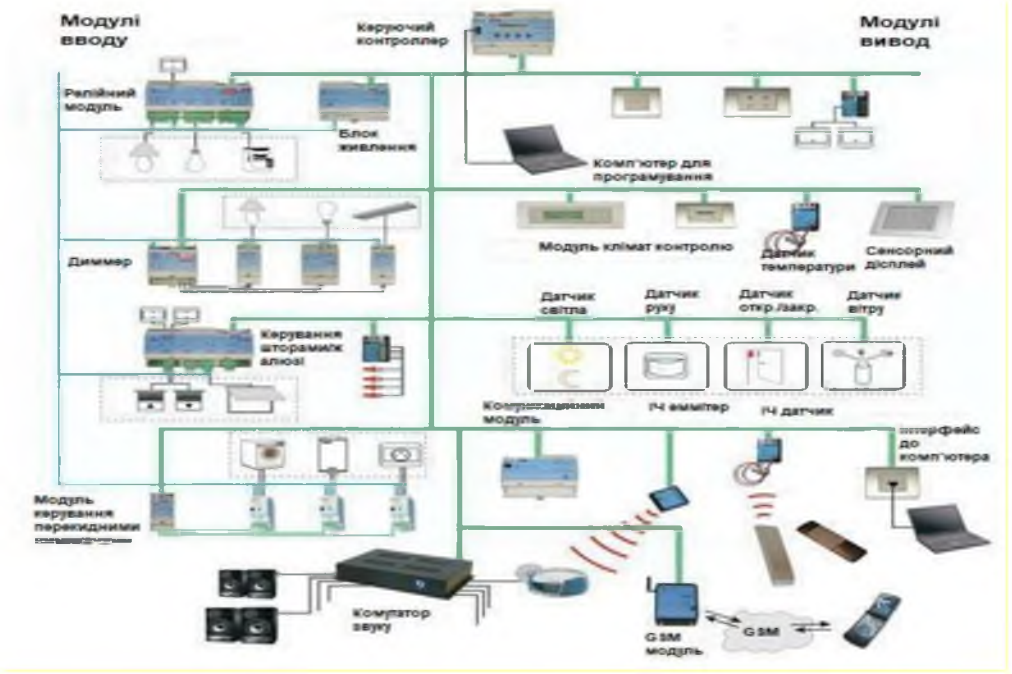


Рисунок 1.2 – Схема централізованої системи розумного будинку

Переваги:

– Універсальність – до системи можна підключити будь-які пристрої, навіть від різних виробників;

– Єдиний інтерфейс – керувати всіма об'єктами можна за допомогою одного інтерфейсу;
– Програмування – за допомогою контрольованого модуля можна створювати різні за складністю сценарії керування. При цьому їх можна прив'язувати до певної пори року або доби, а також погодних умов

Недоліки:

– Висока вразливість – оскільки робота централізованої системи залежить від логічного модуля, вихід контролера з ладу призведе до зупинки роботи технології «Розумний будинок»;
– Складність перепрограмування – якщо потрібне перепрограмування, а необхідний спеціаліст буде недоступний, то доведеться писати новий алгоритм. Тому слід купувати лише якісне обладнання

1.4.2 Децентралізовані системи автоматизації

Управління датчиками здійснюється за допомогою великої кількості контролерів. Кожен модуль підключається до конкретного елемента. При цьому контролер має автономне живлення, а значить може продовжувати працювати навіть при поломці центрального комп'ютера. Крім того, модуль зберігає інформацію про управління.

Переваги:

– Надійність – можливість автономної роботи підвищує надійність роботи технології;
– Функціональність – технологія дозволяє в разі потреби встановлювати додаткові контролери та розширювати функціональність;
– Зручність – автономні датчики, що закріплені на певному пристрої, дозволяють керувати великою кількістю механізмів

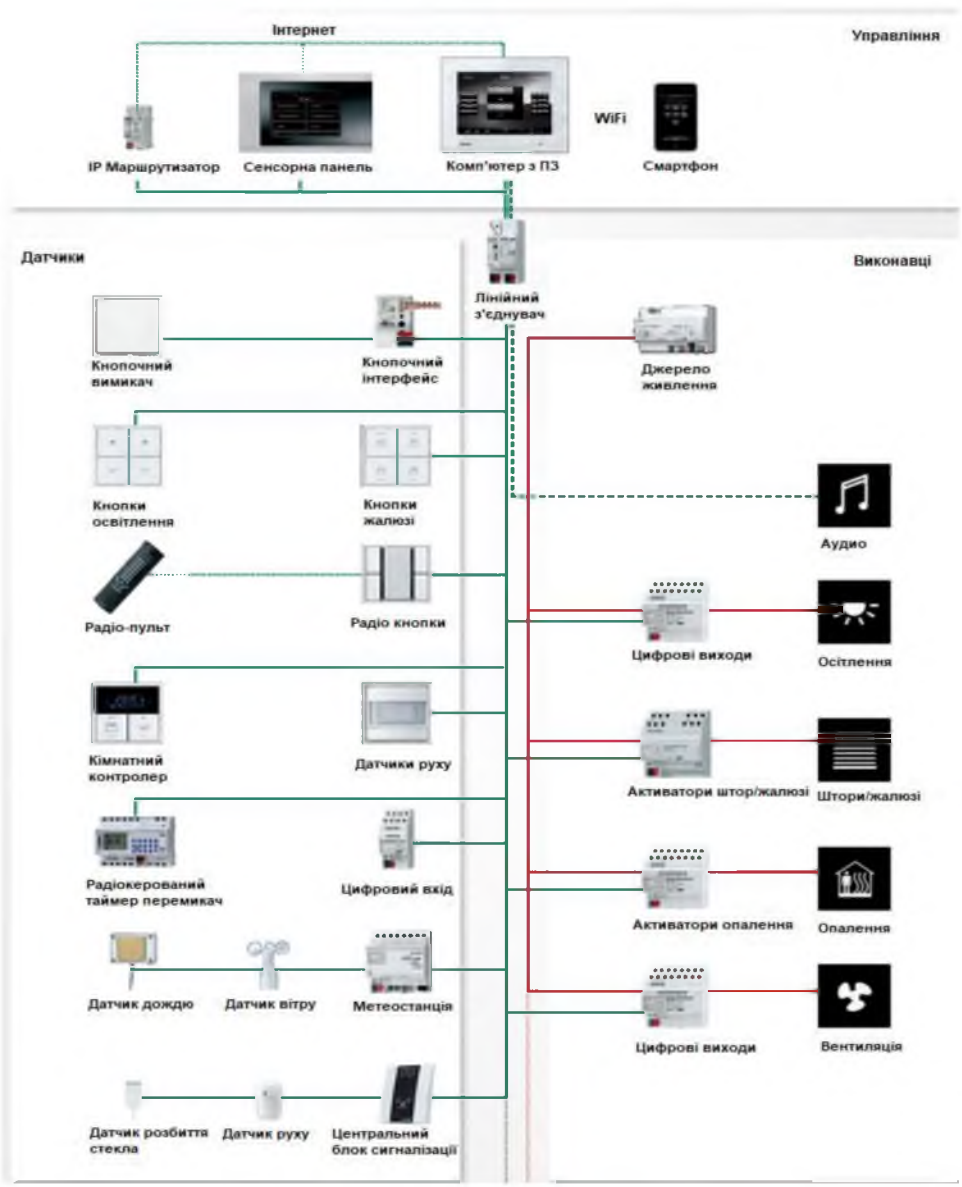


Рисунок 1.3 – Схема децентралізованої системи розумного будинку

Недоліки:

– Відсутність єдиної інформаційної мережі – це ускладнює проведення діагностики. Щоб це зробити, потрібно вивчати всю мережу або використовувати спеціальні прилади;
– Велика кількість модулів – великі витрати на покупку або ремонт модулів

1.4.3 Комбіновані системи автоматизації

Комбінована технологія поєднує в собі централізовану та децентралізовану системи. Зазвичай в даній системі є центральним контролер,

який приймає всі рішення, і кілька датчиків. Саме за такою схемою працює більшість розумних домів.

Технологія поєднала два типи, взявши від них найкраще. Це робить її практичною та функціональною, адже вона дозволяє стежити за роботою кожного датчика. При цьому налагодження кожної підсистеми дуже просте.

1.5 Поширені вразливості кібербезпеки в розумних пристроях

В екосистемі IoT можна виявити низку вразливостей безпеки. Проблеми кібербезпеки існують і виникають на всіх різних транспортних рівнях комунікаційної моделі.

Вразливості безпеки взяті з 10 найбільших недоліків безпеки в IoT за проектом безпеки відкритих веб-додатків (OWASP). Ця десятка стосується всіх пристроїв IoT і включає, пристрої розумного дому. Усі чотири можна (принаймні частково) віднести до виробників пристроїв. Припущення полягає в тому, що вжиття заходів проти цих поширених вразливостей кібербезпеки належить до основних методів кібербезпеки, яких можна очікувати від виробників пристроїв розумного дому. Будуть розглянуті чотири такі вразливості кібербезпеки:

1. Вразливості програмного/прошивного програмного забезпечення;

2. Недостатня аутентифікація/авторизація;

3. Відсутність транспортного шифрування;

4. Відсутність захищенних каналів зв’язку

Вразливості стосуються переважно програмних компонентів розумних пристроїв.

1.5.1 Вразливості програмного/прошивного програмного забезпечення

Пристрій розумного дому складається з двох основних компонентів: апаратного та програмного/прошивного. Перший відноситься до фізичних

елементів, з яких складається пристрій. Програмне забезпечення, — це набір інструкцій або програм, які інструктують комп'ютер виконувати конкретні завдання; це назва для всіх комп'ютерних програм, які запускаються на апаратному забезпеченні. Мікропрограмне забезпечення — це тип програмного забезпечення, яке напівпостійно записане на апаратному забезпеченні і яке є критичним для функціонування пристрою або окремої частини апаратного забезпечення. Загальновизнано, що неможливо створити програмне забезпечення, яке є на 100% безпечним або повністю вільним від помилок. Відомі вразливості програмного забезпечення («помилки») можуть бути використані, а невідомі уразливості можуть бути виявлені. Вразливість програмного забезпечення часто можна виправити за допомогою оновлення програмного забезпечення. Тому наявність безпечного програмного забезпечення є постійним процесом, який триває протягом усього життєвого циклу програмного забезпечення. По-перше, важливо з самого початку оснастити пристрої сучасним програмним забезпеченням, тобто в момент, коли пристрій виходить із заводу. По-друге, важливо мати безпечний механізм оновлення.

Наявність такого механізму оновлення гарантує, що оновлення безпеки ввімкнено. Захист такого механізму передбачає шифрування як з'єднання, через яке завантажується оновлення, так і шифрування самих файлів оновлень, щоб сторонні особи не могли перехоплювати та змінювати ці файли або виконувати власні оновлення (наприклад, інсталювати шкідливе програмне забезпечення на пристрої).

Інші заходи безпеки включають забезпечення безпеки сервера оновлень, відсутність доступу до конфіденційних даних, автентифікацію файлу оновлення перед його застосуванням безпечне перезавантаження пристрою.

Слід зазначити, що не всі вразливості програмного забезпечення можна виправити за допомогою оновлення програмного забезпечення, навіть за

наявності механізму оновлення. Деякі вразливості програмного забезпечення вимагають заміни апаратного забезпечення, що є набагато більш громіздким завданням, ніж випуск програмного виправлення. Крім того, оновлення програмного забезпечення можуть негативно вплинути на продуктивність пристрою. Це стало очевидним після нещодавніх наслідків помилок безпеки Spectre та Meltdown, пов'язаних із комп'ютерними чіпами, коли керівник Microsoft заявив, що за деяких обставин підвищення безпеки не переважить втрати продуктивності, спричинені виправленням програмного забезпечення.

Іншим побічним ефектом є те, що оновлення безпеки часто поєднуються з оновленнями функцій (змінами функціональності) у так званих пакетах оновлень, тоді як ці зміни функціональності можуть бути небажаними для споживача.

Незалежно від точного вирішення проблеми вразливостей та оновлень програмного забезпечення, програмне забезпечення в пристроях IoT часто відсутнє у всіх згаданих вище сферах. По-перше, пристрої IoT часто поставляються з заводу з уже застарілим програмним забезпеченням. Це означає, що програмне забезпечення містить багато відомих уразливостей, які можна використовувати, як тільки пристрій буде вперше підключено до Інтернету. З цієї причини важливо, щоб оновлення безпеки було реалізовано під час першої конфігурації пристрою в домі користувача. По-друге, пристрої IoT можуть не мати відповідного механізму оновлення для виправлення вразливостей. Механізму оновлення може взагалі не бути, або механізм оновлення небезпечний.

Це проблематично в IoT, особливо для пристроїв із тривалим життєвим циклом, тобто пристроїв, які не часто замінюються. Дослідження HP щодо безпеки популярних пристроїв IoT показало, що 60% пристроїв не використовували безпечне з'єднання для завантаження оновлень або не шифрували файли оновлень.

Небезпечне програмне забезпечення в розумних пристроях створює загрозу кібербезпеці. Можна розрізнити внутрішні та зовнішні загрози. Внутрішні загрози – це вразливості програмного забезпечення, які самі по собі можуть викликати інцидент безпеки. Наприклад, помилка програмного забезпечення в розумному термостаті може призвести до розрядження батареї та повного вимкнення пристрою, що відіграє в будинку холодок. Цей інцидент безпеки не виникає через зовнішнього зловмисника, який використовує вразливість програмного забезпечення/прошивки. Скоріше, була внутрішня помилка в програмному забезпеченні термостата, яка спричинила цей інцидент. Зовнішні загрози пов'язані з третіми сторонами, які використовують уразливість програмного забезпечення. Наприклад, злодій зламав розумний замок, щоб отримати доступ до помешкання. Точні загрози, які випливають із вразливості програмного забезпечення, залежать від обставин справи. Як правило, небезпечне програмне забезпечення/програмне забезпечення може призвести до несанкціонованого доступу або неправильного використання особистих даних, несанкціонованого контролю над пристроєм або атаки на інші системи (наприклад, через атаки DDos).

1.5.2 Недостатня аутентифікація/авторизація

Другим недоліком кібербезпеки є недостатня аутентифікація та/або авторизація. Аутентифікація в контексті обчислювальної техніки означає «процес або дію перевірки особистості користувача чи процесу». Іншими словами, це процес ідентифікації користувача, як правило, за логіном користувача та паролем. У контексті обчислювальної техніки авторизація відноситься до процесу надання доступу користувачеві на основі його особистості. Загалом, недостатня аутентифікація або авторизація як недолік безпеки означає, що процеси ідентифікації користувача та дозволу доступу до системи є небезпечними.

Управління компонентами системи розумного дому має вестись тільки після аутентифікації користувача в системі та його подальшої авторизації. Зважаючи на те, що управління системою розумного дому часто керується зі смартфона або іншого портативного пристрою, що з'єднується з системою розумного дому за допомогою бездротового зв'язку, виникає загроза перехоплення ідентифікаційних та (або) аутентифікаційних даних третіми особами. Перехоплення може бути реалізовано через впровадження шкідливого ПЗ у пристрої розумного дому, використання існуючих вразливостей програмного забезпечення пристроїв, прослуховування каналу зв'язку керуючого пристрою (наприклад, смартфона користувача системи) з пристроями розумного дому.

Відсутність механізму аутентифікації санкціонованого користувача у більшості пристроїв розумного дому, підтверджується існуванням ПЗ, за допомогою якого можна отримати несанкціонований доступ до пристроїв розумного дому. Прикладами таких програмних засобів є Shodan та Censys.

На практиці важливим і легко досяжним рішенням безпеки є безпечне керування паролями. Це включає в себе те, що надійні паролі є технічно можливими та необхідними. Це також означає наявність унікальних імен користувачів і паролів за замовчуванням або вимогу користувачам змінювати їх під час налаштування пристрою, а також відсутність облікових записів адміністратора, якими можна легко скористатися. Крім того, він включає в себе інші функції, такі як забезпечення безпечних механізмів відновлення пароля, захищене зберігання облікових даних, забезпечення детального контролю доступу, де це необхідно, впровадження двофакторної аутентифікації, де це можливо, тощо. Політика надійних паролів також може включати підказки про періодичне оновлення паролів, хоча ця практика обговорюється. Згідно з дослідженнями, змушування людей регулярно змінювати паролі призводить до передбачуваних моделей і варіацій одних і тих самих паролів. Було математично продемонстровано, що незручності для

користувачів через періодичну зміну паролів не переважують переваги безпеки. Ця дискусія демонструє динамічну природу передових методів кібербезпеки. Пристрої IoT, включаючи пристрої розумного дому, відомі тим, що мають слабкі паролі (за замовчуванням), наприклад «1234». Кілька звітів підтверджують, що слабкі паролі є серйозним недоліком безпеки в Інтернеті речей.

У дослідженні 2015 року з оглядом найпопулярніших пристроїв Інтернету речей, включаючи розумні термостати та розумні замки, комп'ютерна компанія HP виявила, що 80% пристроїв (разом із компонентами хмари та мобільних додатків) не вимагають паролів достатньої складності та довжини. Інше дослідження 2015 року, яке спеціально розглядало безпеку радіонянь, також визначило слабкі паролі за замовчуванням локальних облікових записів як загальний недолік безпеки. Згідно зі звітом Semantic за червень 2017 року, паролі за замовчуванням залишаються найбільшою слабкістю безпеки для пристроїв IoT. Помітним прикладом інциденту безпеки, пов'язаного з використанням слабких паролів, є ботнет Mirai. Він отримував доступ до 400 000 пристроїв IoT і використовував їх ("згрупований") за допомогою 61 поширеної комбінації імені користувача та пароля, наприклад admin-admin або admin-1234. Ботнет Mirai використовувався для запуску різних розподілених атак відмови в обслуговуванні (DDoS) на веб-сайти, шляхом безпосередньої атаки на веб-сайт або шляхом націлювання на DNS або постачальника хостингу. Атаки призвели до тимчасової недоступності цих веб-сайтів, зокрема Spotify, Twitter та Paypal. Інші помітні інциденти безпеки, які, ймовірно, були викликані слабкими (за замовчуванням) паролями, включають злом радіонянь, у результаті чого відеоканали були розміщені в Інтернеті, або коли неавторизовані особи використовували динаміки, щоб кричати на дитину. Інші зареєстровані інциденти включають отримання контролю доступу до всього розумного будинку через повну відсутність захисту паролем системи домашньої автоматизації.

Ці приклади показують деякі з можливих наслідків слабкого керування паролями або недостатньої аутентифікації/авторизації в більш широкому плані. Згідно з OWASP, недостатня аутентифікація та авторизація можуть призвести до «втрати даних або пошкодження даних, відсутності відповідальності або відмови у доступі та можуть призвести до повної скомпрометації пристрою та/або облікових записів користувачів.

1.5.3 Відсутність транспортного шифрування

Третя вразливість кібербезпеки в розумних пристроях – це відсутність транспортного шифрування. Іншими словами, це процес, який робить інформацію нерозбірливою для ненавмисних одержувачів. В електронних комунікаціях однією з основних функцій шифрування є збереження конфіденційності інформації. Іншим є аутентифікація інформації; встановлення джерела інформації та забезпечення того, щоб інформація не була підроблена.

Шифрування інформації досягається шляхом перекладу зрозумілої (відкритого тексту) фрази в незрозумілу (шифротекст), яку можна розшифрувати за допомогою ключа шифрування, який спільно використовували довірений (автентифікований) відправник і одержувач. Це можна зробити різними криптографічними методами, такими як симетрична криптографія або криптографія з відкритим ключем.

Коли пристрій IoT передає незашифровані дані, вони можуть бути перехоплені у вигляді простого тексту під час передачі по локальній мережі чи Інтернету, що означає, що інформація є зрозумілою для всіх. Це особливо проблематично, якщо це стосується конфіденційної (особистої) інформації або, наприклад, комбінацій імені користувача та пароля.

В пристроях IoT часто не вистачає транспортного шифрування, коли дані передаються в локальну мережу. Це робить інформацію вразливою для перехоплення будь-ким у зоні дії локальної мережі. У дослідженні пристроїв

Інтернету речей, проведеному HP у 2015 році, одним з основних висновків було те, що більшість пристроїв – 70 відсотків – не шифрували дані, які передавались у локальну мережу чи Інтернет. Ускладнюючим фактором реалізації транспортного шифрування в пристроях IoT є те, що деякі пристрої мають обмежені ресурси, тобто вони мають обмежену потужність обробки та пам'ять. Залежно від точних характеристик пристрою, деякі криптографічні рішення будуть неможливими. Тому легкі механізми шифрування мають першорядне значення для захисту IT-пристроїв. Наприклад, BITAG закликає виробників пристроїв використовувати захист транспортного рівня (TLS) або легку криптографію (LWC) для забезпечення транспортного шифрування. Відсутність транспортного шифрування, очевидно, є загрозою для конфіденційності (особистої) інформації під час передачі. Дані можуть бути перехоплені та потрапити в руки неавторизованих осіб (наприклад, атака «людина в середині»), і якщо критична інформація, як-от імена користувачів та паролі, буде перехоплена, весь пристрій або обліковий запис може бути зламано.

1.5.4 Відсутність захищенних каналів зв'язку

Використання симетричних криптографічних систем, дистанційне керування пристроями розумного дому, оновлення ПЗ пристроїв, переважне використання бездротового зв'язку для комунікації пристроїв один з одним – все це вимагає наявності захищених каналів зв'язку в системі розумного дому. Погана реалізація протоколів захисту на одному з пристроїв може призвести до компрометації всіх даних, що циркулюють в системі. Так, каналам зв'язку властиві такі основні вразливості:

- Канал Bluetooth є вкрай ненадійним і легко може прийняти файл із вірусом від зловмисника, не попросивши автентифікаційних даних;
- По каналу Wi-Fi зловмисник може авторизуватися у внутрішній мережі Wi-Fi та встановити шкідливе ПЗ;

- Вразливості HTTP-каналу, за яким пристрої із системи «Розумний дім» комунікують із зовнішньою мережею Інтернет, добре вивчені і можуть дозволити зловмиснику отримати контроль над розумним будинком, навіть не перебуваючи у його локальній обчислювальній мережі;
- Через канал GSM зловмисник може відправити керуючі команди «Розумний будинок», підмінивши свій номер номером санкціонованого користувача;

1.6 Причини відсутності кібербезпеки в розумних пристроях

Існує чотири основні причини слабкості або відсутності кібербезпеки у пристроях розумного дому.

По-перше, властиві обмеження деяких розумних пристроїв з точки зору ресурсів та інтерфейсів. Розумні пристрої розроблені з компромісом між розміром, потужністю ваги, пам'яттю, потужністю обробки та ціною. У результаті деякі розумні пристрої оснащені обмеженим апаратним забезпеченням, що означає, що вони мають малу обчислювальну потужність і пам'ять, що не дозволяє використовувати певні рішення безпеки. За даними ENISA, більшість розумних пристроїв мають дуже обмежені можливості. Прикладом може бути те, що розумний замок не має можливості використовувати механізми шифрування. Обмежені або неіснуючі інтерфейси в розумних пристроях обмежують його функціональність і ускладнюють, наприклад, змінити пароль або вимкнути віддалені служби.

Другою причиною відсутності кібербезпеки в розумних пристроях є відсутність технічних знань та інтерес до кібербезпеки з боку споживача. Кінцеві користувачі часто не знають про ризики кібербезпеки. Якщо так, то їм, швидше за все, не вистачає технічних знань, щоб захистити себе. Вплив споживача на рівень кібербезпеки залежить від конструкції розумного пристрою.

Якщо розумний пристрій покладається на кінцевого користувача, щоб забезпечити рівень кібербезпеки, це може виявитися слабким місцем. Наприклад, довірити споживачам завдання змінити слабкі паролі за замовчуванням (наприклад, 0000 або 1234) або завантажити та встановити оновлення програмного забезпечення. Також можна розробити банку для розумного пристрою з меншою залежністю від споживача, напр. за допомогою надійних паролів за замовчуванням та використання механізмів автоматичного оновлення. Можна сказати, що чим менше впливає користувач на рівень кібербезпеки, тим більшу відповідальність несе виробник смарт-пристрою за кібербезпеку в розумному пристрої.

Третя причина відсутності кібербезпеки – відсутність технічних знань і стимулів для підвищення кібербезпеки на стороні виробника пристрою. Часто традиційні розробники продуктів додають програмне забезпечення та підключення до свого існуючого портфоліо продуктів, не звертаючи особливої уваги на кібербезпеку. Вони не мають попереднього досвіду в питаннях конфіденційності чи безпеки, а отже, їм не вистачає досвіду в цих галузях, які є вирішальними для проектування та підтримки безпечних розумних пристроїв. По-друге, у виробників розумних пристроїв бракує стимулів для підвищення кібербезпеки своїх пристроїв. По суті, ринок надає перевагу функціям і низьким витратам, а не безпеці.

Сфера економіки кібербезпеки дає уявлення про цю проблему. Ця область дослідження вивчає стимули, які мають гравці ринку, щоб запровадити хорошу, погану або не запровадити кібербезпеку взагалі. Відсутність кібербезпеки вказує на провал ринку (наприклад, асиметрія інформації, негативні зовнішні ефекти та моральний ризик), що означає, що ринок не карає виробників за те, що вони випускають на ринок продукти з поганою кібербезпекою. В результаті виробники спонукаються підтримувати низькі витрати, не інвестувати в заходи кібербезпеки і якомога швидше просувати продукцію на ринок, щоб отримати конкурентну перевагу. Цю

ринкову недостатність можна було б подолати різними заходами, у тому числі юридичними рішеннями.

Четвертою причиною є те що багато пристроїв розумного дому встановлюється від різних виробників. Кожна компанія-виробник розробляє пристрій свого власного технологічного процесу з можливим використанням внутрішніх (нестандартизованих) протоколів обміну даними. З огляду на це впровадження пристроїв від різних виробників до системи розумного дому тягне за собою потенційну наявність вразливостей інформаційної безпеки Наприклад, некоректна реалізація захищеного з'єднання між двома пристроями може призвести до перехоплення зловмисником конфіденційної інформації.

1.7 Аналіз існуючих методів забезпечення кібербезпеки в системі розумного будинку

– Технологія Blockchain

Запропонована архітектура для захисту даних на основі блокчейну для систем розумного дому надає наступні рішення для мінімізації проблем конфіденційності, цілісності та аутентифікації:

Алгоритм шифрування SHA2 використовується для вирішення проблем конфіденційності та аутентифікації, які виникають у системі розумного дому.

Крім того, технологія блокчейн використовується для підтримки цілісності даних, що зберігаються на шлюзі. Алгоритм перетворення даних реалізований в архітектурі шляхом ефективного формування необроблених даних.

Основним недоліком мережевої архітектурі, що складена на основі блокчейн є те, що така має певні обмеження в командах, які мають додаткову обчислювальну складність за рахунок роботи блокчейну.

– Метод забезпечення конфіденційності аналізу даних

Цей метод має три модулі для захисту конфіденційності аналізу даних для систем розумних будинків.

Перший, модуль збору даних – збирає дані з встановленних у розумному будинку датчиків та надсилає їх до модуля приймача.

Цей модуль перетворює та зберігає їх дані у двох різних наборах даних.

Третій, модуль результатів – забезпечує контроль доступу до результатів обробки даних.

Перевагою цього методу є те що він забезпечує доступ лише аутентифікованому корисутвачеві та завдяки двом наборам даних неможливо пов'язати дані користувачів один з одним.

Недоліком є те що, в цьому методі відсутнє забезпечення конфіденційності, коли корисутвач передає дані постачальнику послуг, і це є основю вразливістю данного методу.

– Метод обмеження на рівні мережі

Метод обмеження на рівні мережі забезпечує захист IoT пристроїв. Коли до мережі підключається новий пристрій, то адміністратор, користувач мережі або інтернет провайдер може запитувати метод захисту від постачальника SaaS.

Перевагою цього методу є те, що воно зменшує навантаження на кінцевих користувачів і дозволяє забезпечити безпеку як послугу накладення інтернет провайдером або спеціалізованим постачальником в хмарі.

Недоліком є те, що цей метод має велику вразливість перед атаками, які здійснені зі смартфонів користувачів.

1.8 Постановка задачі

Технологія розумного дому з кожним роком набирає популярність серед користувачів. Функціонал який пропонує домашня автоматизація вражає своєю інноваційністю – керування кліматом, освіщенням, можливість спростити побутові задачі тощо.

Та попри це питання забезпечення кібербезпеки у розумному домі стоїть досить гостро – можна виділити два основних типа вразливостей надмірні дозволи та небезпечні повідомлення.

Щодо надмірних дозволів або прав, часто, близько половини встановлених додатків мають доступ до набагато більшої кількості даних та можливостей, ніж це необхідно. Крім того, при взаємодії з фізичними пристроями програми обмінюваються повідомленнями, які містять конфіденційні відомості.

Додаток для контролю рівня заряду автоматичного замку може отримувати ще й PIN-код для його розблокування. Програмне забезпечення деяких розумних пристроїв генерує повідомлення, схожі на реальні сигнали від фізичних пристроїв. Такий підхід дає зловмисникам можливість передавати до мережі недостовірну інформацію. В результаті користувач, наприклад, може бути впевнений, що двері заблоковані, а вони насправді відчинені. Такий підхід дає зловмисникам можливість передавати до мережі недостовірну інформацію.

Крім надмірних дозволів і небезпечних повідомлень є ще одна істотна проблема – передача конфіденційної інформації на сервери компаній, що займаються технічною підтримкою цих пристроїв. Тобто гаджети «стежать» за своїми господарями, щохвилини надсилаючи інформацію про їхню взаємодію з пристроями на сервер. Завдяки цій інформації можна відновити точний розпорядок дня мешканців.

Також окремо можно виділити бєкдор вразливості – часто розробники залишають собі «чорний хід», який дозволяє отримати повний доступ або контроль над пристроєм. Виробники виправдовуються необхідністю надавати технічну підтримку користувачам, однак навмисне створення таких уразливостей суперечить практиці захисту інформації і є справжньою вразливістю. Багато хто з виробників компонентів розумного дому залишають для себе «чорний хід». Отже, це потенційна діра у безпеці всього розумного дому, до будь-яких пристроїв якого зловмисник має можливість підключитися.

Таким чином у данній роботі повинні бути реалізовані такі задачі:

- Аналіз основних вразливостей та загроз у системі розумного будинку;
- Аналіз рівня загроз використовуючи метод оцінки ризиків;
- Запропонувати методи підвищення кібербезпеки у розумному домі;
- Розробити метод забезпечення кібербезпеки у системі розумного дому;
- Обґрунтувати економічну доцільності розроблених методів

ВИСНОВКИ ДО РОЗДІЛУ І

У цьому розділі було розглянуто застосування Інтернету речей та розумного дому, наведені його основні підсистеми розумного дому. Також були проаналізовані системи автоматизації розумного будинку, наведені переваги та недоліки кожної з них.

Описані основні вразливості кібербезпеки в розумних пристроях, причини їх виникнення.

Проаналізовано існуючі методи забезпечення кібербезпеки в системі розумного будинку.

РОЗДІЛ 2. АНАЛІЗ ЗАГРОЗ І ВРАЗЛИВОСТЕЙ. МЕТОДИ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ У РОЗУМНОМУ ДОМІ

2.1 Аналіз основних вразливостей та загроз у системі розумного будинку

У цьому розділі будуть розглянуті та проаналізовані основні загрози та вразливості у системі розумного будинку, що порушують К, Ц, Д. Згідно даного аналізу буде виявлено найбільш небезпечні загрози.

Таблиця 2.1 – Аналіз основних вразливостей та загроз

Об'єкт атаки	**Вразливість**	**Наслідок**	**Що порушує**
1	**2**	**3**	**4**
Усі пристрої розумного будинку, які підключені до мережі інтернет	Надлишкові права та дозволи – пристрої розумного дому мають доступ до набагато більшої кількості даних і можливостей, ніж це необхідно	ПЗ пристроїв може генерувати повідомлення, подібні до реальних сигналів від фізичних пристроїв. Такий підхід дає зловмисникам можливість передавати до мережі недостовірну інформацію	К, Ц
Датчики	Дешеві та неякісні датчики	Дешеві та неякісні датчики можуть з затримкою реагувати на підозрілу активність в домі	К, Ц, Д
ПЗ	Неліцензійне або застаріле ПЗ	Помилки ПЗ	Д
Центральний сервер	Передача конфіденційної інформації на сервери компаній, що займаються технічною підтримкою пристроїв розумного дому	Пристрої «стежать» за своїми власниками, надсилаючи інформацію про їхню взаємодію з пристроями на сервер	К
	Слабкий захист мережі розумного будинку	Атака на центральний сервер може спричинити порушення К, Ц, Д	К, Ц, Д

Продовження таблиці 2.1

1	2	3	4
Розумний термостат	Програмна помилка в розумному термостаті	Розрядження акумулятора і повне відключення пристрою	Д
Розумний замок	Відсутність механізмів шифрування для шифрування трафіку, що проходить через інтернет	Можливість перехопити облікові дані для входу та персональних даних власників будинку використавши пошукову систему пристроїв, які підключені до інтернету – Shodan або використовуючи Bluetooth-сніффер	К, Ц
Розумна радіоняня	Слабкий пароль	Доступ до відеоканалу та підключення до радіоняні третьою особою	К
Розумні лампочки	Розумні лампочки мають доступ до домашньої мережі, де є пакети з різною конфіденційною інформацією	Витік данних	К
	Слабкий захист при "спілкуванні" лампочок один з одним у локальній мережі (наприклад, коли виробник обмежується тільки застосуванням шифрованогобездротового протоколу)	Можливість запустити в локальну мережу підроблене оновлення софту, яке охопить усі лампи. Таким чином зловисник отримає можливість підключати лампи до DDoS-атак	К, Ц, Д

Продовження таблиці 2.1

1	2	3	4
Розумна розетка	Використання тільки логіну та паролю для захисту сторінки з налаштуваннями; відсутність можливості поміняти авторизаційні дані – використання однакових паролів на більшості пристроїв компанії	Зловмисник може прочитати будь-які повідомлення або перехопити керування пристроєм для підключення до DDoS-атак	К, Ц, Д
Відеокамери	Простий чи застарілий механізм захисту	Взлом відеокамер для створення ботнет та подальше використання у DDoS-атаках	К, Ц, Д
	Слабкий пароль або незмінений мастер пароль від виробника		К, Ц, Д
	Відсутність шифрування при передачі данних при підключенні до відеокамери через «хмару»		К, Ц, Д

Продовження таблиці 2.1

2	3	4	5
Смарт ТВ	Слабкий захист у вбудованих у ТВ браузерів	Фішинг – можна підсунути користувачеві підроблені сторінки, збираючи паролі, інформацію про банківські картки та інші конфіденційні дані	К
	Передача данних через USB	Передача вірусів через флешку	К, Ц, Д
	Вбудована система розпізнавання голосу	Слова, сказані у присутності телевізора, можуть бути передані третій стороні	К
Захищені файли	Слабкий механізм розмежування доступу	Доступ до захищених файлів з використанням обхідного шляху	К, Ц
Апаратура та носії інформації	Незахищене зберігання	Крадіжка апаратури або носіїв інформації	К, Ц, Д
	Відсутність системи автономного електроживлення. Чутливість до перепадів напруги	Знищення апаратури або носіїв інформації	Д

У таблиці 2.1 присутні такі скорочення:

К – Конфіденційность; Ц – Цілісність; Д – Доступність.

Згідно аналізу, найбільшу загрозу представляють собою ті, що порушують К, Ц та Д:

– Дешеві та неякісні датчики;
– Слабкий захист мережі розумного будинку;

- Слабкий захист при "спілкуванні" лампочок один з одним у локальній мережі (наприклад, коли виробник обмежується тільки застосуванням шифрованого бездротового протоколу);
- Використання тільки логіну та паролю для захисту сторінки з налаштуваннями; відсутність можливості поміняти авторизаційні дані – використання однакових паролів на більшості пристроїв компанії;
- Простий чи застарілий механізм захисту;
- Слабкий пароль або незмінений мастер пароль від виробника;
- Відсутність шифрування при передачі данних при підключенні до відеокамери через «хмару»;
- Передача данних через USB;
- Незахищене зберігання

Далі, у цьому розділі буде запропоновано методи забезпечення конфіденційності, цілісності та доступності.

2.2 Аналіз рівня загроз

З таблиці 1 можна описати основні загрози для кожного об’єкту атаки та за допомогою методу оцінки ризиків, який використовує «Microsoft» оцінити:

- Вірогідність реалізації: висока – вірогідність реалізації загрози протягом року, середня – вірогідність реалізації загрози протягом 2-3 років, низька – малоймовірна;
- Вплив, який буде завданний, якщо загроза буде реалізована: високий, середній, низький;
- Вартість кожного ризику: висока, середня, низька

Для аналізу рівня загроз, необхідно розробити відповідну таблицю (таблиця 2.2), яка скадатиметься з загрози (що буде оцінюватися), об’єкту атаки (взято з таблиці 2.1), вірогідності, рівню впливу і вартості ризику.

Таблиця 2.2 – Аналіз рівня загроз

Загроза	**Об'єкт атаки**	**Вірогідність**	**Рівень впливу**	**Вартість ризику**
1	**2**	**3**	**4**	**5**
Перехоплення сигналу та передача недостовірної інформації у мережу	Усі пристрої розумного будинку, які підключені до мережі інтернет	Висока	Високий	Висока
Нереагування або невчасне реагування датчиків	Датчики	Середня	Високий	Висока
Некоректна робота ПЗ	ПЗ	Середня	Середній	Середня
Надсилання інформації про взаємодію користувача з пристроями на центральний сервер	Центральний сервер	Висока	Низький	Низька
Атака на центральний сервер		Висока	Високий	Висока
Непланове відключення або розряджання розумного термостату	Розумний термостат	Середня	Середній	Середня
Нелігитимний доступ до облікових даних для входу та персональних ланих користувачів	Розумний замок	Висока	Високий	Висока

Продовження таблиці 2.2

1	2	3	4	5
Нелігитимний доступ до відеоканалу	Розумна радіоняня	Середня	Середній	Середня
Витік конфіденційної інформації	Розумні лампочки	Середня	Високий	Висока
Впровадження шкідливого коду або програми		Середня	Високий	Висока
Використання пристроїв у ботнет	Розумні розетки	Низька	Високий	Висока
	Відеокамери	Середня	Високий	Висока
Неправомірне відключення спостереження		Середня	Середній	Середня
Несанкціонований доступ до відеоканалу		Середня	Низький	Низький
Фішингова атака	Смарт ТВ	Висока	Високий	Високий
Зараження ПЗ вірусами		Середня	Середній	Середня
Витік голосових повідомлень		Низька	Середній	Середня
Доступ до захищених файлів з використанням обхідного шляху	Захищені файли	Середня	Середня	Середня

Продовження таблиці 2.2

1	2	3	4	5
Крадіжка апаратури або носіїв інформації	Апаратура та носії інформації	Низька	Високий	Висока
Знищення апаратури або носіїв інформації		Низька	Високий	Висока

Згідно отриманих результатів оцінки ризиків, найнебезпечніші загрози це:

- Перехоплення сигналу та передача недостовірної інформації у мережу;
- Атака на центральний сервер;
- Нелігитимний доступ до облікових даних для входу та персональних даних користувачів;
- Фішингова атака

Також небезпечними є:

- Нереагування або невчасне реагування датчиків;
- Витік конфіденційної інформації;
- Впровадження шкідливого коду або програми;
- Використання пристроїв у ботнет

До фізичних загроз можна віднести пожежі, протікання, проникнення до будинку без дозволу власника, відключення електроживлення тощо.

2.3 Методи підвищення кібербезпеки у розумному домі

На основі проведеного аналізу необхідно застосувати такі захисні заходи:

- Встановлення паролю високої складності на профіль адміністратора системи;
- Оновлення ПЗ усіх пристроїв системи розумний будинок до останньої версії;
- Використання системи стеження за несанкціонованим доступом до розумного дому;
- Налаштування мережі VPN для системи;
- Встановлення міжмережевого екрану (файрвола) на межі локальної мережі розумного дому;
- Використання антивірусного ПЗ;
- Встановити систему контролю управління доступом;
- Регулярна перевірка справності всіх пристроїв розумного дому;
- Використання резервного джерела живлення

2.4 Розроблення методу забезпечення кібербезпеки у системі розумного дому

Згідно попередніх розділів, найкритичнішим для систем розумного дому є забезпечення конфіденційності даних. Тож у цьому розділі буде розглянуто як забезпечити захист додатку, з якого ведеться керування розумним домом.

Для забезпечення конфіденційності даних на пристрої має бути захищене сховище даних, яке може забезпечити безпечне читання та запис файлів.

Для кращого рівня безпеки має бути реалізовано шифрування файлів «на льоту», наприклад, при отриманні їх із сервера. Відомо, що протоколи передачі даних через мережу дроблять файли на пакети та передають їх. Принцип полягає в отриманні файлів частинами, по блоках. При цьому кожен наступний блок шифрується і зберігається в пам'яті пристрою. Це робиться для того, щоб у пам'яті пристрою дані не затримувалися на довгий час, і

шифрувалися відразу по мірою надходження. Схожий алгоритм працює при розшифрування файлу для його читання.

Блокове шифрування має бути послідовним, так як для відтворення медіа-контенту потрібно розшифровувати дані послідовно. Тож зашифрований файл має зберігатися на носії та перед використанням розшифровуватися в оперативну пам'ять. Далі файл буде зчитуватися і після цього видалятися з оперативної пам'яті.

Шифрування відбувається згідно такого алгоритму: при отриманні файлів весь файл спочатку записується в оперативну пам'ять, потім шифрується і записується в основну пам'ять, при ьому після шифрування файл видаляється з оперативної пам'яті.

Найбільш поширеними симетричними алгоритмами блокового шифрування даних є AES та DES.

Оскільки однією з умов є можливість зберігання даних на пристрої та їх використанні без наявності інтернету, необхідно розглядати симетричні алгоритми попереднього розподілу ключів, щоб пристрій міг розшифровувати дані без доступу до каналу передачі даних. Цю вразливість можна мінімізувати за допомогою схеми розподілу ключів Блома.

2.4.1 Схема розподілу ключів Блома

Суть схеми розподілу ключів Блома наступна: довірена сторона роздає кожному учаснику відкритий та закритий ключ. Далі всі учасники, обмінюються між собою тільки відкритими ключами по каналах зв'язку (які можуть бути незахищеними), а також можуть згенерувати секретний сеансовий ключ для спілкування між собою.

Спочатку відбувається ініціалізація – довірена сторона вибирає симетричну матрицю D розмірності k на k над кінцевим полем GF(p). Далі, коли новий учасник хоче приєднатися до системи (тобто з'являється новий

клієнт), довірена сторона обирає для нього новий відкритий ключ, який представляє собою вектор (стовпець) I розміру k. В якості довіреної сторони буде використан сервер зберігання даних клієнт-серверної архітектури.

Далі довірена сторона обчислює закритий ключ g = D * I. Потім відкритий та закритий ключ повідомляються учаснику по надійному каналу без можливості прослуховування.

Якщо клієнт і сервер хочуть встановити між собою секретний канал, вони посилають один одному по відкритому каналу свої відкриті ключі. Далі кожен з них множить свій закритий ключ на відкритий ключ іншої сторони.

$$S_A = (g^t_A I_B)^t = (I^t_A D I_B)t = I^t_B D I_A$$

$$S_B = (g^t_B I_A)^t = (I^t_B D I_A)t = I^t_A D I_B \qquad (2.1)$$

$$S_A = S_B$$

В результаті у них вийде одне і те ж число (це випливає із симетричності матриці D, яке і буде використовуватися як загальний сеансовий ключ). Далі – сеансовий ключ буде використаний для шифрування на стороні сервера та розшифровки на стороні клієнта. Іншими словами, одним із учасників завжди буде сервер зберігання даних, іншим – клієнт.

Надійність схеми безпосередньо залежить від розміру секретної матриці, яка використовується у схемі. Для відновлення секретної матриці (або, будь-якої, що виконує аналогічну функцію) необхідно мати число ключів, що дорівнює кількості рядків матриці.

В якості алгоритму шифрування було обрано реалізацію AES-CBC із довжиною ключа 256 біт.

Вразливим місцем цього алгоритму є обов'язковість наявності секретного каналу передачі для передачі відкритого та закритого ключа.

2.4.2 Аналіз симетричних протоколів розподілу ключів, що реалізують забезпечення конфіденційності

– Протокол Wide Mouth Frog

Frog – найпростіший протокол керування ключами. Він дозволяє двом абонентам встановити загальний сесійний ключ для захищеного спілкування між собою. У протоколі бере участь довірений центр.

Аліса хоче встановити сесійний ключ із Бобом. Вона починає, формуючи: K – випадковий сеансовий ключ, TA – мітку часу та відправляє Тренту (довіреному центру), додавши своє ім'я:

$$M0 = A, EA\ (TA, B, K) \tag{2.2}$$

Трент, використовуючи спільний з Алісою секретний ключ, розшифровує повідомлення та перевіряє правильність мітки часу TA та ідентифікатора Боба. Якщо все добре, він формує:

TB – нову мітку часу (яка може відрізнятись від TA) і відправляє Бобу.

$$M1 = EB\ (TB, A, K) \tag{2.3}$$

Боб отримує повідомлення, розшифровує його спільним з Трентом ключем і перевіряє мітку часу TA та ідентифікатор Аліси. Якщо повідомлення пройшло перевірку, то тепер Боб має спільний з Аліса ключ.

Недоліком цього протоколу є те, що він є досить тривіальним і має крипто-нестійкі точки.

– Протокол Нідхема-Шрьодера

Цей протокол є прикладом протоколу, який не залежить від міток часу і при цьому забезпечує вироблення та підтвердження ключа.

Ситуація перед початком роботи протоколу:

3 дійових особи (ідентифікатора): клієнти Аліса та Боб, які хочуть отримати ключ для спілкування між собою, Трент – довірений центр.

У Аліси та Боба є секретні ключі EA та EB відповідно спілкування з Трентом. Аліса вибирає число NA, Боб вибирає число NB.

Отже, Аліса запускає протокол, формує повідомлення, що складається зі свого і Боба ідентифікаторів, а так само обраного числа NA і відправляє його Тренту.

$$M0 = A, B, NA \tag{2.4}$$

Отримавши повідомлення від Аліси, Трент формує повідомлення, що складається з двох частин. В першу частину він кладе NA, ідентифікатор Боба, а також новий ключ K, який хочуть отримати Аліса та Боб. Друга частина повідомлення також містить новий ключ K і ще ідентифікатор Аліси, але при цьому вона зашифрована секретним ключем Трента та Боба EB. Все повідомлення шифрується секретним ключем Аліси та Трента EA і відсилається Алісі.

$$M1 = EA\ (NA, B, K, EB\ (K, A)) \tag{2.5}$$

Аліса розшифровує повідомлення. Знайшовши в повідомленні NA, вона переконується, що поговорила з Трентом. Другу частину, зашифровану EB, вона прочитати зовсім не здатна, тому пересилає її Бобові.

$$M2 = EB\ (K, A) \tag{2.6}$$

Боб отримує та розшифровує повідомлення, дістає звідти новий ключ K і формує повідомлення для Аліси, в якому повідомляє їй своє число NB, шифрований новим ключем.

$$M3 = EK\ (NB) \tag{2.7}$$

Аліса отримує повідомлення, дістає звідти NB змінює його і відправляє назад Бобу.

$$M4 = EK\ (NB - 1) \tag{2.8}$$

Аліса та Боб володіють спільним ключем K.

– Протокол Отвея-Рііса

Протокол Отвея-Рііса – протокол на симетричних ключах, що дозволяє розподіляти ключі, не використовуючи позначки часу.

Перед початком роботи протоколу маємо: довірений центр Трент, 2 користувача: Аліса та Боб, які отримали EA та EB. Аліса вибирає числа N та NA, Боб вибирає NB.

Аліса формує повідомлення для Боба, в якому відкритим текстом передає N, A, B, а також ті ж самі N, A, B з NA, зашифровані спільним з Трентом ключем EA.

$$M0 = N, A, B, EA(NA, N, A, B) \tag{2.9}$$

Боб отримує повідомлення, друга частина якого для нього не розшифровується, додає ще один рядок, який шифрує ключем EB та відправляє Тренту.

$$M1 = N, A, B, EA(NA, N, A, B), EB(NB, N, A,B) \tag{2.10}$$

Трент, знаючи обидва ключі, може розшифрувати повідомлення Аліси та Боба. Тепер його мета – підтверджувати, що він – Трент і сформувати ключ K для подальшого спілкування Аліси та Боба.

Трент генерує ключ K та посилає Бобу зі спілкування.

$$M3 = EA\ (NA, K), EB\ (NB, K) \tag{2.11}$$

Першу частину, зашифровану ключем Аліси, Боб розшифрувати не може, а другу частину він розшифровує та зчитавши NB, усвідомлюється, що повідомлення прийшло від Трента. Далі приймає згенерований ключ K. Тепер

Боб готовий до спілкування з Алісою, залишилося тільки діставити їй ключ. Боб відправляє Алісі першу частину повідомлення від Трента.

$$M4 = EA\ (NA,\ K) \tag{2.12}$$

Аліса приймає повідомлення, засвідчується, що воно від Трента (NA), та зчитує ключ K. Аліса та Боб готові до спілкування.

В результаті Боб впевнений, що поговорив із Трентом: Боб відправив йому число NB, шифроване секретним ключем EB, і отримав інше повідомлення, що містить те саме число і шифроване тим самим ключем.

Аліса також переконана, що Боб поговорив із Трентом, бо вона послала своє число NA, шифроване ключем EA, і отримала назад інше повідомлення, що при цьому теж містить NA і шифроване EA.

У Аліси та Боба з'явився спільний ключ K.

Недіолком цього протоколу є те, що Аліса ніяк не може бути певна, що Боб – це Боб. Вона лише впевнена, що спілкується з якоюсь особою, яка може ходити до Трента.

Щоб вирішити цю проблему на 4 кроці Боб може відправити Алісі не тільки EA(NA, K), але ще й, наприклад, EK (NA, NB), доводячи тим самим, що він знає ключ K. А Аліса в свою чергу може відповісти Бобу EK (NB), теж доводячи, що знає ключ K.

2.4.3 Симетричний протокол розподілу ключів Kerberos

Проаналізувавши протоколи розподілів ключів, був обраний протокол Kerberos, тому що він може забезпечити конфіденційність та цілісність одночасно та немає таких недоліків, як у тих що буди розглянуті у першлому розділі. Тому для аутентифікації на сервері (довіреній стороні) використовуватиметься Kerberos.

Протокол Kerberos – це розподілена система аутентифікації, яка дозволяє клієнту довести свою особистість серверу без надсилання даних по мережі. Kerberos за потреби забезпечує цілісність і конфіденційність даних, що передаються між клієнтом і сервером.

Перед початком роботи протоколу необхідно визначити 3 дійові особи (ідентифікатори): Аліса – клієнт, Боб - сервер, якому Аліса хоче довести свою справжність, Трент – довірений центр.

У Аліси та Боба є секретні ключі EA та EB відповідно для спілкування з Трентом. Аліса вибирає число NA, а так само встановлює мітку часу TA за своїм годинником. t – період валідності (lifetime), що обирається Трентом.

Потім Аліса, запускаючи протокол, у відкритому вигляді, передає Тренту свій ідентифікатор, ідентифікатор Боба і NA.

$$M0 = A, B, NA \tag{2.13}$$

Трент, отримавши повідомлення від Аліси, генерує ключ K для подальшого спілкування Аліси та Боба і передає назад Алісі повідомлення з двох частин: перша частина зашифрована секретним ключем Аліси і містить K, NA, період валідності t та ідентифікатор Боба; друга частина невідома Алісі – вона зашифрована секретним ключем Боба, і в ній міститься K, t та ідентифікатор Аліси.

$$M1 = EA\ (K, NA, t, B), EB\ (K, A, t) \tag{2.14}$$

Аліса розшифровує першу частину прийнявши того від Трента повідомлення, і отримавши ключ K, створює новий пакет для відправки Бобу, в який входять ідентифікатор Аліси, t та мітка часуTA.

Після цього Аліса надсилає Бобу повідомлення з двох частин: перша частина - це та, що прийшла від Трента, а друга – створена Алісою.

$$M2 = EB\ (K, A, t), EK(A, TA, t) \tag{2.15}$$

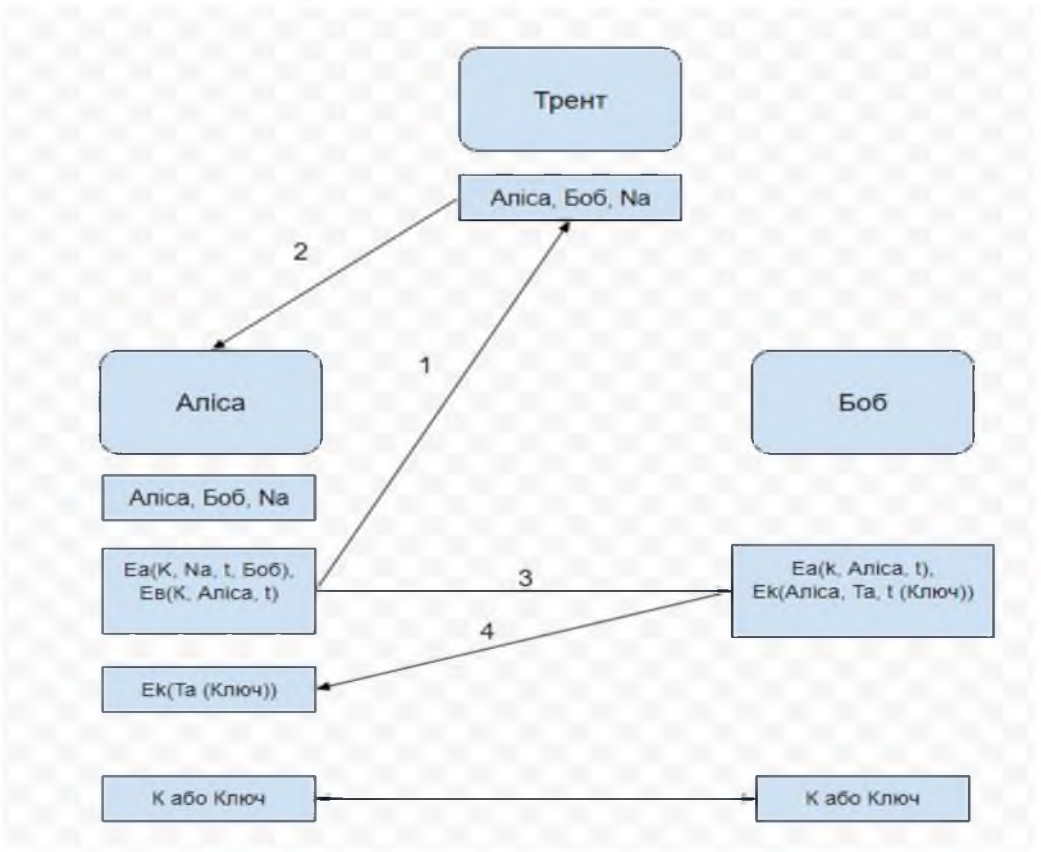
Боб приймає повідомлення. Розшифрувавши першу частину, він дістає новий ключ K, а потім, використовуючи його, розшифровує другу частину.

Щоб підтвердити Алісі, що він знає новий ключ K, Боб надсилає їй повідомлення з позначкою часу, зашифроване новим ключем K.

$$M3 = EK\ (TA) \tag{2.16}$$

Аліса засвідчує, що Боб – це Боб. Тут застосовні такі міркування: Боб міг розшифрувати повідомлення від Аліси з позначкою часу, тільки якщо він знав ключ K. А ключ K він міг дізнатися тільки якщо знає ЕВ. А оскільки це секретний ключ Боба і Трента, то надіслав повідомлення Алісі – Боб.

Далі, при використанні схеми Блома відкритий та закритий ключі передаються з використанням ключа K.



Рисинок 2.1 – Схема роботи протоколу Kerberos

2.4.4 Механізм шифрування та розшифровки

Шифрування та розшифрування будуть реалізовані з використанням бібліотеки "CryptoCommon".

Вибраний алгоритм – AES-256, тобто. Алгоритм AES із довжиною ключа 256 біт.

Також, можна зробити алгоритм більш гнучким, якщо використовувати замість «жорстко зашитих» у код чисел змінні шифрування, які час від часу змінюватимуться.

2.5 Вразливості протоколу Kerberos

Поєднання привілейованих облікових записів з атаками на аутентифікацію Kerberos в доменах Windows підвищує ризик взлому. Під час таких атак учасники загроз націлені на права адміністратора домену, які забезпечують необмежений доступ і контроль над системою. Маючи привілеї адміністратора, зловмисники можуть приховано маніпулювати контролерами домену і створювати квитки Kerberos для отримання несанкціонованого доступу.

Основними пробелмами протоколу Kerberos є доступ, неясність та постійність.

Доступ: як тільки зловмисник отримає привілеї локального адміністратора, можна отримати додаткові облікові дані, які, якщо їх залишити на зламаних машинах, дозволять зловмиснику переміщатися по мережі, підвищити привілеї та отримати несанкціонований доступ до цінних активів.

Неясність: щоб обійти контроль безпеки та уникнути виявлення, зловмисник може повторно використовувати квитки Kerberos, щоб видавати себе за авторизованих користувачів і обійти процеси аутентифікації, маскуючи активність та уникаючи слідів журналу аутентифікації.

Постійність: зловмисники часто воліють залишатися в мережі невиявленими протягом тривалого періоду часу, поступово відправляючи інформацію. Атаки Kerberos дають зловмисникам те, що їм найбільше потрібно для цього: час. За допомогою квитків Kerberos можна підтримувати стабільність, навіть якщо облікові дані були змінені.

Хоча існує кілька типів атак на протоколи аутентифікації, включаючи Pass-the-Hash, Overpass-the-Hash і Pass-the-Ticket, найбільш руйнівною з усіх є «золотий квиток».

Суть цієї атаки полягає в тому що якщо у зловмисника є доступ адміністратора/локального адміністратора до домену Active Directory, він можете маніпулювати квитками Kerberos, щоб отримати несанкціонований доступ. Атака «золотий квиток» — це атака, під час якої зловмисник створюєте квиток, який генерує Kerberos, який діє протягом 10 років. Зловмисник можете бути ким завгодно та за умови, що у нього є хеш, додавати будь-який обліковий запис до будь-якої групи (включаючи високопривілейовані групи) і робити що завгодно в межах можливостей автентифікації Kerberos. Зловмисника може створити придатні для використання квитки Kerberos для облікових записів користувачів/комп'ютерів/служб, яких не існує в Active Directory. Золотий квиток – це підроблений центр розповсюдження ключів Kerberos, яка порушує одночасно конфіденційність і цілісність.

Отже, у наступному розділі буде запропоновано модифікація Kerberos, яка допоможе підвищити рівень конфіденційності та цілісності.

2.6 Модифікація протоколу Kerberos

Модифікація протоколу Kerberos для генерації та розподілу ключової інформації в комп'ютерній мережі відрізняється тим, що в серверах TGS (Ticket Granting Server) обчислюються пакети ключової інформації, що

доставляють клієнтам із сервера додатків у складі посилок TGT (Ticket Granting Ticket).

Нехай є один або більше серверів автентифікації (AS) і, принаймні, така сама кількість серверів видачі квитків (TGS).

Кожен сервер TGS відповідає одному серверу AS. Кожен домен мережі зв'язується із сервером TGS та абоненти домену прив'язуються до цього TGS. Якщо сервер додатків NAS міститься в декількох доменах, він прив'язується до всіх TGS, що належать даним доменам. Усі абоненти мережі підтримують службу одноразових паролів OTPS (One-Time Password Service) з кількома AS, до яких прив'язані відповідні TGS.

Сервер програм NAS підтримує службу одноразових паролів однієї або більше OTPS. Абонент Ai та сервер автентифікації ASj з OTPS мають одноразовий пароль.

На етапі ініціалізації (Рисунок 2.2) кожен сервер ASj обчислює ключі для зв'язку з TGSt та прив'язаних до нього абонентів Ai, для зв'язку TGSt та прив'язаних до нього NASp. Припустимо, що кожен ASj має ключ зв'язку з прив'язаними до нього TGSt і кожен TGS будує KDP(P,F)-схему для відповідного домену мережі: кожному абоненту Ai чи NASp цього домену обчислюються пакети Si, Ss.

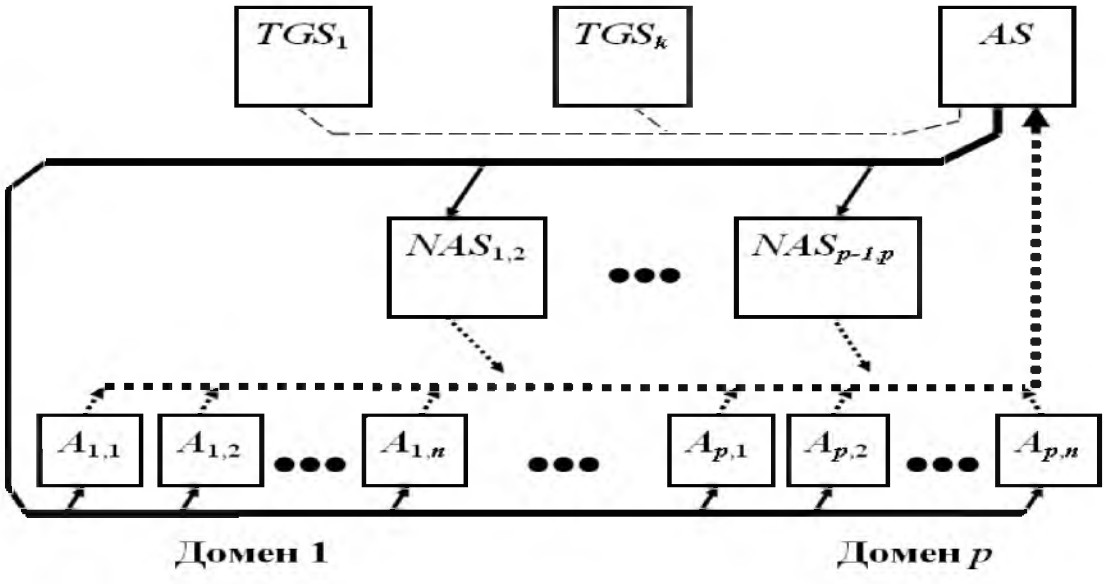


Рисунок 2.2 – Протокол обміну з сервером автентифікації з метою отримання дозволу на видачу ключової інформації

Тепер кожен учасник Ai, який підтримує службу одноразового пароля з відповідним сервером аутентифікації ASj, може отримати свій пакет Ki ключової інформації, ініціалізуючи та виконуючи протоколи:

- протокол обміну з сервером аутентифікації з метою отримання дозволу TGT на отримання ключової інформації (Рисунок 2.2);
- протокол обміну з сервером TGS з метою отримання ключової інформації (Рисунок 2.3);

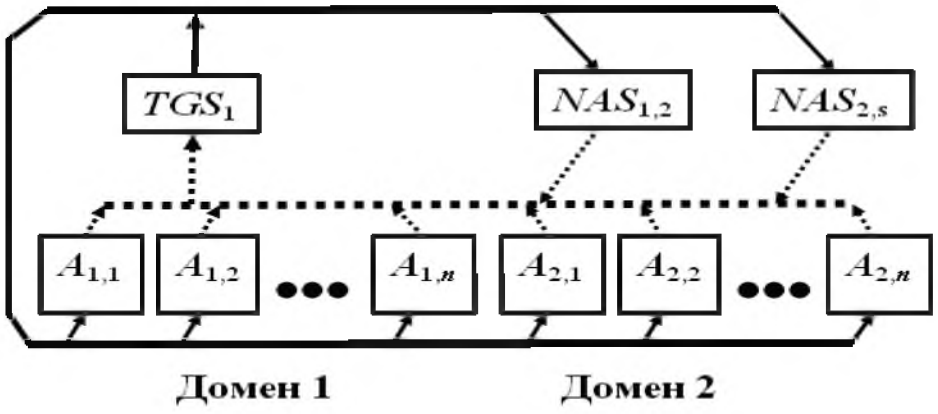


Рисунок 2.3 – Протокол обміну із сервером TGS з метою отримання ключового матеріалу абонентами мережі А та серверами додатків NAS

Для безпечного обміну інформацією між абонентами мережі використовується протокол комунікації абонентів мережі, зокрема через сервер додатків NAS (Рисунок 2.4).

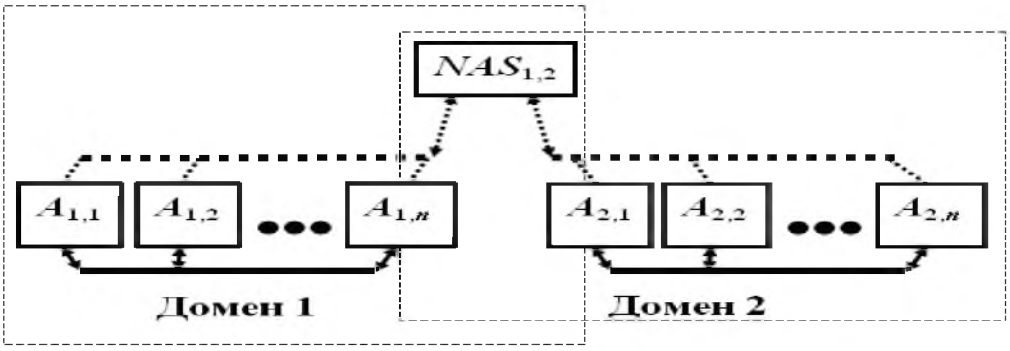


Рисунок 2.4 – Протокол комунікацій абонентів мереж

Дано оцінки ключової інформації, необхідної для організації захищених комунікацій, для мереж різних типів.

Дані, представлені в таблиці 2.3 показують переваги використання нецентралізованих 10KDP(1002, 56) та 10HAKDP(1002, 56, 10)-схем.

Таблиця 2.3 – Порівняльна таблиця нецентралізованих 10KDP(1002, 56) та централізованих 10HAKDP(1002, 56, 10)-схем

	Без попереднього розподілу	10KDP(1002, 56)	10HAKDP(1002, 56, 10)
Середня довжина пакета	1001	37	28
Число переданих ключів	10030020	370740	280560

З цієї таблиці видно, що у нецентралізованій мережі (KDP) порівняно з централізованою (HAKDP) число ключів, що пересилаються від ТА учасникам, скорочується. Застосування схем із хешуванням призводить до ще більшого скорочення середньої довжини пакетів ключової інформації та обсягу ключової інформації, що передається від довіреного центру ТА.

ВИСНОВКИ ДО РОЗДІЛУ II

У цьому розділі був проведений аналіз основних вразливостей та загроз у системі розумного будинку. Були проаналізовані рівні загроз та методи підвищення ІБ у системі розумного будинку.

Було розглянуто та реалізувано масштабовану систему, що розрахована на багато користувачів системи розумний будинок, а також знайдено міри для забезпечення конфіденційності, цілісності та доступності даних. Для підвищення ефективності захисту було запропоновано модифікувати відомий алгоритм Kerberos.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Застосування концепції безпеки системи розумного будинку потребує обґрунтування економічної її доцільності, виходячи з аналізу витрат на розробку та впровадження. Тому метою економічного розділу є аналіз економічної ефективності розробки системи розумного будинку. Для цього необхідно здійснити розрахунок:

– капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення;

– річних експлуатаційних витрат на утримання і обслуговування;

– річного економічного ефекту;

– показників економічної ефективності розробки.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

До капітальних витрат належать витрати на розробку політики безпеки інформації, які визначаються виходячи з трудомісткості розробки політики безпеки інформації.

Визначення трудомісткості розробки політики безпеки інформації

Трудомісткість запровадження розподілена система аутентифікації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = tmз + tв + tа + tвз + tозб + tовр + tд, \text{ годин,}$$

де $tmз$ – тривалість складання технічного завдання на запровадження розподіленної системи аутнтифікації;

$tв$ – тривалість розробки концепції безпеки інформації для системи розумний будинок;

$tа$ – тривалість процесу аналізу ризиків;

$tвз$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$tозб$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$tовр$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування системи;

t_{∂} – тривалість документального оформлення політики безпеки.

Визначено, що відповідно до етапів розробки розподіленої системи аутентицфікації, тривалість операцій складає наступні величини: $t_{тз}$=120 годин, $t_{в}$=30 годин, $t_{тз}$=15 годин, $t_{вз}$=10 годин, $t_{озб}$=10 годин, $t_{овр}$=6 годин, $t_{д}$=6 годин.

Отже, t=120+30+15+10+10+6+6= 197 годин,

Розрахунок витрат на створення політики безпеки інформації

Витрати на розробку розподіленої системи аутентицфікації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки розподіленої системи аутентицфікації Змч.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 120170 + 1014{,}55 = 121184{,}55 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 197*610 = 120170 \text{ грн.}$$

де t – загальна тривалість розробки розподіленої системи аутентицфікації, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки розподіленої системи аутентицфікації визначається за формулою:

$$З_{мч} = t*С_{мч} = 197*5{,}15 = 1014{,}55 \text{ грн.}$$

де $t_{д}$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу, грн./година.

Вартість 1 години машинного часу визначається за формулою:

$См_ч$ =0,8 * 15 * 1,1 + (15600 * 0,3)/1920 + (5770 * 0,1)/1920 = 15,94 грн.

Відповідно до розроблених рекомендації щодо забезпечення конфіденційності, цілісності, доступності інформації планується додатково оновлення ПЗ усіх пристроїв системи розумний будинок до останньої версії, налаштування мережі VPN для системи, встановити систему контролю управління доступом, проводити регулярну перевірку справності всіх пристроїв розумного дому, встановити резервне джерело живлення.

Таким чином, капітальні (фіксовані) витрати на створення політики безпеки інформації:

$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}$ = 210569 грн.

де $К_{рп}$ – вартість розробки розподіленої системи аутентицфікації, 121184,55 грн;

$К_{зпз}$ – вартість оновлення та закупівлі програмного забезпечення (ПЗ), 11,385 тис. грн; вартість VPN та антивірусного ПЗ

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, 8 тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, 15 тис. грн; вартість міжнережевого єкрану

$К_{навч}$ – витрати на технічних фахівців, 50 тис. грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, 5 тис. грн.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad грн.$$

де $С_в$ - вартість відновлення й модернізації системи ($С_в = 0$);

$С_к$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Витрати на технічних фахівців й кінцевих користувачів визначаються ($С_н = 15000$ грн.).

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему розумного буинку ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 50000 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо налаштувань інфраструктури безпечних підключень мобільних користувачів до інтрамережі підприємства потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$С_з = (50000*12 + 50000*12*0,1)*0,25= 165000$ грн.

З 01.01.2019 р. Ставка ЄСВ для всіх категорій платників складає 22%.

$$С_{єв} = 165000 *0,22 = 36300 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \quad грн.,$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,4 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$C_е$ – тариф на електроенергію, ($C_е$ = 1,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$C_{ел} = 1,4*1920*1,8 = 4838,4 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% (Стос = 149385*0,01=1493,85 грн).

Річний фонд амортизаційних відрахувань ($C_а$) за прямолінійним методом для ПЗ склад два роки тобто:

$C_{а1}$ = 15000/5 = 3000 грн.

$C_{а2}$ = 11385/2 = 5692,5 грн.

С = 3000 + 5692,5 = 8692,5 грн.

Витрати на керування системою інформаційної безпеки ($C_к$) визначаються:

$C_к$ = 15000+165000+36300+4838,4+1493,85+8692,5 = 231324,75 грн.

Отже, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$C = 231324,75 \text{ грн.}$$

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента систему розумний будинок внаслідок атаки, 2 години;

$t_в$ – час відновлення після атаки персоналом, що систему розумний будинок, 1 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або систему розумний будинок, 4 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 18000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла, 23000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особи;

$Ч_с$ – чисельність співробітників атакованого вузла, 3 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 5000000 грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 30.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = (\sum Зс/F) * tn = (23000 * 12)/176)) * 2 = 3136{,}36 \text{ грн.}$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$Пви = (\sum Зс/F) * tви = (23000 * 12)/176)) * 4 = 6272{,}72 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$Ппв = (\sum З_о/F) * t_в = (18000 * 12)/176)) * 1 = 1227,27 \text{ грн.}$$

Витрати на заміни встаткування або запасних частин можуть скласти 1600 грн.

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в = 6272,72 + 1227,27 + 5000 = 12499,99 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із средньогодинного обсягу прибутку і сумарного часу простою системи:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = (5000000/2080) * (2 + 1 + 4) = 16826,92 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 3136,36 + 12499,99 + 16826,92 = 32462,28 \text{ грн.}$$

Таким чином, загальний збиток від атаки на систему розумного будинку організації складе:

$$В = \sum_1 \sum_{30} 32462,28 = 973868,4 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.},$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент системи, частки одиниці (60%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 973868,4*0,6 - 231324,75 = 352996,29 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = 352996,29 / 210569 = 1,68 \text{ частки одиниці}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (20%);

$N_{інф}$ – річний рівень інфляції, (15%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$1,68 > (20 - 15)/100 = 1,68 > 0,05.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_o = K/E = 1/ROSI = 1/1,68 = 0,6 \text{ років}$$

ВИСНОВКИ ДО РОЗДІЛУ ІІІ

Розробка системи розумного є економічно доцільним, оскільки коефіцієнт повернення інвестицій ROSI складає 1,68 грн./грн., що означає отримання 1,68 грн. економічного ефекту на кожну гривню капітальних вкладень на розробку конфігурації налаштувань інфраструктури безпечних підключень мобільних користувачів. Отримане значення коефіцієнту повернення інвестицій вище дохідності альтернативного вкладення коштів. Термін окупності при цьому складатиме 0,6 років (біля 6 років). Капітальні витрати складають 149385 грн.

ВИСНОВКИ

В кваліфікаційній роботі був проведений аналіз систем автоматизації та існуючих методів забезпечення інформаційної безпеки в системі розумного будинку.

Було проаналізовано основні вразливості та загрози, проведена оцінка ризиків згідно з якої найбільшу загрозу представляють ті, що порушують одночасно конфіденційність, цілісність та доступність. А саме неякісні датчики, слабкий захист мережі розумного будинку, слабкий захист при взаємодії пристроїв один з одним у локальній мережі, використання тільки логіну та паролю для захисту сторінки з налаштуваннями, використання однакових паролів на більшості пристроїв компанії, простий чи застарілий механізм захисту, слабкий пароль або незмінений мастер пароль від виробника, відсутність шифрування при передачі данних при підключенні до відеокамери через «хмару», передача данних через USB, незахищене зберігання апаратури.

Описано механізм роботи симетричних протоколів розподілу ключів, серед яких: протокол Wide Mouth Frog, протокол Нідхема-Шрьодера, протокол Отвея-Піса, Kerberos. Серед проаналізованих протоколів був обраний Kerberos, оскільки порівнянно з іншими він не

має крипто-нестійкі точки та клієнти, що спілкуються між собою можуть бути певні в справжності один одного.

Оскільки Kerberos є досить нестійким до атак з боку адміністратора системи, де зловмисник може маніпулювати квитками Kerberos для отримання несанкціонованого доступу, було запропоновано систему забезпечення захисту даних шляхом застосування модифікованого алгоритму Kerberos, який виключає цю загрозу. Обґрунтувана економічна доцільність розроблених методів. Термін окупності яких, враховуючи коефіцієнт повернення інвестицій ROSI, становить 0,56 років

ПЕРЕЛІК ПОСИЛАНЬ

1. Що таке «розумний будинок» і навіщо він потрібен? [Електронний ресурс] – Режим доступу до ресурсу: https://stylus.ua/uk/articles/528.html
2. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process [Електронний ресурс] – Режим доступу до ресурсу: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-020-00111-0
3. CYBERSECURITY CONSIDERATIONS FOR CONNECTED SMART HOME SYSTEMS AND DEVICES [Електронний ресурс] – Режим доступу до ресурсу: https://industrie-4-0.ul.com/wp-content/uploads/2018/02/UL_Cybersecurity_SmartHome_White_Paper_en.pdf
4. Методика аналізу ризиків Microsoft [Електронний ресурс] – Режим доступу до ресурсу: http://ni.biz.ua/3/3_5/3_52705_metodika-analiza-riskov-Microsoft.html
5. НД-ТЗІ-2.5-005--99 [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-005--99.pdf
6. Weakness Within: Kerberos Delegation [Електронний ресурс] – Режим доступу до ресурсу: https://www.cyberark.com/resources/threat-research-blog/weakness-within-kerberos-delegation

7. Как защитить умный дом: Решение от команды Университета ИТМО [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/company/spbifmo/blog/317454/
8. Умный Дом – оборудование и автоматика для дома [Електронний ресурс] – Режим доступу до ресурсу: https://www.ivd.ru/stroitelstvo-i-remont/bezopasnost-i-domasnaa-avtomatika/12-luchshih-sistem-umnogo-doma-2021-i-sovety-po-vyboru-88162
9. CYBERSECURITY CONSIDERATIONS FOR CONNECTED SMART HOME SYSTEMS AND DEVICES [Електронний ресурс] – Режим доступу до ресурсу: https://industrie-4-0.ul.com/wp-content/uploads/2018/02/UL_Cybersecurity_SmartHome_White_Paper_en.pdf
10. МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РОЗУМНОГО БУДИНКУ [Електронний ресурс] – Режим доступу до ресурсу: https://oaji.net/articles/2020/8096-1594973817.pdf
11. A blockchain-based smart home gateway architecture for preventing data forgery [Електронний ресурс] – Режим доступу до ресурсу: https://hcis-journal.springeropen.com/articles/10.1186/s13673-020-0214-5
12. Privacy Preserving Data Analytics for Smart Homes [Електронний ресурс] – Режим доступу до ресурсу: https://www.ieee-security.org/TC/SPW2013/papers/data/5017a023.pdf
13. Pablo Giambiagi. Secrecy for Mobile Implementations of Security Protocols. – 2001. – ISSN 1403-5286
14. An Analysis of the Needham-Schroeder Public-Key Protocol with MGS – Olivier Michel - University of Paris-Est – 2009
15. Kerberos: An Authentication Service for Computer Networks [Електронний ресурс] – Режим доступу до ресурсу: https://courses.cs.vt.edu/~cs5204/fall09-kafura/Papers/Security/Kerberos-Paper.pdf
16. Щуров Ігорь «Методи та програмні засоби попереднього розподілу ключ
17. Kerberos Weaknesses: Pass the Ticket Is a Real Threat [Електронний ресурс] – Режим доступу до ресурсу: https://www.varonis.com/blog/kerberos-loopholes-pass-ticket
18. Укрощение Kerberos. Захватываем Active Directory на виртуальной машине с HackTheBox [Електронний ресурс] – Режим доступу до ресурсу: https://xakep.ru/2019/06/27/htb-kerberos/

19. Эксплоит для уязвимосты в протоколе Kerberos [Електронний ресурс] – Режим доступу до ресурсу: https://xakep.ru/2020/12/11/bronze-bit/
20. Kerberos Attack: How to Stop Golden Tickets? [Електронний ресурс] – Режим доступу до ресурсу: https://www.varonis.com/blog/kerberos-how-to-stop-golden-tickets

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	23	
6	А4	Спеціальна частина	23	
7	А4	Економічний розділ	11	
8	А4	Висновки	1	

9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1. Презентація Колодій.ppt
2. Диплом Колодій.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

ВІДГУК

на кваліфікаційну роботу студента групи 125м-20-2

Колодія Єгора Сергійовича

на тему: «Методи оцінки ризиків кібербезпеки

в системах "Розумний будинок"»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 73 сторінках.

Метою кваліфікаційної роботи є дослідження вразливостей та загроз у системах типу “розумний будинок” та розробка методів підвищення рівню кібербезпеки подібних систем.

Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз систем автоматизації та існуючих методів забезпечення інформаційної безпеки в системі розумного будинку. Запропоновано систему забезпечення захисту даних шляхом застосування модифікованого алгоритму Kerberos.

Практичне значення результатів кваліфікаційної роботи полягає у отриманих результатах аналізу вразливостей системи розумного будинку та запропонованому методі захисту даних.

За час дипломування Колодій Є.С. проявив себе фахівцем, здатним в цілому вирішувати поставлені задачі, та заслуговує присвоєння кваліфікації магістра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Кваліфікаційна робота заслуговує оцінки «добре».

Керівник к.т.н. доц. каф БІТ _____ Сафаров О.О.
(підпис) (прізвище, ініціали)