Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
в. о. завідувача кафедри
кібербезпеки та захисту інформації
_____Н. В. Лукова-Чуйко
“_____”_____2020 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
випускної кваліфікаційної роботи
бакалавра
(назва освітнього рівня)

галузь знань Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма «Кібербезпека та захист інформації»
(назва освітньої програми)

на тему: Розробка системи захисту об’єкта інформаційної діяльності, яка базується на двофакторному контурі

Виконавець: студентка IV курсу, групи КБ-41
Блохіна Дар’я Михайлівна
(підпис) (прізвище ім’я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Браіловський М. М.	

Нормоконтроль	Даков С. Ю.	

Київ
2020

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:

в. о. завідувача кафедри

кібербезпеки та захисту інформації

_____ Н. В. Лукова-Чуйко

“_____”_____20__ р.

ЗАВДАННЯ

на виконання дипломної роботи (проекту)

спеціальності 125 Кібербезпека

(код і назва спеціальності)

освітньої програми «Безпека інформаційних і комунікаційних систем»

(назва освітньої програми)

студентці **КБ-41** **Блохіній Дар’ї Михайлівні**

(група) (прізвище ім’я по-батькові)

Тема дипломної роботи Розробка системи захисту об’єкта інформаційної діяльності, яка базується на двофакторному контурі

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Застосунок законів Ома, першого і другого законів Кіргофа, методи та способи моделювання загроз, нюанси двофакторного контуру, архітектура системи.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з побудовою схем та перетворенням моделей у систему з двофакорним ланцюгом, моделюванням загроз, впровадженням Інтернету-речей, задання системи з декількох елементів електро-магнітних полей.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розвинену модель можна використовувати у системі «Розумний замок», «Розумні будинки».

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 05 жовтня 2020

Завдання видав		М. М. Браіловський
	(підпис)	(ініціали, прізвище)
Завдання прийняла		Д. М. Блохіна
до виконання	(підпис)	(ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	20.01.2020 – 22.01.2020	*виконано*
2	Аналіз літератури	23.01.2020 – 09.02.2021	*виконано*
3	Збір відомостей з електро-механіки	10.02.2021 - 23.02.2021	*виконано*
4	Опис моделей загроз	24.02.2021 - 08.03.2021	*виконано*
5	Збір відомостей щодо Інтернету-речей	09.03.2021 – 29.03.2021	*виконано*

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
6	Дослідження законів Ома і Кіргофа	30.03.2021 – 19.04.2021	*виконано*
7	Збір відомостей про баланс потужностей	20.04.2021 – 03.05.2021	*виконано*
8	Створення та аналіз моделі загроз	04.05.2021 – 17.05.2021	*виконано*
9	Оформлення пояснювальної записки	18.05.2021 – 08.06.2021	*виконано*
10	Підготовка до захисту дипломної роботи	09.06.2021 – 21.06.2021	*виконано*

Студент-дипломник _____ Д. М. Блохіна
(підпис) (ініціали, прізвище)

Керівник випускної кваліфікаційної роботи _____ М. М. Браіловський
(підпис) (ініціали, прізвище)

Термін подання дипломної роботи до ЕК

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Розробка системи захисту об’єкта інформаційної діяльності, яка базується на двофакторному контурі» складається зі вступу, основної частини, що містить 3 розділи, висновків і списку літератури та джерел. Загальний обсяг роботи – 75 сторінок. Робота містить 8 рисунків, 13 таблиць. Список використаних джерел включає 25 джерел.

Об’єкт дослідження – процес моделювання системи з двофакторним контуром.

Мета роботи – обрахувати і виявити найбільш оптимальну модель для обраного об’єкту.

Предмет дослідження – фізичний захист інформації.

Метод дослідження – синтез інформації щодо поєднання елементів електро-магнітного поля.

Практичне значення роботи полягає у створенні моделі з двофакторним контуром для захисту об’єкта інформаційної діяльності.

Результати здійснених у дипломній роботі досліджень можуть бути використані спеціалістами із захисту інформації та при подальшому проведенні науково-дослідницьких робіт.

Напрямки подальших досліджень: створення подібних моделей для різних об’єктів інформаційної діяльності та їх аналіз для покращення рівня безпеки окремих об’єктів.

Ключові слова: електро-магнітне поле, двофакторний контур, діаелектрики, діамагнетики, модель загроз.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

API – Application Programming Interface
BLE – Bluetooth Low Energy
CAPEC – Common Attack Pattern Enumeration and Classification
CSMA/CA – Carrier Sense Multiple Access/Collision Avoidance
CVSS – The Common Vulnerability Scoring System
CWE – Common Weakness Enumeration
(D)DoS – (Distributed) Denial-of-Service
IDS – Intrusion Detection System
IEEE – Institute of Electrical and Electronics Engineers
IoT – Internet-of-Things
IPS – Intrusion Prevention System
MTMT – Microsoft Threat Modeling Tool
NFC – Near-field communication
PASTA – Process for Attack Simulation & Threat Analysis
RFID – Radio-frequency identification
SSL – Secure Sockets Layer
TLS – Transport Layer Security
VPN – Virtual Private Network
XML – Extensible Markup Language
XMPP – Extensible Messaging and Presence Protocol
ПЗ – програмне забезпечення

ЗМІСТ

ВСТУП

Сьогодні наше життя піддається великому впливу зі сторони інформаційних технологій. Ми вже не можемо уявити своє життя без нових сервісів та приладів.

Із розквітом сучасних технологій люди все частіше потребують допомоги в покращенні свого життя. Об'єднання багатьох процесів в єдину систему, або навіть їх автоматизація, можуть зменшити наші витрати (як матеріальні, так і фізичні) і надати більше вільного часу.

Системи з двофакторним контуром можуть надати таку можливість. Хоча на українському ринку вони перебувають не так давно, але кожного року їх популярність зростає в декілька разів.

Вже зараз будуються нові прилади із влаштованими всередині однофакторними та багатофакторними контурами, які мінімізують втрати інфомаційних продутів. Все це є результатом розвитку даних систем за останні роки, що, насправді, є дивовижним феноменом.

Останні тенденції, побічні ефекти глобальної пандемії і статистика кібербезпеки показують величезне зростання числа зламаних і втрачених даних з джерел, які все частіше зустрічаються на робочому місці, таких як мобільні пристрої та пристрої Інтернету речей. Крім того, COVID-19 збільшив віддалену робочу силу, що призвело до кібератак.

Крім того, недавні дослідження в галузі безпеки показують, що більшість компаній мають незахищені дані та погану практику кібербезпеки, що робить їх вразливими до втрати даних. Для успішної боротьби зі зловмисними намірами вкрай важливо, щоб компанії зробили обізнаність про кібербезпеку, профілактику і кращі практики безпеки частиною своєї культури.

2020 рік приніс з собою кілька випробувань і тріумфів. COVID-19 змусив компанії створювати віддалені робочі місця і працювати на хмарних платформах. Впровадження 5G зробило підключені пристрої більш доступними, ніж будь-коли. Все це говорить про те, що індустрія кібербезпеки ніколи не була більш важливою.

Ці недавні події, а також наведені нижче статистичні дані і цифри з кібербезпеки, ось деякі галузеві тенденції, а також прогнози, які слід очікувати в 2021 році і в наступний період.

Віддалені працівники як і раніше будуть мішенню для кіберзлочинців.

Як побічний ефект віддаленої робочої сили будуть збільшуватися порушення в хмарі.

Дефіцит навичок в галузі кібербезпеки залишиться проблемою.

В результаті збільшення пропускної здатності підключених пристроїв 5G пристрої Інтернету речей стануть більш уразливими для кібератак.

За прогнозами Gartner, в 2023 році світовий ринок інформаційної безпеки досягне 170,4 мільярда доларів [5]. Багато в чому це пов'язано з тим, що організації розвивають свій захист від кіберзагроз — і зростанням таких загроз, в тому числі в їх власних компаніях. За даними Cybint, 95% порушень кібербезпеки викликані людською помилкою. Це красномовний висновок про ландшафт кібербезпеки, і ми виклали більше, щоб дати уявлення про цю область в цілому, а також про загальний вплив кібератак.

- 95% порушень кібербезпеки викликані людськими помилками. (Кибинт)
- 88% організацій по всьому світу зіткнулися зі спробами фішингу в 2019 році. (Коректура)
- 68% бізнес-лідерів вважають, що їх ризики в області кібербезпеки зростають. (Accenture)
- У середньому лише 5% папок компаній належним чином захищені. (Варонис)
- Порушення даних виявили 36 мільярдів записів у першій половині 2020 року. (на основі ризику)
- 86% порушень були фінансово мотивовані, а 10% - шпигунством. (Verizon)
- 45% порушень були пов'язані зі зломом, 17% - з шкідливими програмами і 22% - з фішингом. (Verizon)

- У період з 1 січня 2005 року по 31 травня 2020 року було зареєстровано 11 762 порушення. (Ресурсний центр по крадіжці ідентифікаторів)
- Основними типами шкідливих вкладень електронної пошти є .doc і .dot, які складають 37%, наступним за величиною є .exe з 19,5%. (Symantec)
- За оцінками, 300 мільярдів паролів використовуються людьми та машинами у всьому світі. (Засоби масової інформації з кібербезпеки)

Дана дипломна робота є актуальною, тому що у ній розглядається розумний об’єкт, який належить до системи Розумний Дім, що функціонує на основі Інтернету-речей. З кожним роком кількість таких пристроїв, що встановлюються у помешканнях людей, зростає, а це у свою чергу породжує питання і хвилювання щодо їх захищеності та загроз, які постають перед власниками житла. Також дана робота вміщує відомості щодо моделювання загроз – методу пошуку та оцінки загроз, який поки що є дуже бажаною до використання рекомендацією, а не розповсюдженою та обов’язковою практикою серед постачальників пристроїв і сервісів, але стрімко набуває популярності серед науковців і дослідників.

Враховуючи, що метою роботи було створення моделі загроз для кіберфізичного об’єкту, для її досягнення було визначено такі завдання:

- розгляд методу моделювання загроз;
- визначення найбільш популярних способів моделювання загроз;
- аналіз концепції Інтернету-речей;
- характеристика сфер використання IoT;
- дослідження властивостей розумного дому;
- опис кіберфізичного об’єкту у системі розумного дому;
- використання програмного забезпечення для створення моделі.

Розбір отриманої моделі двофакторного контуру та декілька рекомендацій для підвищення рівня безпеки об’єкту під час його функціонування також наведені у дипломній роботі. Результати даного дослідження можуть бути корисними для фахівців, які займаються забезпеченням захищеності пристроїв IoT.

Тези стосовно важливості впровадження моделювання загроз у процеси, пов’язані з IoT, та проблем, з якими стикається IoT, були апробовані на IV

(четвертій) міжнародній науково-практичній конференції “проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS).

РОЗДІЛ 1
ПОНЯТТЯ ФІЗИЧНОГО ЗАХИСТУ

1.1 Види захисту інформації

Проблеми кібербезпеки стають повсякденною боротьбою для бізнесу. Порушення можуть призвести навмисні або ненавмисні передачі захищеної або приватної/конфіденційної інформації в ненадійне середовище. Інші терміни для цього явища включають ненавмисне розкриття інформації, витік даних, витік інформації. Інциденти варіюються від узгоджених атак чорних капелюхів або осіб, які зламують для будь-якої особистої вигоди, пов'язаних з організованою злочинністю, політичними активістами або національними урядами, до недбалого поводження з використаним комп'ютерним обладнанням або носіями даних і недоступним джерелом.

Визначення: "порушення даних-це порушення безпеки, при якому конфіденційні, захищені або конфіденційні дані копіюються, передаються, проглядаються, крадуться або використовуються особою, яка не має на це права". Порушення даних можуть включати фінансову інформацію, таку як дані кредитної картки або банківські реквізити, особисту медичну інформацію (PHI), особисту ідентифікаційну інформацію (PII), комерційну таємницю корпорацій або інтелектуальну власність. Більшість порушень даних пов'язані з надмірно відкритими та вразливими неструктурованими даними-файлами, документами та конфіденційною інформацією.[2]

Порушення даних можуть бути досить дорогими для організацій з прямими витратами (виправлення, розслідування і т. д.) і непрямими витратами (репутаційний збиток, забезпечення кібербезпеки жертвам скомпрометованих даних і т. д.)

За даними неприбуткової організації з захисту прав споживачів, в цілому 227 052 199 індивідуальних записів, що містять конфіденційну особисту інформацію,

були залучені в порушення безпеки в Сполучених Штатах в період з січня 2005 по травень 2008 року, за винятком інцидентів, коли конфіденційні дані, мабуть, фактично не були розкриті.[3]

У багатьох юрисдикціях прийняті закони про повідомлення про порушення даних, які вимагають, щоб компанія, яка зазнала порушення даних, інформувала клієнтів і вживала інші кроки для усунення можливих травм.

Порушення даних може включати такі інциденти, як крадіжка або втрата цифрових носіїв, таких як комп'ютерні стрічки, диски або портативні комп'ютери, що містять такі носії, на яких така інформація зберігається в незашифрованому вигляді, розміщення такої інформації у всесвітній павутині або на комп'ютері, доступному іншим чином з Інтернету, без належних заходів інформаційної безпеки, передача такої інформації в систему, яка не повністю відкрита, але не має належної або формальної акредитації для забезпечення безпеки на затвердженому рівні, наприклад незашифрованная електронна пошта, або передача такої інформації в інформаційні системи потенційно ворожого агентства, такого як конкуруюча корпорація або іноземна держава, де вона може піддаватися більш інтенсивним методам дешифрування.

ISO / IEC 27040 визначає порушення даних як: порушення безпеки, яке призводить до випадкового або незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до захищених даних, що передаються, зберігаються або іншим чином обробляються.

Поняття довіреної середовища дещо мінливе. Догляд довіреного співробітника, що має доступ до конфіденційної інформації, може стати порушенням даних, якщо співробітник збереже доступ до даних після припинення довірчих відносин. У розподілених системах це також може статися при руйнуванні мережі довіри. Якість даних є одним із способів зниження ризику порушення даних[6], частково тому, що воно дозволяє власнику даних оцінювати дані відповідно до важливості і забезпечувати кращий захист більш важливих даних.

Більшість таких інцидентів, що висвітлюються в засобах масової інформації, пов'язані з приватною інформацією про фізичних осіб, наприклад, номерами

соціального страхування. Втрата корпоративної інформації, такої як комерційна таємниця, конфіденційна корпоративна інформація та деталі контрактів або урядова інформація, часто не повідомляється, оскільки немає вагомих причин для цього за відсутності потенційного збитку приватним особам, і розголос навколо такої події може завдати більшої шкоди, ніж втрата самих даних.

1.2 Актуальність кіберзахисту

Кібербезпека - це мистецтво захисту мереж, пристроїв та даних від несанкціонованого доступу чи злочинного використання та практика забезпечення конфіденційності, цілісності та доступності інформації. Здається, зараз все залежить від комп'ютерів та Інтернету - спілкування (наприклад, електронна пошта, смартфони, планшети), розваги (наприклад, інтерактивні відеоігри, соціальні медіа, додатки), транспорт (наприклад, навігаційні системи), покупки (наприклад, Інтернет покупки, кредитні картки), ліки (наприклад, медичне обладнання, медичні картки), і список можна продовжувати. Скільки у повсякденному житті покладається на технології? Скільки особистої інформації зберігається на власному комп'ютері, смартфоні, планшеті або в чужій системі?

Світ як ніколи раніше покладається на технології. В результаті створення цифрових даних зросло. Сьогодні підприємства та уряди зберігають значну частину цих даних на комп'ютерах і передають їх через мережі на інші комп'ютери. Пристрої та їх основні системи мають вразливі місця, які під час експлуатації підривають здоров'я та цілі організації.

Порушення даних може мати низку руйнівних наслідків для будь-якого бізнесу. Це може розкрити репутацію компанії через втрату довіри споживачів та партнерів. Втрата важливих даних, таких як вихідні файли чи інтелектуальна власність, може коштувати компанії конкурентних переваг. Подальше порушення даних може вплинути на доходи корпорацій через невідповідність нормам захисту даних. За підрахунками, в середньому порушення даних коштує постраждалій організації 3,6 мільйона доларів. У зв'язку з гучними порушеннями даних, що

спричиняють заголовки засобів масової інформації, важливо, щоб організації застосовували та застосовували сильний підхід до кібербезпеки.

Кіберзлочинність стала центром національної безпеки та частою темою дискусій щодо управління ризиками. Новини про великі корпоративні та урядові порушення підтверджують, що жодна організація чи державна установа не застраховані від наполегливих, кваліфікованих нападників. Критична інфраструктура також стає дедалі привабливішою мішенню для злочинців завдяки зростаючій залежності від технологій.

Чому злочинці націлюються на конфіденційні дані? Адаптація та реагування на еволюціонуючі кіберзагрози та захист критичної інфраструктури та власних комерційних активів мають важливе значення як для державних установ, так і для бізнесу. «Посмертні» аналізи порушень пропонують скарбницю отриманих уроків та розкривають тактику, техніку та процедури нападу.

Кіберзлочинці використовують технологічні вразливості та хитрощі, щоб використати людський технологічний розрив - націлюючи на конфіденційні паролі, дані та програми, які регулярно використовуються персоналом. Крадіжка даних є метою останніх порушень. Кіберзлочинці, як правило, проникають у вразливі системи та здійснюють взаємодію між системами, використовуючи викрадені дані або видаючи себе стороннім підрядником, щоб отримати доступ до цінних даних.

Цільові конфіденційні дані включають записи про персонал, публічну платіжну інформацію, номери кредитних карток, фінансові та медичні записи тощо. Крадіжка законно захищених даних у місті може спричинити значні штрафи у законодавстві, втрату довіри громадськості та шкоду репутації міста.

За оцінками Fortune.com, у 2020 році вартість порушення даних становила в середньому 4 мільйони доларів або 158 доларів за запис. Історія хвороби, дані кредитних карток та номери соціального страхування мають найвищу ціну за викрадений запис - 355 доларів.

Дані - це нова валюта. Традиційні методи управління валютними та майновими ризиками також застосовуються для захисту від кіберзлочинності. Регульовані або конфіденційні дані мають грошову цінність і стають привабливою

метою для кіберзлочинців. Зменшення кількості регульованих даних, що зберігаються на руках, еквівалентно практиці управління готівкою, наприклад, переміщення надлишків готівки з реєстрів у загартований сейф або транспортування їх до сховища банку. Зазвичай забороняється необмежений та неспостережений доступ працівників до великої суми готівки; однак державні установи часто не застосовують однаковий рівень контролю за доступом працівників до регульованих або конфіденційних даних.

1.3 Стратегії моделювання загроз

Мозковий шторм являється найпростішим та досить ефективним способом генерації ідей. У той час, як один аналітик безпеки може годинами обмірковувати усі можливі загрози, користуючись своїми знаннями та типом мислення, головною перевагою групи людей, що має на меті визначити якомога більше потенційних вразливостей на стадії проектування, є безліч різних ідей, які можуть стосуватися досить великої кількості аспектів.

Огляд літератури. Під час моделювання загроз може виявитися корисним пошук публікацій та статей, що стосуються продукту, який розробляється. Даний огляд допоможе у виявленні стандартних проблем безпеки, які зустрічаються повсякчас у конкурентів та/або активно розглядаються у наукових роботах з потенціалом бути експлуатованими зловмисниками.

Фокус на активах. Під активами розуміється те, що представляє собою цінність. Моделювання загроз у даному випадку базується навколо таких понять як те, що хоче захистити розробник, і те, що хоче отримати зловмисник, а також іноді способи досягнення мети зловмисником. Найчастіше зустрічається перетин перших двох. Даний спосіб допоможе точно визначитися, що вважатиметься активами, але не принесе жодних інноваційних ідей щодо типів можливих загроз.

Фокус на зловмисниках. Як і попередній спосіб, даний підхід лише узагальнить модель порушника, але не виявиться насправді корисним, якщо говорити саме про загрози більш технічного характеру. Проте іноді це також може

виявитися корисним, особливо коли постає необхідність сфокусуватися на загрозах, залежних від людського фактору.

Фокус на програмному забезпеченні. Моделювання на основі програмного забезпечення – це спосіб, який вимагає ґрунтовних знань про продукт, що створюється, адже конкретні особливості та архітектура ПЗ (програмне забезпечення) визначатимуть конкретні можливі загрози. Проблеми та вразливості, знайдені під час такого моделювання, можуть бути досить унікальними або ж навпаки одними з найпопулярніших, проте у будь-якому випадку можливість їх охарактеризувати досягається завдяки концентрації уваги на ПЗ.

1.4 Види програмного захисту

Мережева безпека захищає мережевий трафік, керуючи вхідними та вихідними з’єднаннями, щоб запобігти входу або поширенню загроз у мережі.

Запобігання втраті даних (DLP) захищає дані, зосереджуючи увагу на розташуванні, класифікації та моніторингу інформації, що перебуває у стані спокою, у використанні та в русі.

Cloud Security забезпечує захист даних, що використовуються в хмарних послугах та додатках.

Системи виявлення вторгнень (IDS) або Системи запобігання вторгненню (IPS) працюють над виявленням потенційно ворожої кібер активності.

Управління ідентифікацією та доступом (IAM) використовує служби автентифікації для обмеження та відстеження доступу співробітників для захисту внутрішніх систем від шкідливих об'єктів.

Шифрування - це процес кодування даних, що робить їх незрозумілими, і часто використовується під час передачі даних, щоб запобігти крадіжці під час транзиту.

Антивірусні/антивірусні програми перевіряють комп'ютерні системи на наявність відомих загроз. Сучасні рішення навіть здатні виявляти раніше невідомі загрози на основі їх поведінки.

1.5 Модель загроз

Під час моделювання загроз постає досить велика кількість питань. Наприклад, що трапиться, якщо зловмисник матиме змогу змінювати параметри системи, або які наслідки того, що зловмисник отримає до неї доступ та збиратиме необхідну йому інформацію, не видаючи своєї присутності. На жаль, якщо просто збирати такі питання до купи без будь-якої структури, то буде дуже складно отримати зрозумілу, детальну та інформативну модель загроз.

Корисним інструментом для наступного етапу після створення ДПД є вже готова модель загроз – STRIDE [3]. STRIDE – це абревіатура, що складається з перших літер шести слів, які складають категорії загроз (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service та Elevation of privilege відповідно). Якщо перекладати на українську мову, то виходить наступне:

- Спуфінг;
- Фальсифікація даних;
- Заперечення;
- Розкриття інформації;
- Відмова в обслуговуванні;
- Підвищення привілеїв.

Спуфінг порушує ознаку автентифікації. Прикладом даної атаки виступає зловмисник або програма, що видають себе не за тих, ким вони являються. Жертвами є люди або процеси. Фальсифікація даних спрямована на порушення цілісності та означає зміну даних у мережі, на диску, в пам’яті і т. д. Постають перед загрозою також процеси і потоки даних.

Заперечення так само націлене на процеси і представляє собою спростовування будь-яких обвинувачень у скоєнні (або іноді навпаки – не скоєнні) того чи іншого вчинку, який призвів до неприємних наслідків. Розкриття інформації – це загроза конфіденційності. Найяскравішим прикладом служить отримання інформації неавторизованими особами.

Відмова в обслуговуванні – це порушення такої ознаки як доступність. Поглинання ресурсів, необхідних для коректної роботи та надання сервісів, негативно впливає на рух даних та процеси у системі. Підвищення привілеїв є недотриманням коректної авторизації. Наприклад, надання прав адміністратора безпеки працівнику з фінансового відділу.

Ця модель охоплює велику кількість можливих загроз, адже вона розглядає різні сфери їх застосування. Так само спуфінг може стосуватися файлу або людини, фальсифікувати можна файли або потоки в мережі, відмова в обслуговуванні відноситься до процесів або сховищ даних, і т. д.

Існує декілька варіацій моделі STRIDE: STRIDE-per-Element (фокус на чотирьох елементах діаграми потоків даних) та STRIDE-per-Interaction (фокус на взаємодіях). У першому випадку акцент робиться на таких міркуваннях, як, наприклад, неможливість сховища даних бути активним елементом загрози, що стосується підвищення привілеїв. На основі цього будується таблиця, що зображує відповідність між різними типами загроз та елементами, на які вони мають вплив (табл. 1.2).

Таблиця 1.2

Загрози та їх вплив на елементи

Елемент	**S**	**T**	**R**	**I**	**D**	**E**
Зовнішня сутність	✓		✓			
Процес	✓	✓	✓	✓	✓	✓
Сховище даних		✓		✓	✓	
Потік даних		✓		✓	✓	

STRIDE-per-Interaction – це ускладнена версія моделі, адже вона розглядає не лише процес, а ще й джерело, адресата та взаємодію. У таблицю, схожу на попередню, замість елементів вписуються маніпуляції, які можуть відбуватися з цими елементами. Загрози, знайдені під час використання цієї варіації, легше зрозуміти, адже вони детальніше описані з самого початку створення таблиці.

HTMM – це гібридний метод моделювання загроз, який характеризується відсутністю хибно позитивних спрацювань, непомічених загроз, постійним результатом та ефективними витратами.

Quantitative Threat Modeling Tool – ще один гібридний метод, який складається з дерев атак, STRIDE та CVSS. Кореневим вузлом у даному випадку виступає одна з категорій STRIDE, для неї будується дерево атак, яке потім оцінюється за допомогою CVSS.

OCTAVE – це ризико-орієнтовний метод стратегічної оцінки та планування для кібербезпеки, представлений підрозділом Комп'ютерної команди реагування на надзвичайні події у 2003 році. У центрі цього методу знаходиться оцінка організаційних ризиків, без урахування технологічних. OCTAVE складається з трьох етапів: побудови профілів загроз на основі цінних володінь, визначення вразливостей інфраструктури, розгортання стратегії та планів безпеки. Існує варіація, яка має назву OCTAVE-S, та призначена для використання у невеликих організаціях. Недоліками даного методу можна вважати велику кількість часу, витраченого на якісне впровадження, та чималу документацію.

1.6 Стратегії керування ризиками

Після здійснення опису характеристик загроз необхідно вплинути на ризики, які вони представляють. Ключовими моментами, вартими уваги, є рівень ризику, бажані крокі у відповідь на ризик та способи/методи досягання цілі. Класичними стратегіями боротьби з ризиками є їх уникання, вирішення, прийняття, переправлення та ігнорування.

1. Уникання ризиків

Уникати ризики зручно і навіть потрібно, якщо це представляється можливим. Під час якісного процесу оцінки ризиків спеціалісти можуть визначити, наскільки великим є ризик в порівнянні з вигодою, та за умови, що він є більшим, обрати саме цю стратегію.

2. Вирішення ризиків

Вирішення ризиків означає саме їх пряме вирішення, тобто, зміну дизайну, властивостей і т. д. Це може бути імплементація криптографічних засобів захисту або убезпечення операційних процесів.

3. Переправлення ризиків

Ризиками, що переправляються, є ті, з якими стикаються покупці або кінцеві користувачі. Це відбуваються через комбінацію умов надання послуг, ліцензійних угод чи інтерфейсу користувача. Постачальник продукту/послуг обов'язково повинен повідомити про наявні та/або можливі ризики.

4. Ігнорування ризиків

Через те, що більшість випадків, пов'язаних з безпекою, трималися в секреті у минулому, формування надійних та якісних датасетів щодо ризиків та оцінки методів боротьби з ними не було, а отже і ефективних та визнаних стратегій також. Ігнорування ризиків було звичною практикою, проте зараз з появою певних законів, це може бути навіть небезпечніше для компанії/підприємця/постачальника послуг, аніж сам ризик. При моделюванні загроз ризики, які не плануються бути вирішеними, все одно повинні бути пронумеровані та описані.

5. Прийняття ризиків

Дана стратегія означає повне усвідомлення усіх наслідків (цим вона і відрізняється від стратегії ігнорування), які можуть виникнути у разі експлуатації вразливості, представленої ризиком. Даній стратегії легше слідувати при управлінні процесами, аніж під час створення цілого продукту, адже якщо продукт представляє ризики, наприклад, користувачам, то це вже вважатиметься переправленням ризиків. Приймати ризики варто тоді, коли загроза є реальною, але ймовірність її виникнення є низькою або ж наслідки вважаються незначними.

Варто також зазначити, що прийняття ризиків може бути бізнес прийняттям або користувацьким. Процес прийняття відбувається у тому випадку, коли організація створює або розробляє продукт виключно для власного користування, тобто будь-які ризики можуть мати вплив лише на неї, і вона є відповідальною кожного разу. За умови, якщо ризики з'являються, коли користувач виконує певні

дії, за які відповідальний лише він сам, виконується користувацьке прийняття. Якщо така можливість має місце бути, то користувача необхідно забезпечити чітким, пояснювальним, дієвим та перевіреним попереджувальним повідомленням про можливі ризики, пов’язані з його діями.

1.7 Тестування моделі загроз

Після процесу вирішення ризиків наступає етап перевірки створеної моделі загроз на достовірність та стійкість та тестування обраних шляхів вирішення. На початку треба створити як мінімум два тести для кожної загрози – один для ситуації, коли загроза жодним чином не адресується, інший – за умови наявності певного рішення з метою обійти його. Для тестування самих рішень в першу чергу необхідно зрозуміти, якими способами вони можуть бути «атаковані». Тест на проникнення може бути додатковим способом оцінки моделі, адже з його допомогою спеціалісти мають змогу впевнитися у її якості на практиці, а іноді навіть і знайти непомічені раніше недоліки.

Насправді, сам процес моделювання загроз ніколи не завершується, але перед тим як випускати продукт на ринок, необхідно також упевнитися в тому, що створена та протестована модель відповідає усім необхідним та поставленим критеріям. Такими є: відповідність реальності на якомога вищому рівні, підтвердження того, що усі загрози, визначені у моделі, адресовані, і помилки та проблеми ПЗ, які зустрілися під час процесу, вирішені.

Відповідність реальності означає, що модель найточніше відображає архітектуру продукту, який створюється. В ідеалі вона повинна перероблюватися та/або доповнюватися щоразу, коли відбуваються зміни у дизайні самого продукту. У деяких випадках загрози, знайдені під час моделювання, підштовхують на переробку дизайну. Якщо під час фінальної оцінки виявляється, що модель застаріла і не надає коректного відображення процесів, її обов’язково необхідно оновити.

Також важливо упевнитися, що кожна загроза, яка була знайдена під час кожного етапу моделювання, адресована, тобто їй ставиться у відповідність будь-

яка із стратегій керування ризиками, що описані у попередньому підрозділі. Те саме стосується і помилок ПЗ: необхідно перевірити та підтвердити (або спростувати, але потім все ж вирішити проблему), що кожна помилка вже не являється такою на момент випуску продукту на ринок. Звісно, після релізу можливі виходи його нових версій, а отже і перегляд існуючої моделі загроз на предмет її доповнення, що підтверджує факт про постійність даного процесу.

1.8 Фізичний захист та його види

Заходи фізичної безпеки призначені для захисту будівель та захисту обладнання всередині. Вони утримують небажаних людей і надають доступ уповноваженим особам. Незважаючи на те, що мережа та кібербезпека важливі, запобігання порушенням фізичної безпеки та загрозам є ключовим фактором для забезпечення безпеки технологій та даних, а також будь-якого персоналу чи викладачів, які мають доступ до будівлі. Без встановлених планів фізичної безпеки офіс чи будівля залишаються відкритими для злочинної діяльності та несуть відповідальність за види фізичної загрози безпеці, включаючи крадіжки, вандалізм, шахрайство та навіть аварії.

У побудованому середовищі ми часто думаємо про такі приклади контролю фізичної безпеки, як замки, ворота та охорона. Хоча вони ефективні, існує багато додаткових і часто забутих рівнів фізичної безпеки офісів, які можуть допомогти захистити всі активи. Комплексний план фізичної безпеки поєднує в собі як технологію, так і спеціалізоване обладнання та повинен містити протидії проти вторгнення, такі як:

- Дизайн і верстка сайту
- Компоненти навколишнього середовища
- Готовність до ліквідації надзвичайних ситуацій
- Навчання
- Управління доступом
- Виявлення вторгнень

- Силовий та протипожежний захист

Починаючи з елементів ландшафтного дизайну та природного спостереження, закінчуючи зашифрованими клавіатурами чи мобільними даними, до можливостей блокування та аварійного збору, існує безліч різних компонентів для запобігання різним типам фізичних загроз безпеці на сучасному робочому місці.

Перш ніж застосовувати заходи фізичної безпеки у будівлі чи на робочому місці, важливо визначити потенційні ризики та слабкі сторони поточної безпеки. Виявлення має найважливіше значення для фізичної безпеки. Незважаючи на те, що неможливо запобігти вторгнень або порушень, наявність відповідних інструментів для виявлення та боротьби із вторгненнями зводить до мінімуму збитки у бізнесі в довгостроковій перспективі.

Щоб визначити зони потенційного ризику у закладі, спочатку потрібно розглянути всі загальнодоступні точки входу. Там, де люди можуть увійти та вийти з закладу, завжди існує потенційний ризик безпеки. Базові процедури фізичного контролю безпеки, такі як належні заходи контролю доступу ключових точках входу допоможе керувати тим, хто приходить і йде, і може попередити про потенційні вторгнення. Опинившись у закладі, одразу потрібно перевірити, занотувати, як дані чи конфіденційна інформація захищаються та зберігаються. Чи є у серверні кімнати, які потребують додаткового захисту? Чи заблоковані та захищені настільні комп’ютери, коли в офісі нікого немає? Чи є у працівників ноутбуки, які вони беруть із собою додому щовечора? Навіть USB-накопичувачі або незадоволений працівник можуть стати серйозною загрозою на робочому місці. Перелічивши усі потенційні ризики у будівлі, можна розробляти плани безпеки, щоб зменшити потенціал злочинної діяльності.

Трьома найважливішими компонентами фізичного контролю безпеки для офісів та будівель є методи контролю доступу, спостереження та методи перевірки безпеки. Хоча інші рівні процедур контролю фізичної безпеки є важливими, ці три контрзаходи є найбільш впливовими, коли йдеться про виявлення вторгнень та пом'якшення загроз.

Управління доступом

Захист записів утримує небажаних людей і дозволяє ввійти авторизованим користувачам. Сучасна система входу без ключів - це перша лінія захисту, тому наявність найкращих технологій є надзвичайно важливим. Доступно кілька різних типів систем; цей посібник з найкращих технологій контролю доступу допоможе вибрати правильну систему для будівлі. Головне, що слід врахувати з точки зору фізичної безпеки, - це ті типи облікових даних, які вибираються, якщо система локальна або хмарна, і якщо технологія відповідає усім унікальним потребам. Що стосується методів доступу, то найпоширенішими є картки клавіш та системи введення fob та мобільні облікові дані. Деякі системи контролю доступу дозволяють використовувати кілька типів облікових даних в одній системі. Контроль доступу, який використовує хмарне програмне забезпечення, рекомендується використовувати на локальних серверах для планів фізичного контролю безпеки, оскільки технічне обслуговування та оновлення системи можна виконувати віддалено, а не вимагати, щоб хтось приїжджав на місце (що зазвичай призводить до простою системи безпеки). Хмарна технологія також пропонує велику гнучкість щодо додавання записів та користувачів, а також значно полегшує інтеграцію з іншими системами безпеки.

1.9 Інструменти спостереження

Нагляд має вирішальне значення для контролю фізичної безпеки будівель з кількома точками входу. Найпоширенішим видом спостереження для контролю фізичної безпеки є відеоспостереження. Системи управління відео (VMS) - це чудовий інструмент для спостереження, який дає візуальне уявлення про діяльність у будівлі. Додаючи спостереження до системи фізичної безпеки, вибирайте камери, які відповідають об'єкту, тобто зовнішні двері потребують зовнішніх камер, які витримують стихію. Для внутрішніх камер враховуйте необхідні кути огляду та варіанти кріплення, які потрібні простору. Іншим фактором, що стосується систем відеоспостереження, є звітність та дані. Щоб отримати максимальну віддачу від відеоспостереження, потрібно мати можливість переглядати як кадри в режимі

реального часу, так і раніше записану активність. При контролі фізичної безпеки приклади випадків використання даних відеоспостереження включають проведення перевірок у системі, надання відеозаписів як доказів після порушення, використання журналів даних у надзвичайних ситуаціях, та застосування аналітики використання для поліпшення функціонування та управління системою. Якщо використовувати систему управління доступом на відкритій платформі, можна інтегрувати із своєю системою керування вмістом, щоб пов'язати візуальні дані з активністю введення, пропонуючи потужну інформацію та аналітику у системі безпеки.

Випробування на готовність до надзвичайних ситуацій та безпеку.

Освіта є ключовою складовою успішного контролю фізичної безпеки офісів. Якщо працівники, орендарі та адміністратори не розуміють нових змін політики фізичної безпеки, система буде менш ефективною у запобіганні вторгнень та порушень. Після налаштування системи сплануйте ретельне тестування на всі різні типи фізичних загроз безпеці, з якими може зіткнутися будівля. Слід провести тренінги з питань безпеки та аварійних ситуацій зі командами на місці, а також протестувати будь-які віддалені функції фізичного контролю безпеки, щоб переконатися, що адміністратори мають доступ, необхідний для активації планів блокування, запуску запитів на розблокування та додавання або скасування доступу користувача. Взаємодія процедур контролю фізичної безпеки з персоналом та щоденними кінцевими користувачами допоможе співробітникам почуватися безпечніше на роботі.

Окрім очевидної переваги систем фізичного захисту, щоб захистити будівлю, обрані будівлею технології та обладнання можуть включати додаткові функції, які можуть підвищити безпеку робочого місця. Особливо завдяки хмарному фізичному контролю безпеки, можна отримати додаткову гнучкість для віддаленого управління системою, а також зв'язок з іншими системами безпеки та управління будівлею.

Запобігання несанкціонованому входу - забезпечення безпечного офісного приміщення є запорукою успішного бізнесу. Близько третини працівників не почуваються в безпеці на роботі, що може постраждати від продуктивності праці та службового моралі. Забезпечення безпеки для своїх клієнтів не менш важливо.

Клієнти повинні не тільки відчувати себе в безпеці, але і їх дані також повинні надійно зберігатися. Порушення даних ставить під загрозу довіру, над якою наполегливо працював бізнес. Впровадження суворої системи контролю доступу як частини планів фізичної безпеки дозволить захистити своє майно від несанкціонованого доступу, захищаючи активи та працівників та запобігаючи пошкодженню або втраті.

Проактивне виявлення вторгнень - Як перша лінія оборони для будівлі, важливість фізичної безпеки для запобігання вторгненню не можна недооцінювати. Крім того, хмарне програмне забезпечення дає перевагу перегляду активності в реальному часі з будь-якого місця та отримання сповіщень про вхід щодо типів фізичних загроз безпеці, таких як відчинені двері, спроба несанкціонованого входу, примусовий вхід тощо.

Масштабована реалізація фізичної безпеки - завдяки даним, що зберігаються у хмарі, немає необхідності в локальних серверах та обладнанні, які є одночасно дорогими та вразливими до атак. Хмарні системи фізичного контролю безпеки можуть інтегруватися з існуючими платформами та програмним забезпеченням, що означає відсутність перерв у робочому процесі. Як для малих підприємств, що переживають експоненціальне зростання, так і для підприємств, що розглядають багато сайтів і місць, масштабоване рішення, яке легко встановити і швидко налаштувати, забезпечить плавний перехід до нової системи фізичної безпеки. Хмарні системи, природно, більш гнучкі порівняно із застарілими системами, що полегшує додавання або видалення записів, встановлення нового обладнання або впровадження системи в нових місцях будівлі.

Безпроблемна системна інтеграція - ще однією перевагою систем фізичної безпеки, які працюють у хмарі, є можливість інтеграції з іншим програмним забезпеченням, програмами та системами. Хоча чудова система контролю доступу є важливою для будь-якого плану фізичної безпеки, наявність можливості підключення до інших інструментів безпеки зміцнює весь протокол безпеки.

Аудиторські стежки та аналітика - Однією з переваг систем контролю фізичної безпеки є те, що додаткові методи виявлення зазвичай включають звітність

та аудиторські стежки діяльності у будівлі. Ці дані мають вирішальне значення для загальної безпеки. Можливість легко та швидко виявити можливі слабкі місця у системі дозволяє впроваджувати нові плани фізичної безпеки для охоплення будь-яких вразливих районів. Якщо у вас трапиться порушення, наявність детальних звітів забезпечить необхідні докази для правоохоронних органів та допоможе швидко встановити винного. Аналіз ефективності заходів фізичного захисту дозволяє бути активними у пошуку ефективності, забезпечуючи краще управління та зменшуючи навантаження на кадрові та IT-команди.

Безпека є важливою для будь-якого великого бізнесу, незалежно від того, чи це одиночний офіс, чи глобальне підприємство. Найкращі практики фізичної безпеки, викладені в цьому посібнику, допоможуть створити кращу систему запобігання та виявлення вторгнень, а також відзначити різні міркування при плануванні процедур контролю фізичної безпеки. Ось короткий огляд найкращих практик впровадження фізичного захисту будівель.

По-перше, безпека периметра є важливою для запобігання проникненню. Фізичні бар'єри, такі як огородження та озеленення, можуть допомогти створити приватну власність, тоді як системи контролю доступу забезпечують наступний рівень безпеки, утримуючи небажаних людей поза будинком. Вибираючи систему контролю доступу, рекомендується вибрати хмарну платформу для максимальної гнучкості та масштабованості. Можна інтегрувати свій контроль доступу з іншими системами фізичної безпеки, такими як відеоспостереження та платформи управління користувачами, щоб зміцнити загальну безпеку. Як найкращу практику, слід регулярно перевіряти заходи фізичної безпеки, щоб переконатися, що немає недоглядів. Також важливо повідомити про будь-які зміни у системі фізичного захисту свою команду.

Висновки за розділом 1

Останнім часом моделювання загроз набуває все більшої популярності, але досі не є обов’язковим етапом або частиною загального життєвого циклу продукту,

не дивлячись на те, що існує досить багато методів та способів знаходження та адресування загроз в залежності від галузі, в якій це відбувається. Трьома найбільш популярними способами ідентифікації загроз є модель STRIDE, дерева атак та бібліотеки атак. Діаграми потоків даних та/або будь-які інші діаграми, які зображують взаємодію між процесами, є невід'ємною частиною якісної моделі. STRIDE та інші моделі, схожу на дану, дозволяють зручно класифікувати загрози та постійно їх оновлювати у разі необхідності.

Необхідність моделювання загроз пояснюється популяризацією понять безпеки та зокрема кібербезпеки серед широких мас, що створює попит серед споживачів на доведено безпечні продукти їхнього користування. Водночас даний процес є вигідним для виробників, тому що він може допомогти зекономити на витратах у подальшому, адже своєчасно (під час фаз створення архітектури, розробки та тестування) виявити та вирішити проблеми набагато легше. Також моделювання загроз є фундаментом для культури DevSecOps всередині організацій: певні закономірності та патерни, отримані у попередніх моделях, можуть стати стандартами (зразками) для нових.

Коли проблематика фізичного захисту розкрита, є доцільним роздивитися основні характеристики двофакторного контуру та надати визначення Інтернет речей.

РОЗДІЛ 2
ХАРАКТЕРИСТИКИ ДВОФАКТОРНОГО КОНТУРУ ТА ОСОБЛИВОСТІ ІНТЕРНЕТ РЕЧЕЙ

2.1 Характеристика об’єкту

Провідники-речовини, в яких присутня велика кількість вільних, не пов'язаних зарядів. Добрими провідниками струму вважаються метали, в яких багато вільних електронів і електроліти, в яких багато вільні позитивних і негативних іонів. Чим більше вільних зарядів знаходиться в речовині, тим краще його провідність. Провідність провідників залежить від структури речовини. Чим більше електронів на зовнішніх орбітах атомів і чим слабкіше вони пов'язані з ядром, тим більше електронів стає вільними, і речовина краще проводить струм.

Характеристикою провідності струму є питомий опір речовини, яке наводиться в довідниках. Розглянемо сенс питомого опору. Відома залежність опору провідників від параметрів цього провідника.

$$R = \rho \frac{l}{S},$$

де R — опір провідника (Ом);

l — довжина провідника (м);

S — переріз провідника ($м^2$);

p — питомий опір матеріалу (Ом·м);

Чим довше провідник, тим більше перешкод на своєму шляху зустрічає рухливий заряд, тим більше опір провідника току. Збільшення перетину провідника створює збільшення можливості для маневру вільного заряду, тим більше вільних зарядів може пройти в одиницю часу через поперечний переріз провідника, що знижує його опір.

Але опір провідника залежить і від його індивідуальних властивостей - число вільних зарядів в одиниці обсягу. Кожен провідник має свою певну кількість

вільних зарядів в одиниці об'єму при певній температурі. Цією характеристикою є питомий опір.

З огляду на наведену вище розмірність отримаємо фізичний сенс цієї величини.

Питомий опір в системі інтернаціональної (Сі) показує, яким опір володіє провідник довжиною 1м і перетином 1м2 . Такий провідник нескладно уявити-це кубічний метр речовини, рис. 1

В умовах виробництва таких провідників не застосовують, а застосовують провідник, перетин яких вимірюється А мм2, довжина в метрах. Тому крім питомого опору в системі СІ застосовують поняття питомого опору в технічній системі.

Питомий опір в технічній системі показує, яким опором володіє провідник довжиною 1м перетином 1 мм2. рис. 2.

Оскільки довжина провідників ви системах СІ і технічній системі однакові, а перетин по-різному, легко переконатися в тому, що чисельні значення цих параметрів відрізняються в стільки разів, у скільки відрізняється їх перетину, тобто 1м2 відрізняється від 1мм2 в 106 разів.

В таблиці 2.1. наведено деякі значення питомого опору в системі СІ і в технічній системі. Найбільш часто зустрічаються речовини в електротехнічній промисловості це: алюміній, мідь, срібло, графіт, ніхром, константан і т. д.

Таблиця 2.1.

Значення питомого опору

Речовина	ρci 10-6 *Ом м*	ρtex *Ом мм*^{2} */м*
Алюміній	0.027	0,027
Вольфрам	0.055	0.055
Графіт	8.0-20.0	8.0-20.0
Дюралюміній .	0.033	0.033
Константан	0.5	0.5

Продовження табл.2.1.

Мідь	0.017	0.017
Ніхром	1.0-1.1.	1.0-1.1.
Срібро	0.016	0.016

Порівняльні характеристики опорів цих речовин дозволяють визначити, які речовини найбільш краще застосовувати в якості провідників електричного струму.

З таблиці видно, що мінімальним питомим опором володіє мідь і срібло, які і є кращими провідниками струму.

Поряд з хорошими провідниками в електротехнічній промисловості знайшли широке застосування вольфрам і ніхром, що володіють значними питомими опорами. Такі речовини застосовуються в електронагрівальних приладах, реостатах і потенціометрах.

Поряд з поняттям питомого опору в електротехніці широко застосовують поняття провідності - величини зворотного опору. Провідність в 1 Сіменс має провідник опір 1 Ом.

Провідність (G) - найбільш зручна величина при розрахунках складних електричних ланцюгів з паралельними гілками.

При виборі апаратури управління і захисту, при виборі струмопровідних елементів найбільш часто застосовують поняття щільності струму і допустимої щільності струму.

$$\delta = \frac{I}{S},$$

де δ-щільність струму,

I-струм провідника,

S-перетин провідника.

Щільність струму показує, який струм проходить через одиничну площу поперечного перерізу провідника.

Для кожної речовини існує критична щільність струму, при якій речовина починає плавиться.

Електроматеріали можуть витримати не будь-який струм. В таб. 1.2. наведено критичні значення струму при різних перетинах проводу.

Таблиця 2.2.

Допустимі струми в проводах різного перетину

МАТЕРІАЛИ	Допустима сила сруму в *А* при перерізі провідника в $мм^2$							
	1,0	1,5	2,5	4,0	6,0	10	16	25	
Мідь		11	14	20	25	31	43	75	100
Алюміній		8	11	16	20	24	34	60	80
Залізо		-	-	8	10	12	17	30	-

З таблиці випливає, що при перетині 1мм2 мідний провід витримує струм 11 А, а алюмінієвий провід – 8 А, зазначені струми при перетині 1 мм2 і є критичні значення щільності струму.

Зазвичай доводиться вирішувати завдання по вибору перетину дроту по відомому струму. Для цього достатньо діюче значення струму розділити на критичну щільність струму, і ми знайдемо перетин провідника, менший перетин якого допускати не можна. Перетину дроту вибирається більше мінімально допустимого з певним коефіцієнтом запасу.

Діелектрик

Речовини, що містять мале число вільних зарядів називаються діелектриками. Струм в діелектриках залежить від властивостей речовини, з яких він виготовлений і практично являє собою струм витоку. Електрони, що знаходяться на орбітах атомів міцно пов'язані з ядром, тому електрон може стати вільним за певних умов.

Наприклад, при нагріванні діелектрика електрони збуджуються і стають вільними. Діелектрик починає пропускати струм. Приклад тому скло, яке при низьких температурах проявляє властивості діелектрика, а при нагріванні проявляє властивості провідника. Будь діелектрик при певному зовнішньому впливі стає провідником. Таким зовнішнім впливом може бути температура, радіація, механічний удар хімічний вплив і т. д.

Діелектрики, поміщені в електричне поле, його послаблюють, тому що в цьому полі вони поляризуються. Всередині діелектрика виникає внутрішньо електричне поле, спрямоване проти зовнішнього поля. Ступінь ослаблення електричного поля характеризується відносною діелектричної проникністю середовища, яка показує, у скільки разів даний діелектрик послаблює електричне поле.

Діелектрик, потрапивши в електричне поле, створює своє внутрішнє електричне поле, спрямоване проти зовнішнього поля. Це дуже важлива обставина дозволяє розташовувати близько один до одного дроти, що знаходяться під дуже високою напругою. Для цього достатньо провідник покрити діелектриком. Для більшої діелектричної міцності застосовують кілька шарів діелектриків, яку в побуті називають «ізоляція». Діелектричні властивості матеріалів прийнято відображать в таблицях, що вказують відносну діелектричну проникність. Відносна діелектрична проникність показує, у скільки разів даний діелектрик послаблює електричне поле.

В таб. 2.3. представлені деякі діелектричні матеріали та їх діелектрична проникність.

Таблиця 2.3.

Діелектричні матеріали та їх діелектрична проникність

РЕЧОВИНА	ε
Дистильована вода	80,1
Трансформаторне масло	2,0 – 2,5

Гетінакс	3,5 – 6,5

Продовження табл. 2.3

Дерево	2,2 – 3,7
Плексиглас	3,0 – 3,6
Поліхлорвініл	3,0 – 5,0
Гума	2,6 – 3,0
Слюда	4,0 – 8,0
Текстоліт	7,0
Фарфор	4,4 – 6,8

2.2 Визначення Інтернет речей.

Мільярди фізичних пристроїв по всьому світу відноситься до Інтернет речей, або IoT. Всі вони збирають і обмінюються даними. Пристрої, підключені до Інтернету, використовують вбудовані датчики для збору даних і, в деяких випадках, впливають на них. Підключені до IoT пристрої і машини можуть поліпшити нашу роботу і життя. Приклади застосування Інтернету речей: від розумного будинку, який автоматично регулює опалення та освітлення, до розумної фабрики, яка контролює промислові машини для пошуку проблем, а потім автоматично налаштовується, щоб уникнути збоїв. Завдяки появі наддешевих комп'ютерних чіпів і повсюдному поширенню бездротових мереж можна перетворити все, що завгодно, від чогось такого маленького, як таблетка, до чогось такого великого, як літак, в частину Інтернету речей. Підключення всіх цих різних об'єктів і додавання до них датчиків додає рівень цифрового інтелекту до пристроїв, які в іншому випадку були б тупими, дозволяючи їм передавати дані в режимі реального часу без участі

людини. Інтернет речей робить тканину навколишнього світу більш розумною і більш чуйною, об'єднуючи цифрову і фізичну всесвіти.

2.3 Сфери застосування IoT

Практично будь-який фізичний об'єкт може бути перетворений в пристрій Інтернету речей, якщо його можна підключити до Інтернету для управління або передачі інформації.

Лампочка, яку можна включити за допомогою програми для смартфона, є пристроєм Інтернету речей, як і датчик руху, розумний термостат в офісі або підключений вуличний ліхтар. Пристрій Інтернету речей може бути таким же пухнастим, як дитяча іграшка, або таким же серйозним, як вантажівка без водія. Деякі більші об'єкти самі по собі можуть бути заповнені безліччю дрібних компонентів Інтернету речей, таких як реактивний двигун, який тепер заповнений тисячами датчиків, що збирають і передають дані назад, щоб переконатися, що він працює ефективно. У ще більшому масштабі проекти "розумних міст" наповнюють цілі регіони датчиками, щоб допомогти нам зрозуміти і контролювати навколишнє середовище.

Термін IoT в основному використовується для пристроїв, які зазвичай не повинні мати підключення до Інтернету і які можуть взаємодіяти з мережею незалежно від дій людини. З цієї причини ПК зазвичай не вважається пристроєм Інтернету речей, як і смартфон, навіть незважаючи на те, що останній напханий датчиками. Однак розумні годинники, фітнес-браслети або інший пристрій можуть вважатися пристроєм Інтернету речей.

2.4 Переваги Інтернету речей для бізнесу

Переваги Інтернету речей для бізнесу залежать від конкретної реалізації; гнучкість і ефективність зазвичай є головними міркуваннями. Ідея полягає в тому, що підприємства повинні мати доступ до більшої кількості даних про свої власні

продукти та власні внутрішні системи, а також більшу здатність вносити зміни в результаті.

Виробники додають датчики до компонентів своїх продуктів, щоб вони могли передавати дані про те, як вони працюють. Це може допомогти компаніям визначити, коли компонент може вийти з ладу, і замінити його до того, як він призведе до пошкодження. Компанії також можуть використовувати дані, що генеруються цими датчиками, для підвищення ефективності своїх систем і ланцюжків поставок, оскільки вони матимуть набагато більш точні дані про те, що відбувається насправді.

Корпоративне використання Інтернету речей можна розділити на два сегменти: галузеві пропозиції, такі як датчики на електростанціях або пристрою позиціонування в реальному часі для охорони здоров'я; пристрої інтернету речей, які можуть використовуватися у всіх галузях, таких як інтелектуальні системи кондиціонування повітря або системи безпеки.

У той час як галузеві продукти з'являться на ранній стадії, до 2020 року Gartner прогнозує, що міжгалузеві пристрої досягнуть 4,4 мільярда одиниць, в той час як вертикальні пристрої складуть 3,2 мільярда одиниць. Споживачі купують більше пристроїв, але компанії витрачають більше: аналітична група заявила, що в той час як споживчі витрати на пристрої IoT в минулому році склали близько 725 мільярдів доларів, витрати компаній на IoT досягли 964 мільярдів доларів. До 2020 року витрати бізнесу і споживачів на обладнання IoT досягнуть майже 3 трлн доларів.

За прогнозами, основними галузями для Інтернету речей будуть дискретне виробництво (витрати на 119 мільярдів доларів), обробне виробництво (78 мільярдів доларів), транспорт (71 мільярд доларів) і комунальні послуги (61 мільярд доларів). Для виробників проекти з підтримки управління активами будуть мати ключове значення; в галузі транспорту пріоритет буде віддаватися моніторингу вантажів і управління парком. Витрати на IoT у комунальній галузі переважатимуть над проектами інтелектуальних мереж для електроенергії, газу та води.

За прогнозами, споживчі витрати на IoT досягнуть 108 мільярдів доларів, що зробить його другим за величиною галузевим сегментом: більша частина витрат припадатиме на Розумний будинок, особисте оздоровлення та інформаційно-розважальну систему для підключених транспортних засобів.

У разі використання, виробничі операції ($100 млрд), управління виробничими активами ($44,2 млрд), Розумний будинок ($44,1 млрд) і моніторинг вантажних перевезень ($41,7 млрд) будуть найбільшими напрямками інвестицій.

2.5 Питання кібербезпеки під час використання IoT.

Безпека – одна з найбільших проблем Інтернету речей. Ці датчики в багатьох випадках збирають надзвичайно конфіденційні дані-наприклад, про те, що ви говорите і робите в своєму власному будинку. Збереження цієї безпеки є життєво важливим для довіри споживачів, але до цих пір послужний список безпеки Інтернету речей був надзвичайно поганим. Занадто багато пристроїв Інтернету речей мало замислюються про основи безпеки, таких як шифрування даних при передачі і в стані спокою.

Недоліки в програмному забезпеченні-навіть у старому і добре використовуваному коді-виявляються регулярно, але багато пристроїв Інтернету речей не мають можливості виправлятися, що означає, що вони постійно піддаються ризику. Хакери в даний час активно націлюються на пристрої Інтернету речей, такі як маршрутизатори і веб-камери, тому що притаманне їм відсутність безпеки дозволяє легко компрометувати їх і перетворювати в гігантські ботнети.

Недоліки залишають розумні домашні пристрої, такі як холодильники, духовки та посудомийні машини, відкритими для хакерів. Дослідники виявили 100 000 веб-камер, які можна легко зламати, в той час як деякі підключені до Інтернету. Розумний годинник для дітей містить уразливості в системі безпеки, які дозволяють хакерам відстежувати місце розташування користувача, підслуховувати розмови або навіть спілкуватися з користувачем.

Уряди все більше турбуються про ризики тут. Уряд Великобританії опублікував свої власні рекомендації щодо безпеки споживчих пристроїв Інтернету речей. Він очікує, що пристрої матимуть унікальні паролі, що компанії нададуть загальнодоступну точку контакту, щоб кожен міг повідомити про вразливість (і що вони будуть усунені), і що виробники будуть явно вказувати, як довго пристрої будуть отримувати оновлення безпеки. Це скромний список, але для початку.

Коли вартість створення інтелектуальних об'єктів стане незначною, ці проблеми стануть тільки більш поширеними і важкорозв'язними.

Все це відноситься і до бізнесу, але ставки ще вище. Підключення промислового обладнання до мереж Інтернету речей збільшує потенційний ризик виявлення і атаки хакерами цих пристроїв. Промислове шпигунство або руйнівна атака на критичну інфраструктуру є потенційними ризиками. Це означає, що підприємствам потрібно буде переконатися, що ці мережі ізольовані та захищені, а шифрування даних із захистом датчиків, шлюзів та інших компонентів є необхідністю. Однак нинішній стан технологій Інтернету речей ускладнює їх забезпечення, так само як і відсутність послідовного планування безпеки Інтернету речей в різних організаціях. Це дуже тривожно, враховуючи задокументовану готовність хакерів втручатися в промислові системи, які були підключені до Інтернету, але залишилися незахищеними.

IoT усуває розрив між цифровим світом і фізичним світом, а це означає, що злом пристроїв може мати небезпечні наслідки в реальному світі. Злом датчиків, що контролюють температуру на електростанції, може змусити операторів прийняти катастрофічне рішення; взяття під контроль автомобіля без водія також може призвести до катастрофи.

2.6 Протоколи, які можна застосовувати у системі з двофакторним контуром.

Zigbee – це бездротовий протокол передачі даних, який широко використовується найбільшими провайдерами екосистем розумного дому: Amazon’s

Echo Plus, Samsung SmartThings, Signify (Philips Hue) та інші. Максимальний розмір мережі на основі даного стандарту – 65000 вузлів, а швидкість передачі даних – 250 кбіт/с. Шифрування забезпечується AES-128 на мережевому рівні (даний алгоритм шифрування доступний також на прикладному рівні). Офіційний сайт Zigbee Alliance вказує, що Zigbee – це єдине повноцінне рішення для IoT, від сітчастої мережі до універсальної мови, що дозволяє смарт об'єктам працювати разом. Zigbee передає пакети даних енергоефективним шляхом, через що споживання енергії зводиться до мінімуму. Також даний протокол розроблено із можливістю передньої та зворотної сумісності (застарілі пристрої мають змогу під'єднатися до мережі Zigbee так само, як і пристрої Zigbee можуть під'єднатися до застарілих мереж).

Z-Wave – це бездротова радіочастотна технологія, що використовується переважно саме для автоматизації домашніх систем, яка працює на частоті 908.42 МГц у США та Канаді та 868.40 МГц в Європейському Союзі та яка надає смарт об'єктам можливість спілкуватися один з одним. Z-Wave – це високомасштабна технологія, що використовує сітчасту топологію мережі та дозволяє контролювати від 1 до 232 пристроїв на території одного розумного дому. У 2013 році Z-Wave Alliance представили розширену версію протоколу – Z-Wave Plus. Нова версія підтримує більшу на 67% дальність дії, а її пропускна здатність сягає 100 кбіт/с, що на 250% перевищує попередню. У специфікації за 2008 рік (Z-Wave S0 Security) було представлено шифрування за допомогою алгоритму AES-128, проте у 2013 році виявилося, що у момент первинної ініціалізації перед початком сеансу зв'язку пристрою передавався ключ шифрування, який складався зі 128 нулів. У 2016 році вийшла оновлена версія специфікації, Z-Wave S2 Security, в якій використовується протокол Діффі-Геллмана під час первинної видачі ключа.

KNX – це відкритий стандарт для комерційної та домашньої автоматизації. Дана технологія контролює автоматизацію таких функцій як опалення, вентиляція та кондиціювання повітря, мультимедіа, системи освітлення, керування енергією, безпека та ін. KNX відповідає стандартам EN 50090, EN 13321-1 та ISO/ IEC 14543 та забезпечує усі пристрої та функції можливістю миттєвої та віддаленої комунікації, використовуючи єдину мову.

DASH7 (D7A) – це відкритий протокол для бездротового зв'язку, розроблений для сенсорних та датчикових приладів, що використовують приватні мережі. Сенсори надійно повідомляють про події, а датчики отримують команди з приблизною затримкою в 1 секунду, при цьому споживаючи всього 30 мкА. D7A підходить для міських та промислових мережевих установок, де необхідно поєднати сенсори та датчики у діапазоні до 500 м.

Wi-Fi – це бездротовий протокол, який було створено з метою заміни на нього Ethernet., який підходить для підтримки широкосмугових та вузькосмугових IoT-додатків. Wi-Fi 802.11a/b/g/n/ac легко імплементувати, а вартість інфраструктури та пристроїв досить низька, проте мінусами є споживання великої кількості енергії, скупчення спектру та помірний діапазон. У специфікаціях для WiFi HaLow (802.11ah) та HEW (802.11ax) було опубліковано рішення щодо проблем з дальністю та енергоспоживання для IoT систем.

Bluetooth – це протокол з низькою потужністю та діапазоном, проте з високою пропускною здатністю. Завдяки тому, що Bluetooth використовує слабкі сигнали, завади лімітовані і пристрої можуть обмінюватися інформацією у шумних середовищах. Даний протокол корисний для рішень у розумному домі, адже його нові версії дозволяють створювати самовідновлювану сітчасту мережу, у якій вихід з ладу одного девайсу не спричинить проблем для спілкування інших між собою.

BLE було випущено у 2010 році як низько енергетичний варіант класичного Bluetooth. Оскільки BLE може частково використовувати апаратне забезпечення Bluetooth, то пристрій, який підтримує класичний Bluetooth, також може підтримувати BLE за умов низьких додаткових витрат. Таким чином, BLE використовується у смартфонах, які можна використовувати і для збору даних або передачі команд оточуючим датчикам та сенсорам, і як шлюз для взаємодії між ними та Інтернетом.

NFC – дана технологія бере свій початок в іншій – технології радіочастотної ідентифікації (RFID), яка використовує електромагнітні поля для кодування та зчитування інформації. Будь-який пристрій з підтримкою NFC має невеликий чіп, який активується, якщо він знаходиться в безпосередній близькості від іншого

пристрою з NFC (10 сантиметрів або менше). Таким чином, NFC забезпечує просту та безпечну двосторонню взаємодію між електронними пристроями.

IEEE 802.15.4 – це сімейство бездротових технологій, призначених для забезпечення моніторингу і контролю за застосунками у бездротовій особистій локальній мережі (Wireless Personal Area Network – WPAN). Публікація першої версії у 2003 році була знаковою, оскільки вперше було представлено відкритий стандарт, націлений на низькошвидкісний зв'язок з акцентом на простоту та низьке енергоспоживання. IEEE 802.15.4 не розроблений для конкретного домену додатків. Натомість він задуманий як загальна технологія, яка врешті стала основою певних архітектурних протоколів, що підтримують IPv6, а також рішень для протоколів не на основі IP, таких як ZigBee. Тим не менш, IEEE 802.15.4 був оптимізований для конкретних середовищ, таких як IEEE 802.15.4e Time Slotted Channel Hopping (TSCH), що призначений для подолання пошкоджень в індустріальному середовищі.

LoRaWAN – це неліцензована бездротова технологія, яка входить до нової категорії широкосмугових мереж з низькою потужністю (LPWAN). LoRaWAN використовує технологію LoRa на фізичному рівні, що дозволяє збільшити діапазон зв'язку. На основі топології «Зірка», за допомогою якої шлюз збирає дані від сотень тисяч пристроїв, таких як датчики, вона пропонує низьку інфраструктурну вартість за рахунок значного обмеження швидкості передачі повідомлень та швидкості передачі бітів.

DECT-ULE – це низькоенергетичний варіант DECT, який є основною технологією, що використовується для передачі голосу та даних для внутрішньої бездротової телефонії. Використання DECT-ULE було запропоновано для того, щоб забезпечити зв'язок між шлюзом та датчиками або приладами в будинку, використовуючи обладнання DECT.

Ethernet – найчастіше використовується у технологіях локальної мережі (LAN). В його основі лежить стандарт IEEE 802.3. У системі IoT Ethernet можна використовувати для підключення стаціонарних або нерухомих пристроїв IoT. Наприклад, кабелі Ethernet використовуються для з'єднання комп'ютерів з маршрутизаторами для забезпечення підключення до Інтернету.

Thread – протокол бездротового зв'язку, розроблений групою компаній, включаючи Nest, Samsung, QUALCOMM та OSRAM та призначений для того, щоб пристрої в його протоколі могли спілкуватися навіть тоді, коли мережа WiFi виявляється недоступною. Як і Zigbee, Thread побудований за допомогою відкритих стандартів (включаючи IP) і спілкується на радіостандарті 802.15.4. З його допомогою можна полегшити зв'язок між пристроями або між пристроями та хмарою.

2.7 Проблеми, притаманні об'єктам IoT системи з двофакторним контуром

Усі виклики, з якими стикаються кіберфізичні об'єкти, можна розглядати, розділивши на три категорії відповідно до рівня представлення, а саме – пристрої, комунікація та сервіси.

Перш за все, фізичні пристрої виявляються вразливими через ресурсне обмеження, адже найчастіше вони працюють на основі батарей та використовують центральні процесори з низькою потужністю і лімітовану пам'ять. Такі характеристики унеможливлюють імплементацію дорогих та енергозатратних криптографічних алгоритмів і наражають девайси на атаки на відмову в обслуговуванні. Також майже завжди пристрої не мають ні клавіатури, ні будь-якого іншого методу вводу даних, а отже користувачам доводиться комунікувати з ними, використовуючи смартфони або сайти. Фізична доступність пристроїв, у свою чергу, робить їх вразливими для атак з використанням фізичних маніпуляцій.

Різні протоколи, які використовуються для взаємозв'язку пристроїв у розумному домі, вимагають використання проміжних шлюзів, що є значним обмеженням для впровадження комплексних рішень безпеки між кінцевими пристроями та Інтернет-додатками. До того ж більшість протоколів не гарантує доставку пакета. Деякі пристрої можуть під'єднуватися до домашньої мережі та покидати її у будь-який час з будь-якої локації, що перетворює розробку стійких

алгоритмів захисту у необхідність і змушує замислитися над якісним відслідковуванням кінцевих пристроїв та їх управлінням.

Віддалене репрограмування є частиною боротьби над вразливостями безпеки, проте не всі пристрої можуть йому піддаватися, адже операційні системи або стек протоколів не обов'язково підтримують властивість динамічного виправлення. Певні пристрої, наприклад, розумні лічильники, розроблялися з наміром залишатися в режимі онлайн протягом багатьох років без необхідності заміни або обслуговування окремих компонентів.

2.8 Атаки, націлені на систему з двофакторним контуром

Наведемо класифікацію типових атак (табл. 2.2) відповідно до певного архітектурного рівня. Структурно це можна уявити так:

Таблиця 2.4.

Класифікація атак на системи з використанням двофакторного контуру [20]

Рівень	**Протокол**	**Атака**
Прикладний	CoAP, XMPP, MQTT	XMPPloit
Транспортний	TCP, UDP	UDP флуд, TCP SYN флуд, десинхронізація
Мережевий	MPL, RPL, 6LoWPAN	KillerBee, атака «чорна діра», зміна інформації про маршрутизацію, перехоплення пакетів, Hello Flood, Wormhole, Sybil, Tiny Fragmentation
Канальний	802.15.4, 802.11, 802.15.1	KillerBee, атака GTS, зворотна маніпуляція, ACK атака
Фізичний	802.15.4, 802.11, 802.15.1	Глушіння, фізичні

		маніпуляції

Головні атаки фізичного рівня – це глушіння та фізичні маніпуляції. Глушіння представляє собою випромінювання радіосигналів з метою часткового або повного порушення можливості цільового пристрою спілкуватися. Глушіння, на відміну від бездротових перешкод, є умисним та має певну ціль. Наслідками даної атаки можуть бути відмова в обслуговуванні пристрою (через виснаження батареї внаслідок постійної необхідності ретрансляції сигналів), а також навіть порушення зв'язку у всій цільовій мережі. Введення зловмисного коду для порушення роботи мережі або передачі усіх даних до атакуючого, добування інформації про рівень безпеки (наприклад, викрадення драйверу або підключення до пристрою для отримання ключів шифрування) і дуплікація пристроїв з встановленим зловмисним програмним забезпеченням для отримання чутливої інформації або зменшення ефективності роботи пристроїв у мережі – це приклади фізичних маніпуляцій.

KillerBee, атака GTS (Guaranteed Time Slot), атака ACK та зворотна маніпуляція – усе це приклади атак на канальному рівні. KillerBee – це фреймворк, що дозволяє експлуатувати вразливості у мережах з такими протоколах як ZigBee та 802.15.4 та робить легшими для зловмисника процеси сніфінгу, ін'єкції трафіку та розшифрування пакетів. Атака GTS базується на властивостях суперфрейму IEEE 802.15.4. У [22] описано, що слоти GTS створюють вразливу точку, яка надає зловмиснику можливість порушити зв'язок між пристроєм та його шлюзом у результаті чого він може отримати виділений час GTS та бути в змозі створити перешкоди в будь-який із цих моментів. Подібне втручання спричиняє зіткнення та пошкодження пакетів даних, що передаються між пристроями, та змушує цільові вузли повторно передавати пакети даних. Застосування зловмисником атаки ACK до цільового середовища розумного будинку відбувається через підслуховування бездротового каналу передачі даних. Тобто, він може заблокувати пристрою-приймачу можливість прийому переданого пакету, а після цього ввести в оману пристрій-відправник, надіславши підроблений ACK, який нібито надійшов від приймального пристрою. Зворотна маніпуляція можлива у мережах на основі

CSMA/CA (наприклад, IEEE 802.11 та IEEE 802.15.4). Під час такої атаки зловмисний пристрій постійно обирає невеликий інтервал для створення перешкод, використовуючи розподілену координаційну функцію, що унеможливлює управління доступом до середовища для цільових пристроїв.

На мережевому рівні мережа розумного дому схильна до атак флудингу, спуфінгу, сніфінгу, перехоплення та модифікації даних та DoS. Специфічною саме для цієї системи атакою є атака «чорна діра» на RPL (Routing Protocol for Low-Power and Lossy Networks), що власне спрямована на реалізацію RPL у ContikiOS. Чорна діра, яку ініціює компрометований вузол, що несанкціоновано діє в мережі і скидає маршрутизовані через неї пакети, викликає перебої в потоці даних мережі. Така атака може бути ефективно замаскована і призвести до того, що атакована мережа поводиться так само, як і неатакована. Проте ця атака успішно здійснюється лише на пристроях на базі ContikiOS [24], а інші ОС (наприклад, Tiny OS та RIOT OS), що мають інші реалізації протоколу, не виявляються вразливими до неї.

Загальновідомі атаки транспортного рівня, такі як флудинг і десинхронізація, і прикладного можуть бути націлені і на мережу розумного дому, а специфічною атакою прикладного рівня є XMPPloit. Це експлойт, що використовує командний рядок для атаки на з'єднання XMPP та користується вразливостями на стороні клієнта та сервера, базуючись на протоколі XMPP. XMPPloit може змусити розумний домашній пристрій не шифрувати свої комунікації задля того, щоб зловмисник мав змогу їх читати та модифікувати під час передачі.

2.9 Підходи по забезпеченню безпеки

Способи протидії загрозам безпеки та конфіденційності у розумному домі можна розділити на рішення мережевого рівня та рішення пристроїв [25]. У роботі [21] пропонується також брати до уваги рішення на рівні сервісів.

Захист на рівні пристроїв базується на елементах безпеки, які одразу в них вбудовуються. Прикладами цього слугують апаратне шифрування, дизайн з підходом fail-secure (якщо немає доступу до живлення, то пристрій стає

заблокованим, а не навпаки) та механізми контролю доступу на основі пристроїв. Одним із запропонованих підходів є впровадження процедур безпеки на канальному рівні, сумісних з IEEE 802.15.4, в апаратні шифри [26]. Також розроблено оптимізовані версії криптографічних алгоритмів, такі як ECDSA, для обмежених середовищ.

Проблемою залишається те, що більшість пристроїв мають суворі обмеження в ресурсах, і нові стандарти у сфері безпеки є переважно експериментальними, а це обмежує їх більш широке застосування та промислове впровадження. Крім того, це може бути неможливим у великих масштабах з потенційно високими додатковими витратами порівняно з вартістю традиційних пристроїв IoT.

Рішення на рівні комунікацій ефективні, коли дані передаються між пристроями, сервісами та кінцевими користувачами. Популярні схеми передбачають використання віртуальних приватних мереж (VPN), брандмауерів та систем виявлення вторгнень (IDS) або систем запобігання вторгнень (IPS). Такий підхід зазвичай реалізується в центральному шлюзі/проксі та/або в хмарі.

Застосування брандмауерів, IDS та IPS в контексті розумного дому описується у роботі [27]. Проте у роботі [28] висловлюються рекомендації щодо використання анонімної системи на основі TOR для захисту конфіденційності користувачів та підвищення безпеки приладів розумного дому. Існують також спеціалізовані пристрої для розумного дому, які необхідно підключити до домашнього маршрутизатора та які виконують функції мережевих воротарів, наприклад, Cujo, Dojo та Keezel. Cujo і Dojo виступають в якості пристроїв брандмауера, що відстежують, аналізують та блокують загрози в режимі реального часу, а Keezel створює тунель VPN для шифрування пристроїв та з’єднань.

На практиці залишається викликом те, що деякі пристрої мають можливість «бродити» по мережі та спілкуватися за допомогою зашифрованих каналів, а це в свою чергу ускладнює аналіз трафіку за умови відсутності технології докладного аналізу пакетів (DPI – Deep Packet Inspection). Крім того, пристрої залишаються вразливими до локальних атак, таких як встановлення зловмисного коду через скомпрометовану пам’ять.

Підходи на рівні сервісів орієнтовані на програмні ресурси високого рівня. Вони передбачають безпечні процеси розробки, такі як тестування безпеки, принципи безпечного проектування та маскування даних. Останнє може включати використання методів збереження конфіденційності, таких як k-анонімність та криптографічні схеми (наприклад, шифрування на основі атрибутів).

Проект Open Web Application Security Project бере участь у наданні безпечних вказівок щодо розробки, таких як рамки оцінювання та посібники з тестування, пристроїв IoT. Інші організації, такі як Builditsecure.ly та I Am the Cavalry, надають вказівки щодо створення інженерних процесів безпеки. Існують також сайти, такі як BugCrowd, які дозволяють розробникам відправити їх код на перевірку до спеціалістів з безпеки.

Проте у реальному світі не існує офіційного органу управління, який би гарантував кінцевим споживачам репутацію конкретного постачальника послуг. Крім того, деякі методи, незважаючи на плюси у вигляді підвищення конфіденційності та безпеки, можуть мати побічні ефекти (наприклад, втрата інформації).

Висновки за розділом 2

Інтернет-речей – це поняття, яке набуло надзвичайної популярності протягом останнього десятиліття. IoT зараз впроваджується майже у кожну сферу людського життя, починаючи від звичних усім розумних фітнес браслетів та закінчуючи пристроями, які використовуються на потужних виробництвах. IoT зустрічається у сфері охорони здоров’я, енергоспоживання, розробки автономних транспортів пересування, розумних підприємств, розумних міст та навіть сільського господарства. Така популярність легко пояснюється: IoT девайси роблять щоденні процеси простішими та ефективнішими, економлять час та сили. Проте поруч з великою популярністю стоїть також і велика відповідальність. Все частіше обговорюється захищеність IoT та безпека тих, хто користується його послугами. Багато провідних країн замислюється про впровадження рекомендацій на

державному рівні та/або законів щодо регулювання діяльності IoT, чітко визначаючи поняття та прописуючи відповідальність, яку має нести сторона, що є провайдером сервісів, у разі порушення конфіденційності, цілісності та доступності інформації, яка циркулює у мережі.

Проте як можна поєднати систему з двофакторним контуром таки чином, щоб захист відбувався тільки в бік несанкціонованого доступа? За допомогою системи з девайсів власника об'єкта інформаційного продукта, Bluetooth, Wi-Fi або NFC з'єднання. Однак необхідно розуміти, що будь-який з пристроїв може бути вразливим, тим самим ставлячи під загрозу безпеку інших пристроїв у домі та навіть мережі, що врешті-решт є критичним для персональних даних, які там зберігаються. Через це питання безпеки та захищеності є ключовими та найбільш обговорюваними серед експертів, які намагаються захистити комунікацію між пристроями у мережі, та кінцевих користувачів, які розуміють, що розумний не завжди означає безпечний.

Через надану характеристику двофакторного контуру та визначення IoT слід дослідити контур фізично, впровадити розрахунки та охарактеризувати модель загроз.

РОЗДІЛ 3
МОДЕЛЮВАННЯ СИСТЕМИ З ДВОФАКТОРНИМ КОНТУРОМ

3.1 Вихідні дані

Для впровадження двофакторного контуру у систему із декількох приладів, маємо чітко розуміти структуру побудови та розташування декількох елементів. Як правило, початок роботи з одно-, дво- і багатофакторними контурами починається саме з вихідної схеми (рис. 3.1).

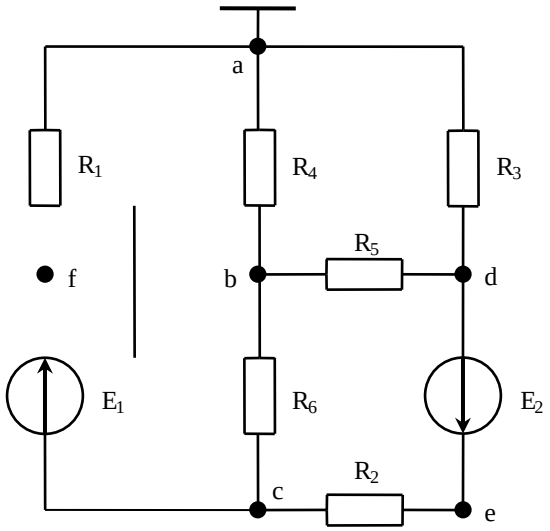

Рисунок 3.1-Вихідна схема

Введемо таблицю 3.1 для надання параметрів ланцюга, з яким матимемо можливість обирати оптимальний варіант в залежності від запитів захисту інформаційних продуктів. Після внесення даних, обираємо потрібний параметр і рухаємося за наступним алгоритмом:

Таблиця 3.1

Дані для розрахунку

Параметри ланцюга							
R_1	R_2	R_3	R_4	R_5	R_6	E_1	E_2
Ом						В	
1	1	5	1	8	1	2	3

0	8		0		0	0	5

Порядок розрахунку ланцюга постійного струму:

1. Перетворити вихідну схему до двоконтурної, замінивши трикутник опорів еквівалентної зіркою.
2. Для вихідної схеми скласти систему рівнянь за законами Кірхгофа і вирішивши її за допомогою ЕОМ, знайти струми в гілках.
3. Для перетвореної схеми скласти систему рівнянь за методом контурних струмів і розрахувати струми у всіх гілках.
4. Для вихідної схеми скласти систему рівнянь за методом вузлових потенціалів і потім розрахувати струми в гілках.
5. Для перетвореної схеми в одній з гілок розрахувати струм методом еквівалентного генератора.
6. Скласти баланс потужностей.
7. Побудувати потенційну діаграму для будь-якого замкнутого контуру, що включає ЕРС, вважаю заземлену точку.

Відтворюємо перетворення трикутника опорів в еквівалентну зірку

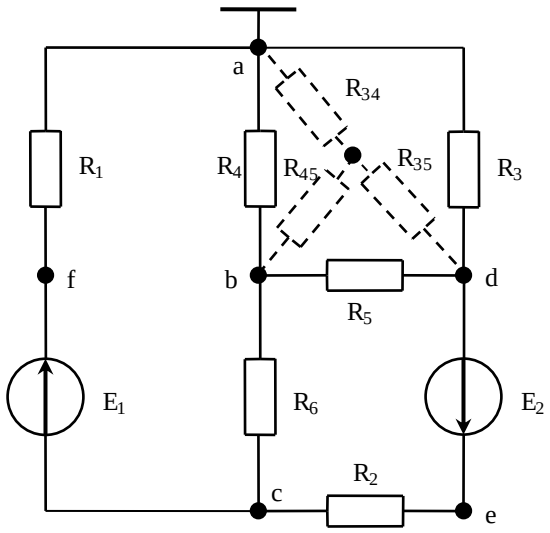

Рисунок 3.2 - Схема перетворення трикутника опорів в еквівалентну зірку

Перетворимо знайдену схему, щоб уникнути подібної зірки.

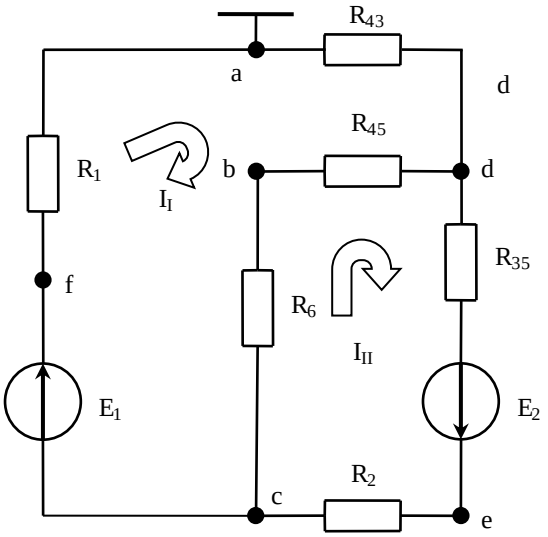

Рисунок 3.3 - Перетворена схема

$$R_{43} = \frac{R_4 \cdot R_3}{R_3 + R_4 + R_5};\ R_{35} = \frac{R_3 \cdot R_5}{R_3 + R_4 + R_5};\ R_{45} = \frac{R_4 \cdot R_5}{R_3 + R_4 + R_5};$$

Якщо в ланцюгах постійного струму ємності і індуктивності помітні тільки при перехідних процесах, то в ланцюгах змінного струму дані компоненти проявляють себе набагато більш значно:

$$R_{43} = \frac{10 \cdot 5}{5+10+8} = 2.174 Ом;$$

$$R_{35} = \frac{5 \cdot 8}{5+10+8} = 1.739 Ом;$$

$$R_{45} = \frac{10 \cdot 8}{5+10+8} = 3.478 Ом;$$

Історично склалося, що опір R в законі Ома для ділянки ланцюга вважається основною характеристикою провідника, так як залежить виключно від параметрів цього провідника.

3.2 Розрахунок струмів в гілках, з використанням законів Кірхгофа

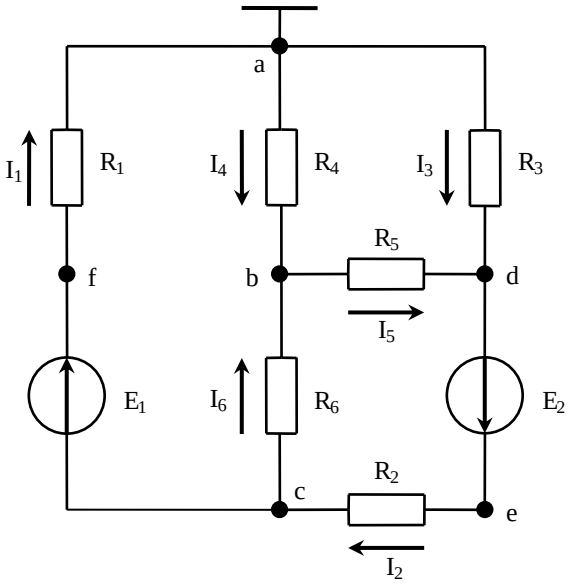

Рисунок 3.4 - Розрахункова схема

Сума всіх струмів, що втікають у вузол, дорівнює сумі всіх струмів, що випливають з вузла. Алгебраїчна сума всіх струмів у вузлі дорівнює нулю. Отже, можемо записати вираз для першого закону Кіргофа:

$$\sum_{k=1}^{n} I_k = 0$$

Алгебраїчна сума ЕРС, що діють в замкнутому контурі, дорівнює алгебраїчній сумі падінь напруги на всіх резистивних елементах в цьому контурі.

Тут термін «алгебраїчна сума» означає, що як величина ЕРС так і величина падіння напруги на елементах може бути як зі знаком «+», так і зі знаком «-». При цьому визначити знак можна за наступним алгоритмом:

1. Вибираємо напрямок обходу контуру (два варіанти або за годинниковою, або проти).
2. Довільно вибираємо напрямок струмів через елементи ланцюга.
3. Розставляємо знаки для ЕРС і напруг, що падають на елементах за правилами:

- ЕРС, що створюють струм в контурі, напрямок якого збігається з напрямок обходу контуру записуються зі знаком «+», в іншому випадку ЕРС записуються зі знаком «-».

- напруги, що падають на елементах ланцюга записуються зі знаком»+«, якщо струм, що протікає через ці елементи збігається у напрямку з обходом контуру, в іншому випадку напруги записуються зі знаком» -".

Тобто сміливо можемо записувати другий закон Кірхгофа:

$$\sum_{k=1}^{n} I_k \cdot R_k = \sum_{k=1}^{n} E_k$$

Щоб підтвердити справедливість формулювання, перенесемо струми в ліву частину виразу, тим самим отримаємо:

$$\begin{cases} I_1 - I_3 - I_4 = 0 \\ I_4 - I_5 + I_6 = 0 \\ -I_2 + I_3 + I_5 = 0 \\ I_1R_1 + I_4R_4 - I_6R_6 = E_1 \\ I_3R_3 - I_4R_4 - I_5R_5 = 0 \\ I_2R_2 + I_5R_5 + I_6R_6 = E_2 \end{cases} \quad \begin{cases} I_1 - I_3 - I_4 = 0 \\ I_4 - I_5 + I_6 = 0 \\ -I_2 + I_3 + I_5 = 0 \\ 10I_1 + 10I_4 - 10I_6 = 20 \\ 5I_3 - 10I_4 - 8I_5 = 0 \\ 18I_2 + 8I_5 + 10I_6 = 35 \end{cases}$$

Виведені дані внесемо в таблицю:

Таблиця 3.2

Дані з обрахунків

1	0	-1	-1	0	0	0	I_1 =	1,695	A
0	0	0	1	-1	1	0	I_2 =	1,741	A
0	-1	1	0	1	0	0	I_3 =	1,342	A
10	0	0	10	0	-10	20	I_4 =	0,352	A
0	0	5	-10	-8	0	0	I_5 =	0,399	A
0	18	0	0	8	10	35	I_6 =	0,047	A

Підвищення щільності струму, що є характерною загальною тенденцією розвитку техніки промислового електролізу, завжди пов'язане зі збільшенням незворотних витрат напруги через зростання електродних потенціалів, омічних опорів і концентраційної поляризації. Тому при інтенсифікації процесу за рахунок підвищення щільності струму завжди застосовують заходи щодо зниження окремих складових загального балансу напруги на осередку, щоб уникнути надмірного зростання напруги на електролізері. Зазвичай для цієї мети розробляють способи

активізації поверхні анодів і катодів для зниження перенапруги на них прагнуть знизити втрати напруги в електроліті, електродах і струмопідводах.

3.3 Розрахунок струмів в гілках, методом контурних струмів

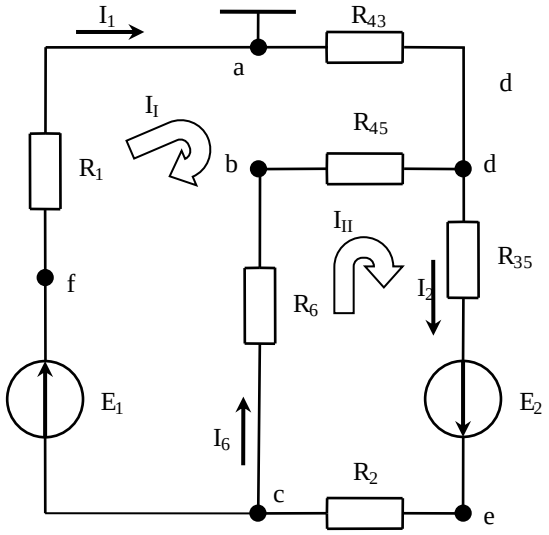

Рисунок 3.5 - Розрахункова схема

Скористаємося наслідком із закону Ома:

$$\begin{cases} E_1 = I_I(R_1 + R_{43} + R_{45} + R_6) - I_{II}(R_6 + R_{45}), \\ E_2 = I_{II}(R_2 + R_6 + R_{45} + R_{35}) - I_I(R_{45} + R_6) \end{cases}$$

За допомогою ключа управління (вибирання) можна вибрати, або постійна напруга, або змінна напруга на виході. У нашому випадку використовується постійна напруга.

Підставимо чисельні значення:

$$\begin{cases} 20 = I_I(10 + 2.174 + 3.478 + 10) - I_{II}(10 + 3.478), \\ 35 = I_{II}(18 + 10 + 3.478 + 1.739) - I_I(3.478 + 10) \end{cases}$$

$$\begin{cases} 20 = 25.652 \cdot I_I - 13.478 \cdot I_{II} \\ 35 = -13.478 \cdot I_I + 33.217 \cdot I_{II} \end{cases}$$

Електричний струм-це спрямований потік електронів від точки В з потенціалом мінус до точки а з потенціалом плюс. І чим вище різниця потенціалів

між цими точками, тим більше електронів переміститься з точки в В точку А, тобто струм в ланцюзі збільшиться, за умови, що опір ланцюга залишиться незмінним.

Висловити I_{II}:

$$33.217 \cdot I_{II} = 35 + 13.478 \cdot I_I;$$
$$I_{II} = \frac{35 + 13.478 \cdot I_I}{33.217};$$
$$25.652 \cdot I_I - \frac{13.478 \cdot (35 + 13.478 \cdot I_I)}{33.217} = 20;$$
$$25.652 \cdot I_I - 5.469 \cdot I_I = 20 + 14.201;$$
$$20.183 \cdot I_I = 34.201;$$
$$\underline{I_I = 1.695.}$$
$$25.652 \cdot 1.695 - 13.478 \cdot I_{II} = 20;$$
$$13.478 \cdot I_{II} = 23.480;$$
$$\underline{I_{II} = 1.742}$$

$$I_1 = I_I = 1.695A; \quad I_2 = I_{II} = 1.742A; \quad I_6 = \left| I_I - I_{II} \right| = 0.047A$$

3.4 Розрахунок струмів в гілках, методом вузлових потенціалів

Для розглянутої схеми (див. рис. 1) за нульовий приймається потенціал вузла а ($\varphi_a = 0$). При цьому система рівнянь набуде вигляду:

$$\begin{cases} \varphi_b(q_4 + q_5 + q_6) - \varphi_c q_6 - \varphi_d q_5 = 0, \\ -\varphi_b q_6 + \varphi_c(q_1 + q_6 + q_2) - \varphi_d q_2 = E_1 q_1 - E_2 q_2, \\ -\varphi_b q_5 - \varphi_c q_2 + \varphi_d(q_2 + q_3 + q_5) = E_2 q_2 \end{cases}$$

де провідності гілок рівні:

$$q_1 = \frac{1}{R_1}; \quad q_2 = \frac{1}{R_2}; \quad q_3 = \frac{1}{R_3}; \quad q_4 = \frac{1}{R_4}; \quad q_5 = \frac{1}{R_5}; \quad q_6 = \frac{1}{R_6}.$$

Підставивши чисельні значення, отримали:

$$\begin{cases} 0.325 \cdot \varphi_b - 0.1 \cdot \varphi_c - 0.125 \cdot \varphi_d = 0, \\ -0.1 \cdot \varphi_b + 0.256 \cdot \varphi_c - 0.055 \cdot \varphi_d = 0.056, \\ -0.125 \cdot \varphi_b - 0.055 \cdot \varphi_c + 0.38 \cdot \varphi_d = 1.944 \end{cases}$$

Таблиця 3.3

Дані з обрахунків

0,325	-0,1	-0,125	0	$\varphi_{b=}$	3,521
-0,1	0,255	-0,055	0,056	$\varphi_{c=}$	3,049
-0,125	-0,055	0,38	1,944	$\varphi_{d=}$	6,715

За законом Ома визначимо струми:

$$I_1 = (\varphi_c - \varphi_a - E_1) \cdot q_1;$$
$$I_1 = (3.033 - 20) \cdot 10^{-1} = \underline{-1.697A}$$
$$I_2 = (\varphi_c - \varphi_d + E_1) \cdot q_2;$$
$$I_2 = (3.033 - 6.711 + 35) \cdot 18^{-1} = \underline{1.740A}$$
$$I_3 = (\varphi_d - \varphi_a) \cdot q_3;$$
$$I_3 = (6.711 - 0) \cdot 5^{-1} = \underline{1.342A}$$
$$I_4 = (\varphi_b - \varphi_a) \cdot q_4;$$
$$I_4 = 3.514 \cdot 10^{-1} = \underline{0.351A}$$
$$I_5 = (\varphi_b - \varphi_d) \cdot q_5;$$
$$I_5 = (3.514 - 6.711) \cdot 8^{-1} = \underline{-0.399A}$$
$$I_6 = (\varphi_b - \varphi_c) \cdot q_6;$$
$$I_6 = (3.514 - 3.033) \cdot 10^{-1} = \underline{0.048A}$$

3.5 Розрахунок струмів в гілках, методом еквівалентного генератора

Необхідно розрахувати струм в середній гілки dc в схемі рис. 3.5.

Для розрахунку напруги холостого ходу $U_{xx} = U_{dc}$ використовується схема, наведена на рисунку 3.6.

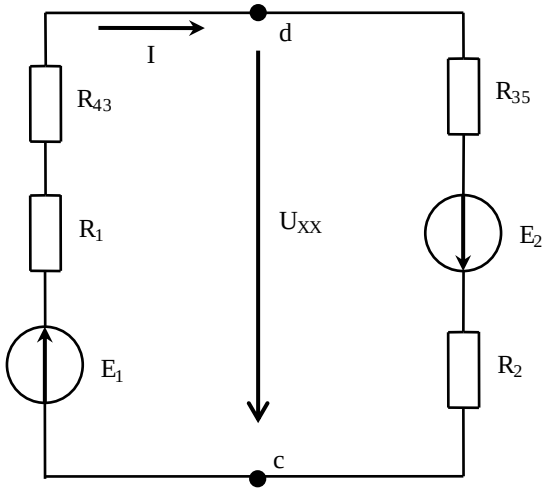

Рисунок 3.6 – Розрахунок напруги холостого ходу

За законом Ома обчислюємо струм:

$$I = \frac{E_1 + E_2}{R_1 + R_{43} + R_{35} + R_2},$$

$$I = \frac{20 + 35}{10 + 2.174 + 1.739 + 18} = 1.723A$$

Напруга холостого ходу визначається для правої або лівої частини зовнішнього контуру.

Для правої частини зовнішнього контуру розрахуємо напруги та відповідний опір:

$$U_{XX} = E_2 - I \cdot (R_2 + R_{35});$$

$$U_{XX} = 35 - 1.723 \cdot (18 + 1.735) = 0.989B$$

$$R_K = \frac{(R_1 + R_{43}) \cdot (R_{35} + R_2)}{R_1 + R_{43} + R_{35} + R_2};$$

$$R_K = \frac{(10 + 2.174) \cdot (1.739 + 18)}{10 + 2.174 + 1.739 + 18} = 7.529Ом$$

Вирішуючи проблему зниження витрати електроенергії, необхідно знати основні джерела електричних і теплових втрат електролізера, що, в свою чергу, вимагає знання балансу напруги на електролізері і теплового балансу.

Еквівалентна схема для розрахунку струму представлена на рис. 3.7:

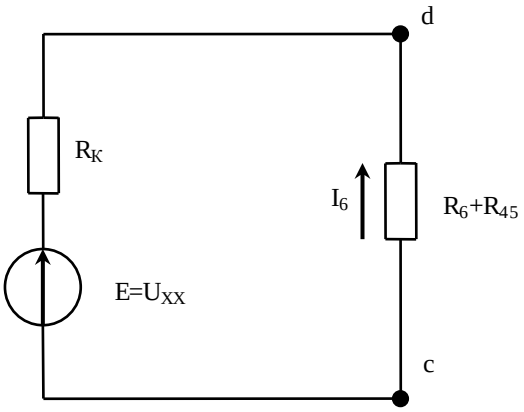

Рисунок 3.7 – Еквівалентна схема для розрахунку струму

Величина впливу провідника на струм залежить від декількох факторів: будь то теплова, хімічна або магнітна дія струму . Тобто, регулюючи силу струму, можна управляти його впливом. Електричний струм, в свою чергу – це впорядкований рух частинок під дією електричного поля.

За законом Ома

$$I_6 = \frac{U_{XX}}{R_K + R_6 + R_{45}};$$

$$I_6 = \frac{0.989}{7.529 + 10 + 3.478} = 0.047A$$

3.6 Баланс потужностей

Напруга на електролізері визначає витрату електроенергії при електролізі. Аналіз складових балансу дозволяє оцінити можливості його зниження шляхом впливу на окремі складові.

$$\sum_{k=1}^{n} E_k \cdot I_k = \sum_{k=1}^{n} I_k^2 \cdot R_k \ ,$$

де $E_k \cdot I_k$ - потужність джерела,

$I_k^2 \cdot R_k$ - потужність споживачів.

Складаємо тотожнє перетворення:

$$E_1 I_1 + E_2 I_2 = I_1^2 R_1 + I_2^2 R_2 + I_3^2 R_3 + I_4^2 R_4 + I_5^2 R_5 + I_6^2 R_6;$$

$$20 \cdot 1.695 + 35 \cdot 1.741 = 1.695^2 \cdot 10 + 1.741^2 \cdot 18 + 1.342^2 \cdot 5 + 0.352^2 \cdot 10 + 0.399^2 \cdot 8 + 0.047^2 \cdot 10;$$

$$94.835 = 28.730 + 54.559 + 9.005 + 1.239 + 1.274 + 0.022;$$

$$94.835 \cong 94.829$$

Дивлячись на можливість похибки тотожність доведена.

3.7 Визначення потенціалів

Домовимося вважати позитивним напрямком зліва направо. Тоді напруга на ділянці дорівнює різниці потенціалів. Для зовнішнього контуру розглянутої вихідної схеми (див. рис. 4), потенціали визначаються зі співвідношень:

$$\varphi_a = 0;$$
$$\varphi_d = \varphi_a - I_3 R_3,$$

т. я. струм спрямований від точки з більш високим потенціалом до точки з менш високим потенціалом;

$$\varphi_e = \varphi_d + E_2,$$

т. я. оскільки ЕРС спрямована від точки з менш високим потенціалом до точки з більш високим потенціалом;

$$\varphi_c = \varphi_e - I_2 R_2;$$
$$\varphi_f = \varphi_c + E_1;$$
$$\varphi_a = \varphi_f - I_1 R_1.$$

Підставимо числові значення для перевірки потенціалів:

$$\varphi_d = 0 - 1.342 \cdot 5 = -6.710B;$$
$$\varphi_e = -6.710 + 35 = 28.290B;$$
$$\varphi_c = 28.290 - 1.741 \cdot 18 = -3.048B;$$
$$\varphi_f = -3.048 + 20 = 16.952B;$$
$$\varphi_a = 16.952 - 1.695 \cdot 10 = 0B.$$

3.8 Типові вразливості об’єкту та атаки на нього

Використання старих протоколів для комунікації, які не передбачають захисних механізмів, також негативно впливає на загальний рівень захищеності. До

того ж контур є об’єктом, фізичний доступ до якого зловмисник може отримати досить легко, що може призвести до певних маніпуляцій, компрометуючих важливу інформацію.

У роботі наводять наступні категорії атак, що стосуються двофакторного контуру та елементів, з якими він взаємодіє:

- атака з фізичною присутністю – означає атаку, під час якої зловмисник може скористатися тим, що контур не був замкнений, та реалізувати неправомірні дії на свою користь;
- атака відкликання – атака, яка передбачає те, що зловмисник представляється особою, яка раніше мала ключ до одного з контурів, для отримання несанкціонованого доступу до об’єкту;
- атака крадіжки – атака, коли зловмисник обирає роль грабіжника та отримує фізичний доступ до ключа, який належить авторизованому користувачеві;
- атака ретрансляції – атака, що передбачає співпрацю двох зловмисників, які передають певні дані для втручання у контроль контуру.

Також можна охарактеризувати атаки за наступними двома показниками: відкриття контуру через отримання привілеїв, відкриття замку без привілеїв. Отримання привілеїв може відбуватися через атаку на пристрій користувача (використання зворотної розробки на додатку для отримання повноважень та використання мобільного зловмисного програмного забезпечення для доступу до додатку) та атаку на сервер автентифікації (отримання доступу до веб адміністрування, за допомогою якого можна додати нового користувача, та аналіз трафіку під час автентифікації для його повтору). Атаки без отримання привілеїв:

- (D)DoS атака на сервер автентифікації або сам контур, результатом якої очікується хибно позитивне спрацювання (відкриття) замку;
- атака «людина посередині» на процес комунікації контуру з сервером;
- відкриття замку через хибне представлення зловмисного ПЗ у якості серверу автентифікації;
- відкриття замку через хибне представлення зловмисного ПЗ у якості самого замку для отримання повноважень.

Також присутні атаки, пов’язані з вразливістю протоколу Bluetooth (наприклад, ненавмисне відкриття, атака relay та атака replay).

3.9 Архітектура об’єкту, алгоритм дій

Для певного розуміння процесу впровадження двофакторного контуру,

Рисунок 3.8 – Загальний алгоритм розумного замка

Додаток, встановлений у смартфоні користувача, комунікує за допомогою Bluetooth із замком для того, щоб повідомити, чи знаходиться користувач поруч. І замок, і додаток мають відокремлені канали зв’язку, які надійно та безпечно передають інформацію до програмного забезпечення через хмарний сервіс. API приймає різні запити і надсилає команди назад до розумного замка та/або відповідь у додаток користувача.

3.10 Модель загроз від MTMT

Вимоги до забезпечення захисту інформації в автоматизованих системах управління виробничими і технологічними процесами на критично важливих

об'єктах, потенційно небезпечних об'єктах, а також об'єктах, що становлять підвищену небезпеку для життя і здоров'я людей і для навколишнього природного середовища. MTMT генерує загрози, базуючись на взаємодіях. У наведених нижче таблицях (табл. 3.4 – табл. 3.8) наводиться перелік отриманих загроз.

Таблиця 1.4.

Загрози взаємодії Bluetooth відповідь між хабом і додатком

Категорія	**Пояснення**
Спуфінг	- зловмисник може підмінити цільовий веб-додаток через некоректно налаштований TLS сертифікат - зловмисник може викрасти чутливу інформацію (наприклад, облікові дані користувача) - зловмисник може створити фейковий веб-сайт для проведення фішингових атак - зловмисник може підмінити хаб і отримати доступ до додатку
Фальсифікація даних	- зловмисник може отримати доступ до чутливої інформації через SQL ін’єкцію додатку - зловмисник може отримати доступ до чутливої інформації, яка зберігається у конфігураційних файлах додатку
Заперечення	- зловмисник може заперечувати виконання неправомірних дій, прибравши футпрінти атаки
Розкриття інформації	- зловмисник може отримати доступ до чутливої інформації через повідомлення про помилки - зловмисник може отримати доступ до чутливої інформації з файлів логування - зловмисник може отримати вміст слабко зашифрованого або хешованого контенту

Таблиця 3.5.

Загрози взаємодії Bluetooth відповідь між хабом і замком

Категорія	**Пояснення**
Фальсифікація даних	- зловмисник може запустити невідомий код на замку
Фальсифікація даних	- зловмисник може фальсифікувати операційну систему пристрою і запустити офлайн атаки - зловмисник може фальсифікувати замок і витягнути з нього дані про криптографічні ключі - зловмисник може експлуатувати відомі вразливості у ще непропатченому пристрої
Підвищення привілеїв	- зловмисник може експлуатувати невикористовувані сервіси або властивості хабу - зловмисник може отримати несанкціонований доступ до привілейованих властивостей замка

Таблиця 3.6.

Загрози взаємодії HTTPS відповідь між API і додатком

Категорія	**Пояснення**
Відмова в обслуговуванні	- зловмисник може виконувати дії на правах іншого кор. через нестачу контролів проти міждоменних запитів
Підвищення привілеїв	- зловмисник може обійти критичні кроки або виконати дії на правах інших користувачів (жертв) через невірну логіку валідації. В системі є патчі і будь-яка інформація про отвори в системі дасть нам додаткову опору для підвищення своїх привілеїв. Конфігураційні файли, які використовуються для процесу установки, містять багато конфіденційної інформації

Продовження табл. 3.6.

Розкриття інформації	- зловмисник може отримати вміст слабко зашифрованого або хешованого контенту - зловмисник може отримати доступ до чутливої інформації з файлів логування - зловмисник може отримати доступ до незамаскованої чутливої інформації (наприклад, номер кредитної картки) - зловмисник може отримати доступ до чутливої інформації через підслуховування трафіку - зловмисник може отримати доступ до чутливої інформації через повідомлення про помилки - зловмисник може отримати доступ до чутливої інформації з непочищеного кешу браузера
Заперечення	- зловмисник може заперечувати виконання неправомірних дій, прибравши футпрінти атаки
Спуфінг	- доступ до сесії користувача через невірний вихід та таймаут - незахищені практики кодування - зловмисник може підмінити цільовий веб-додаток через некоректно налаштований TLS сертифікат - чутлива інформація (наприклад, облікові дані користувача) - незахищені атрибути кукі - зловмисник може створити фейковий веб-сайт для проведення фішингових атак - зловмисник може підмінити API та отримати доступ до додатку
Фальсифікація даних	- зловмисник може дискредитувати цільовий веб-додаток через запуск зловмисного коду або завантаження небезпечних файлів

Продовження табл. 3.6.

	- зловмисник може викрадати повідомлення у мережі і повторювати їх для викрадення сесії користувача - зловмисник може отримати доступ до чутливої інформації через SQL ін'єкцію додатку - зловмисник може отримати доступ до чутливої інформації, яка зберігається у конфігураційних файлах додатку

Таблиця 3.7.

Загрози взаємодії Bluetooth відповідь між користувачем і додатком

Категорія	**Пояснення**
Підвищення привілеїв	- зловмисник може вломитися до пристрою користувача і отримати підвищені привілеї
Розкриття інформації	- зловмисник може отримати вміст слабко зашифрованого або хешованого контенту - зловмисник може отримати доступ до чутливої інформації з файлів логування - зловмисник може отримати доступ до чутливої інформації через підслуховування трафіку, що надходить від мобільного клієнту - зловмисник може отримати чутливу інформацію з мобільного пристрою; - зловмисник може отримати доступ до чутливої інформації через повідомлення про помилки
Заперечення	- зловмисник може заперечувати виконання неправомірних дій, прибравши футпрінти атаки. Прогрес у новітніх інформаційних технологіях робить дуже вразливим будь-яке суспільство.

Продовження табл. 3.7.

Спуфінг	- зловмисник може підмінити цільовий веб-додаток через некоректно налаштований TLS сертифікат - зловмисник може викрасти чутливу інформацію (наприклад, облікові дані користувача) - зловмисник може створити фейковий веб-сайт для проведення фішингових атак - зловмисник може підмінити користувача та отримати доступ до додатку
Фальсифікація даних	- зловмисник може вдатися до зворотної розробки щоб фальсифікувати двійкові файли - зловмисник може отримати доступ до чутливої інформації через SQL ін'єкцію додатку - зловмисник може отримати доступ до чутливої інформації, яка зберігається у конфігураційних файлах додатку

Таблиця 3.8.

Загрози взаємодії між додатком і файловою системою

Категорія	**Пояснення**
Розкриття інформації	- зловмисник може отримати вміст слабко зашифрованого або хешованого контенту - зловмисник може отримати доступ до чутливої інформації з файлів логування - зловмисник може отримати доступ до чутливої інформації через повідомлення про помилки
Заперечення	- зловмисник може заперечувати виконання неправомірних дій, прибравши футпрінти атаки

Продовження табл. 3.8.

Спуфінг	- зловмисник може підмінити цільовий веб-додаток через некоректно налаштований TLS сертифікат - зловмисник може викрасти чутливу інформацію (наприклад, облікові дані користувача) - зловмисник може створити фейковий веб-сайт для проведення фішингових атак - зловмисник може підмінити файлову систему та отримати доступ до додатку
Фальсифікація даних	- зловмисник може отримати доступ до чутливої інформації через SQL ін'єкцію додатку - зловмисник може отримати доступ до чутливої інформації, яка зберігається у конфігураційних файлах додатку

Такий вигляд має отримана модель загроз. Її аналіз та рекомендації щодо можливого вирішення загроз описані у наступних підрозділах.

3.11 Аналіз отриманої моделі загроз

Загрозам, представленим у моделі від MTMT, було присвоєно пріоритет: 56 отримали високий, відповідно 5 – середній. Враховуючи відсутність загроз низького рівня та 91% загроз високого рівня, можна зробити висновок, що захищеність розумного замка є критичною, коли мова йде про безпеку помешкання, адже за допомогою нього можна відкрити багато дверей і в прямому, і в переносному значеннях.

Серед фаз, під час яких необхідно вирішувати загрози, були фаза імплементації та фаза дизайну. До першої відноситься 51 загроза, до другої – 10. Хоч і рекомендується адресувати якомога більше загроз на початкових рівнях задля оптимізації та ефективності процесів, про більшість з них можна дізнатися саме під час такої фази як імплементація. Адресація загроз під час зазначених вище фаз

спрощує фази тестування та релізу і застерігає виробників від додаткових витрат, яких можна уникнути, якщо робити все своєчасно.

Найбільше загроз було отримано для взаємодії «HTTPS відповідь» між API та додатком, що робить користувача разом з додатком у смартфоні, яким він користується на постійній основі, найбільш вразливою частиною у системі розумного замка. Даний факт підтверджується і тим, що OTD також присвоїв загрози з кожної категорії об'єкту «додаток у смартфоні».

Детальніше щодо категорій загроз, то у MTMT 19 відноситься до спуфінгу, 15 – фальсифікації даних, 4 – заперечення, 18 – розкриття інформації, 1 – відмови в обслуговуванні, а 4 – підвищення привілеїв. У OTD розподіл виглядає наступним чином: 5 – спуфінг, 3+12 (12 стосуються взаємодій) – фальсифікація даних, 6 – заперечення, 3+12 – розкриття інформації, 3+12 – відмова в обслуговуванні і 2 – підвищення привілеїв. З цього можна визначити топ-3 категорії загроз від MTMT (у порядку спадання) – це спуфінг, розкриття інформації та фальсифікація даних, та від OTD (займають однакові позиції) – фальсифікація даних, розкриття інформації та відмова в обслуговуванні. Спільними категоріями виступають розкриття інформації та фальсифікація даних, що робить цілісність та конфіденційність найбільш вразливими властивостями системи, які потребують надійного захисту.

3.12 Рекомендації щодо забезпечення безпеки об'єкта

Нижче наведено низку рекомендацій для вирішення ризиків, пов'язаних із представленими у попередніх підрозділах загрозами, задля підвищення загального рівня захищеності системи та об'єкту «розумний замок». Необхідно:

- перевіряти сертифікати X.509, які використовуються для автентифікації з'єднань SSL, TLS та DTLS;
- проводити аудит та забезпечити логування додатків, забезпечити обмежений доступ до лог-файлів, забезпечити логування подій управління користувачами;
- не розкривати деталі безпеки у повідомленнях про помилку;

- впровадити контролі за недопустимістю перебору імені користувача;
- впевнитися, що додаток не логує чутливу користувацьку інформацію;
- використовувати лише затверджені симетричні блочні шифри і довжину ключа та затверджені асиметричні алгоритми, використовувати затверджені генератори випадкових чисел, не використовувати потокові шифри, шифрувати конфігураційні файли, які містять чутливу інформацію;
- відключити атрибут автозаповнення HTML у чутливих формах та введеннях;
- виконувати перевірку даних, що вводяться;
- впровадити безпечне функціонування можливості відновлення паролю, впровадити політику паролів та акаунтів, упевнитися, що адміністраторська панель захищена;
- забезпечити неможливість виконання невідомого коду на пристроях;
- упевнитися, що чутливий контент не кешується в браузері;
- впровадити вихід з додатку у разі неактивності;
- використовувати безпечні кукі-файли;
- перевіряти, чи безпечні перенаправлення всередині додатку;

Висновки за розділом 3

Двоконтурний вхідний ланцюг в порівнянні з одноконтурним дозволяє отримати більш широку смугу пропускання при тому ж значенні коефіцієнта шуму, що є вельми важливим для широкосмугового приймача. Багатоконтурні вхідні ланцюги використовуються для підвищення вибірковості радіочастотного тракту. Вони сприяють більш ефективному ослабленню прийому по побічних каналах: по дзеркальному (симетричному), по сусідньому і на проміжних частотах. Збільшується також і придушення сильної перешкоди, що зменшує перехресні спотворення. Однак багатоконтурні вхідні ланцюги мають менший коефіцієнт передачі. При однакових добротностях контурів двоконтурна вхідний ланцюг дає коефіцієнт передачі в два рази менший в порівнянні з одноконтурним.

Як і інші кіберфізичні об’єкти систем навіть двофакторний ланцюг є вразливим до багатьох атак, націлених на зміну схеми його роботи та отримання доступу окремо до нього та до продукту інформаційної діяльності в цілому через експлуатацію слабких місць. Створена модель загроз для узагальненої архітектури замка показує, що для будь-якого контуру ризики існують. Звісно, окремі моделі замків, які зараз присутні на ринку, мають ті чи інші впроваджені функції безпеки, але загальна картина все одно презентує широке поле для подальшої роботи.

ВИСНОВКИ

Під час виконання даної дипломної роботи було проведено ознайомлення з новий підходом по створенню ефективної системи захисту об’єктів інформаційної діяльності, який базується на використанні функцій двоконтурної системи. Спосіб несе актуальний теоретичні та практичні застосування, має певну методику та алгоритми реалізації. Отримана модель загроз, яка продемонструвала наявність можливих витоків, так як двофкторний контур є лише складовою замкненої системи із девайсу та його програмного забезпечення, протоколами Bluetooth з’єднання. Метою даної роботи було навести оптимізовану модель двофакторного контура і розрахувати ймовірні механічні зв’язки двох контурів, надати матеріал по виробництву даної моделі.

Таким чином, у результаті виконання даної роботи було досягнуто початкову мету, пройдено практику для знаходження теоретичного матеріалу та виконано усі необхідні для цього завдання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Велика енциклопедія нафти і газу [Електронний ресурс]– Режим доступу до ресурсу: https://www.ngpedia.ru/id585265p1.html

2. Браіловський М.М.//Технології захисту інформації: підручник//К. – ЦП «Компрінт», 2021 С.296-297.

3. Torr P. Demystifying the threat modeling process / Peter Torr. // IEEE Security & Privacy. – 2005. – №5. – С. 66–70.

4. The STRIDE per Element Chart [Електронний ресурс] // Microsoft Security Development. – 2007. – Режим доступу до ресурсу: https://www.microsoft.com/security/blog/2007/10/29/the-stride-per-element-chart/.

5. Schneier B. Attack Trees / Bruce Schneier. // Dr. Dobb's Journal of Software Tools. – 1999. – №24. – С. 21–29.

6. Common Attack Pattern Enumeration and Classification [Електронний ресурс] // MITRE – Режим доступу до ресурсу: https://capec.mitre.org/index.html.

7. Common Weakness Enumeration [Електронний ресурс] // MITRE – Режим доступу до ресурсу: https://cwe.mitre.org/about/index.html.

8. Shevchenko N. THREAT MODELING: A SUMMARY OF AVAILABLE METHODS [Електронний ресурс] / Nataliya Shevchenko // Carnegie Mellon University, Software Engineering Institute. – 2018. – Режим доступу до ресурсу: https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html.

9. Lautenbach A. HEAVENS [Електронний ресурс] / A. Lautenbach, M. Islam. – 2016. – Режим доступу до ресурсу: https://autosec.se/wp-content/uploads/2018/03/HEAVENS_D2_v2.0.pdf.

10. SURFACE VEHICLE RECOMMENDED PRACTICE (J3061) [Електронний ресурс] // SAE International. – 2016. – Режим доступу до ресурсу: https://www.sae.org/standards/content/j3061/.

11. Tan L. Future Internet: The Internet of Things / L. Tan, N. Wang. // 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE). – 2010. – С. 376–380.

12. Haller S. The Internet of Things in an Enterprise Context / S. Haller, S. Karnouskos, C. Schroth. // Future Internet - FIS 2008. – 2008. – С. 14–28.

13. Mattern F. From the Internet of Computers to the Internet of Things / F. Mattern, C. Floerkemeier. // Springer. – 2010. – С. 242–259.

14. Evans D. The internet of things: How the next evolution of the internet is changing everything / Dave Evans. // CISCO White Paper. – 2011.

15. Role of smart grid in renewable energy: An overview / [M. Hossain, N. Madlool, N. Rahim та ін.]. // Renewable and Sustainable Energy Reviews. – 2016. – №60. – С. 1168–1184.

16. A Review on latest Internet of Things based Healthcare Applications / V.Philip, V. Suman, V. Menon, D. A. // International Journal of Computer Science and Information Security (IJCSIS). – 2017. – №15. – С. 248–254.

17. Senate Bill No. 327 [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

18. Smart Home Communication Technologies and Applications: Wireless Protocol Assessment for Home Area Network Resources / [T. Mendes, R. Godina, E. Rodrigues та ін.]. // Energies. – 2015. – №8. – С. 7279–7311.

19. Bugeja J. On Privacy and Security Challenges in Smart Connected Homes / J. Bugeja, A. Jacobsson, P. Davidsson. // 2016 European Intelligence and Security Informatics Conference. – 2016. – С. 172–175.

20. Sokullu R. Gts attack: An ieee 802.15. 4 mac layer attack in wireless sensor networks / R. Sokullu, I. Korkmaz, O. Dagdeviren. // International Journal On Advances in Internet Technology. – 2009. – №2. – С. 104–114.

21. Chugh K. Case study of a black hole attack on 6lowpan-rpl / K. Chugh, A. Lasebae, J. Loo. // SECURWARE 2012, The Sixth International Conference on Emerging Security Information, Systems and Technologies. – 2012. – С. 157–162.

22. Sivaraman V. Network-level security and privacy control for smart-home IoT devices / V. Sivaraman. // Wireless and Mobile Computing, Networking and Communications. – 2015. – С. 163–167.

23. Altolini D. Low power link layer security for IoT: Implementation and performance analysis / D. Altolini. // Wireless Communications and Mobile Computing Conference,. – 2013. – С. 919–925.

24. Mantas G. Security in smart home environment / G. Mantas. // Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications. – 2010. – С. 170–191.

25. P. Hoang N. A TOR-based anonymous communication approach to secure smart home appliances / N. P. Hoang, D. Pishva. // Advanced Communication Technology. – 2015. – С. 517–525.