ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо забезпечення безпеки інформаційного середовища Smart City»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Данило КРИВЕЦЬ
(підпис)

Виконав: здобувач вищої освіти групи БСД-43
КРИВЕЦЬ Данило
(прізвище, ім'я)

Керівник д.ф. МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 49 сторінок, 11 рисунки, 28 джерел.

Об'єкт дослідження – інформаційне середовище розумного міста

Предмет дослідження – методи та засоби підвищення рівню захисту інформаційного середовища розумного міста

Методи дослідження – опрацювання технічної літератури та наукових джерел для з'ясування основних принципів сучасних методів захисту інформаційного середовища розумного міста; порівняльний аналіз рішень для захисту інформаційного середовища розумного міста; визначення ключових аспектів захисту; теоретичний розгляд нових методів захисту у контексті інформаційного середовища розумного міста.

Дослідження шляхів та розробка рекомендацій щодо забезпечення безпеки інформаційного середовища Smart City є важливим завданням у контексті сучасної цифровізації міської інфраструктури. Інформаційне середовище розумного міста включає різноманітні технології та системи, що взаємодіють для покращення якості життя мешканців, ефективного управління ресурсами та забезпечення сталого розвитку. Разом із цим зростає необхідність у підвищенні рівня захисту цих систем від кіберзагроз.

У дослідженні приділено особливу увагу сучасним методам захисту, які можуть бути застосовані для підвищення рівня безпеки у розумному місті. Аналізовано технічну літературу та наукові джерела, проведено порівняльний аналіз різних рішень для захисту інформаційного середовища розумного міста. Визначено ключові аспекти захисту та теоретично розглянуто нові методи захисту у цьому контексті.

В результаті дослідження розроблено рекомендації щодо підвищення рівня захисту інформаційного середовища розумного міста. Практичне застосування результатів роботи може знайти використання у різних міських інфраструктурних проєктах, де критично важливим є забезпечення надійності і безпеки інформаційних систем.

Галузь використання – кібербезпека інформаційних ресурсів організації.

КІБЕРБЕЗПЕКА, SMART CITY, IoT, Zero Trust, БЕЗПЕКА КОМУНІКАЦІЙНИХ МЕРЕЖ, МОНІТОРИНГ БЕЗПЕКИ, SIEM.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ	—	програмне забезпечення;
ПК	—	персональний комп’ютер;
ІТ	—	інформаційні технології
ОТ	—	оперативні технології
IEEM	—	промислова інженерія та управління інженерією
P2P	—	однорангова мережа
LAN	—	локальна обчислювальна мережа
WLAN	—	бездротова локальна мережа

ВСТУП

Актуальність дослідження. Забезпечення безпеки інформаційного середовища Smart City є критично важливим у сучасних умовах зростання кіберзагроз та підвищеної цифровізації міської інфраструктури. Smart City системи покладаються на різноманітні технології, що взаємодіють для покращення якості життя мешканців, ефективного управління ресурсами та забезпечення сталого розвитку. Дослідження шляхів забезпечення безпеки та розробка рекомендацій дозволяє своєчасно виявляти потенційні загрози, мінімізувати ризики кіберінцидентів та забезпечити стабільну і безпечну роботу міської інфраструктури, підвищуючи загальний рівень безпеки та комфорту мешканців.

У сучасному розумному місті важливу роль відіграють IoT мережі, які забезпечують взаємодію між різноманітними пристроями та системами. Забезпечення безпеки IoT мереж є одним із головних завдань, оскільки вони часто стають мішенню для кіберзлочинців через численні вразливості. Застосування адаптивних підходів до безпеки дозволяє реагувати на змінювані загрози в реальному часі, забезпечуючи гнучкість і ефективність захисних заходів.

Проте, попри наявність сучасних інструментів та методик, питання інтеграції адаптивних підходів у процеси забезпечення безпеки інформаційного середовища розумного міста залишається недостатньо дослідженим. Це створює прогалини у захисних алгоритмах, особливо в умовах швидкого розвитку технологій та зростання кількості кіберзагроз. У цьому контексті, дослідження, спрямоване на аналіз та розробку рекомендацій щодо ефективного використання адаптивних підходів для підвищення безпеки інформаційного середовища розумного міста, стає актуальним.

Робота над цією темою дозволить не тільки систематизувати наявні знання та найкращі практики по плануванню та побудови інформаційного середовища розумного міста а й допоможе подальшим фахівцям кібербезпеки розвивати та досліджувати цю тему глибше.

Об'єкт дослідження – інформаційне середовище розумного міста.

Предмет дослідження – методи та засоби підвищення рівню захисту інформаційного середовища розумного міста.

Мета роботи – розробити рекомендації щодо застосування новітніх практик та покращення існуючих механізмів захисту інформаційного середовища розумного міста.

Наукові завдання:

визначити ключові аспекти для захисту в інформаційному середовищі розумного міста.

проаналізувати існуючи методології та рекомендації для захисту в інформаційному середовищі розумного міста.

проаналізувати існуючи рішення підвищення рівня захищеності мережевих систем.

визначити вимоги до рішень які можуть використовуватись для захисту в інформаційному середовищі розумного міста.

розробити рекомендації щодо підвищення рівня безпеки інформаційного середовища розумного міста.

Методи дослідження – опрацювання тематичної літератури, інтернет-джерел, аналіз наукових досліджень, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: розроблено рекомендації щодо планування та створення первинних процесів у питанні захисту інформаційного середовища розумного міста. Методи реалізації сучасних стандартів та практик по підвищенню захисту інформаційного середовища

1 АНАЛІЗ СУЧАСНИХ ВИКЛИКІВ ТА ПРОБЛЕМ В ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ В SMART CITY

1.1 Поняття smart City та значення його інформаційних ресурсів

У процесі свого розвитку кожне місто прагне отримати статус "розумного". Місто можна вважати розумним, якщо воно ефективно використовує інформаційно-комунікаційні технології (ІКТ) для оптимізації різних аспектів міського життя, підвищуючи ефективність, стійкість і якість життя своїх мешканців. В основі розумного міста лежить безперешкодна інтеграція технологій в його інфраструктуру, управління, послуги та взаємодію, що призводить до створення більш взаємопов'язаного і керованого даними міського середовища.

Однією з основних вимог для того, щоб місто вважалося "розумним", є розгортання передових технологій IoT (Інтернет речей) у всій його фізичній інфраструктурі. IoT передбачає взаємозв'язок різних пристроїв, датчиків і систем, вбудованих в міську структуру, що дозволяє збирати, передавати і аналізувати дані в режимі реального часу. Ці пристрої IoT слугують сенсорною мережею розумного міста, збираючи різноманітні потоки даних, пов'язані з транспортними потоками, енергоспоживанням, якістю повітря, утилізацією відходів, громадською безпекою, тощо.

У по-справжньому розумному місті пристрої Інтернету речей безперешкодно інтегровані в повсякденні об'єкти та інфраструктуру, такі як вуличні ліхтарі, світлофори, сміттєві баки, громадський транспорт, будівлі та комунальні служби. Ці взаємопов'язані пристрої збирають величезні обсяги даних, формуючи основу для прийняття обґрунтованих рішень та ефективного розподілу ресурсів.

Наприклад, розумні датчики, встановлені на світлофорах, можуть відстежувати схеми руху в режимі реального часу, динамічно регулюючи час увімкнення сигналів, щоб зменшити затори та оптимізувати транспортний потік.

Розглянемо основні компоненти розумного міста (рис. 1.1)

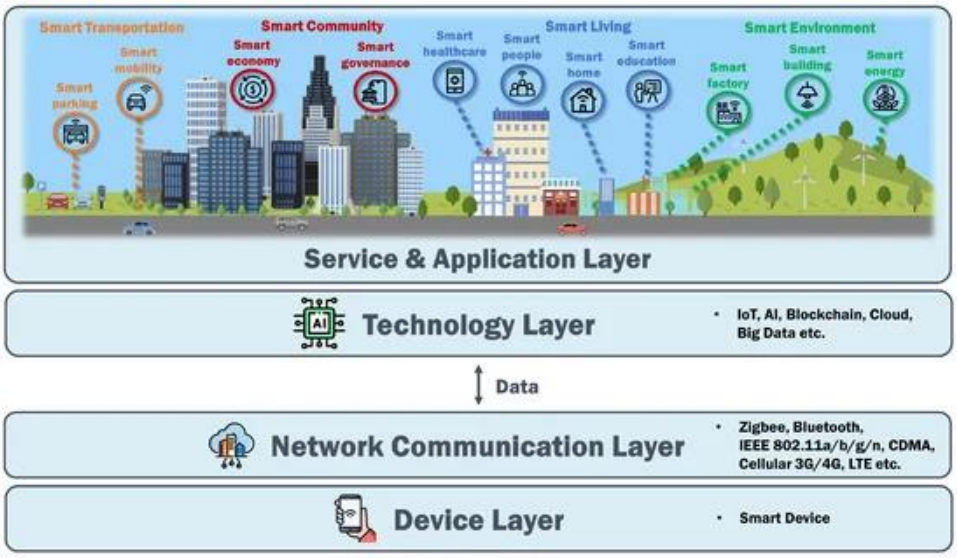

Рис.1.1. Основні рівні розумного міста

Розумні міста можна розділити на чотири шари. У верхньому шарі відбувається надання послуг і додатків для мешканців, які живуть у розумних містах. Нижче розташовані рівні технологій, мережевого зв'язку та пристроїв.

Рівень послуг та додатків

Сервіси та додатки "розумного міста" покликані підвищити якість життя мешканців "розумних" міст. Розумні транспортні системи пропонують широкий спектр послуг - від спрямування користувачів до кращих маршрутів або інформування про умови руху до можливостей спільного користування автомобілями та велосипедами, що робить системи громадського транспорту та мобільність громадян більш ефективними та зручними. Крім того, "розумні" послуги можуть також задовольняти потреби громадян у паркуванні, наприклад, визначати наявність вільних місць для паркування [1].

З точки зору уряду, ІКТ можуть бути використані для сприяння прозорості та участі громади, а також для ефективного управління натовпом і вирішення проблем надзвичайних ситуацій на основі публічних даних [2]. Розумна економіка підвищує гнучкість ринку праці, а також регіональну продуктивність і конкурентоспроможність. Послуги "розумного життя" дозволяють громадянам у розумних містах обмінюватися інформацією в режимі реального часу, тим самим

даючи їм змогу ефективно вирішувати повсякденні проблеми та залишатися на зв'язку [2]. Дистанційний моніторинг здоров'я та послуги електронної охорони здоров'я надають громадянам персоналізовану медичну допомогу [3]. Системи "розумного будинку" дозволяють користувачам дистанційно керувати домашніми приладами Інтернету речей, такими як "розумні телевізори", використовуючи додатки для смартфонів для виконання конкретних завдань [4].

Крім того, міські об'єкти можна використовувати зручніше, а системи освіти можна вдосконалити, щоб забезпечити гнучкі можливості для навчання мешканців. Однією з ключових цілей "розумних" міст є сприяння екологічній стійкості за допомогою цифрових інтегрованих і вдосконалених систем енерго-менеджменту. Смарт-сервіси можуть здійснювати моніторинг та управління в режимі реального часу "розумними" будівлями, "розумними" заводами та "розумними" енергетичними системами, що може підвищити енергоефективність та управління відходами [2].

Рівень технологій

Інноваційні та популярні технології відіграють вирішальну роль у більш ефективному та безпечному вирішенні різних проблем із розумними містами шляхом використання величезних обсягів даних, які генеруються. IoT є фундаментальною технологією, яка з’єднує різні ІКТ-пристрої та закладає основу для передових розумних міст [5]. Було проведено дослідження щодо застосування технологій IoT до різних програм розумного міста, включаючи проблеми забруднення [6,7,8]. Хмарна інфраструктура та платформи також мають вирішальне значення для розумних міст, а розділення даних є серйозною проблемою [9,10].

Дані можна збирати в режимі реального часу за допомогою датчиків у пристроях Інтернету речей, таких як RFID, інфрачервоне випромінювання (ІЧ), системи глобального позиціонування (GPS) і лазерні сканери, і зберігати в хмарі або периферійному сховищі даних. Програми IoT дозволяють дистанційно контролювати та керувати пристроями [5,11]. Технологія штучного інтелекту швидко розвивається, щоб забезпечити швидке та ефективне надання комплексних

послуг для невеликих елементів розумного міста, таких як розумні будинки та розумні будівлі, а також великомасштабні елементи, такі як розумна інфраструктура та розумний транспорт [12].

Технологія "Big data" є ключовим чинником для навчання та використання штучного інтелекту, оскільки вона може збирати й аналізувати величезну кількість даних, створених у розумних містах, таким чином дозволяючи штучному інтелекту прогнозувати або робити висновки про майбутні результати та приймати кращі рішення. Крім того, технології блокчейну та глибокого навчання можуть використовуватися для надання розумніших послуг автоматизації для розумних міст, оскільки дані можна вивчати та визначати автономно [13]. Технологія автентифікації також досліджується для розумних міст з точки зору блокчейну [14].

Рівень мережевих комунікацій

Мережевий зв'язок є ключовим елементом у розумних містах. Додатки, які потребують зв'язку на короткі відстані, такі як "розумні" електромережі, "розумне" водопостачання та "розумні" будівлі з дуже обмеженим споживанням енергії, зазвичай використовують стандарт IEEE 802.15.4 (Zigbee). Ці програми можуть роками працювати від одного акумулятора. Для цих додатків також можна використовувати IEEE 802.15.1 (Bluetooth). Протокол бездротової локальної мережі (WLAN) використовує діапазон 2,4 ГГц зі швидкістю передачі даних 1 Мбіт/с і дуплексом з часовим поділом (TDD) між ведучим і веденим в діапазоні від 10 до 100 м.

Протоколи IEEE 802.11a/b/g/n використовуються майже у всіх системах розумного міста. Остання версія, протокол IEEE 802.11n, працює в діапазонах 2,4 і 5,1 ГГц і використовує ортогональне частотне мультиплексування (OFDM) і пряме розширення спектра (DSSS). Цей протокол також дозволяє здійснювати операції на основі резервування з використанням функцій координації точок (PCF) і операції з використанням розподілених функцій координації (DCF). Послуги PCF корисні для

трафіку відео, реального часу і мультимедійних аудіоданих, які вимагають гарантій QoS для певних параметрів, таких як пропускна здатність.

Рівень пристроїв та датчиків

Рівень пристроїв і датчиків є важливим компонентом розумних міст. Розумні пристрої, оснащені датчиками та приводами, можуть вимірювати, збирати та контролювати різні типи даних [15]. Дані з різних розумних міст, включаючи інформацію про пересування громадян, паркування та дані про будівлі або місто (такі як світло, шум, температура та вологість), можна збирати за допомогою датчиків Інтернету речей і обробляти, об’єднуючи їх з ІКТ [15].Громадяни можуть візуально отримувати та контролювати дані за допомогою фізичних пристроїв, таких як портативні пристрої та смартфони. Об’єкти, обладнані датчиками IoT, можуть контролювати дані в режимі реального часу, аналізувати та контролювати ці дані відповідно до власних конкретних цілей.

Світові приклади застосування

Технології "розумного міста" пропонують безліч варіантів, але їхній потенціал залишається значною мірою невикористаним. Тим не менш, вкрай важливо вивчати приклади успішного впровадження, щоб пролити світло на їхній вплив на міське життя та інфраструктуру. Одним з таких прикладів є впровадження розумної системи вуличного освітлення в Барселоні.

У 2010 році Барселона почала впроваджувати "розумні" технології у свою міську інфраструктуру, розпочавши з реалізації складної системи вуличного освітлення. Ця система використовує сегментовані світильники, оснащені регульованими компонентами (рис. 1.2) [16]

Рис.1.2. Розумний ліхтар

Завдяки використанню датчиків освітленості по всьому місту, система сприяла динамічному регулюванню яскравості та напрямку світла.

З цього місто отримало наступні переваги. По-перше, динамічний характер системи освітлення означає відхід від традиційних статичних установок, пропонуючи адаптивність до мінливих умов навколишнього середовища та міської динаміки. По-друге, значне скорочення споживання електроенергії підкреслює екологічну стійкість системи, що відповідає більш широким цілям енергозбереження та зменшення вуглецевого сліду. Крім того, підвищення ефективності вуличного освітлення підвищує рівень громадської безпеки, сприяючи створенню більш безпечного міського середовища для громадян.

Другим прикладом, але в цей раз більш комплексної імплементації, можна вважати приклад Сінгапуру та імплементацію системи регуляції трафіку в місті (рис. 1.3).

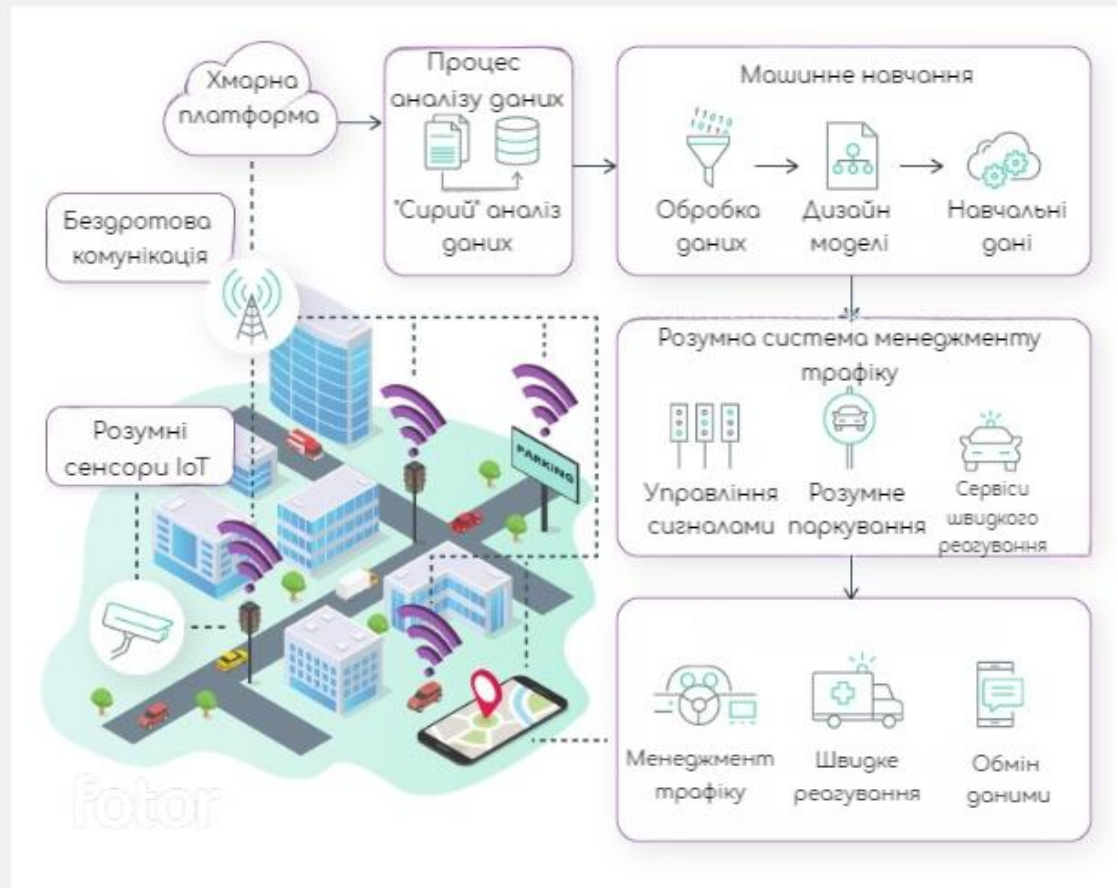

Рис1.3. Модель розумного менеджменту трафіку

Існують декілька варіантів розгортання подібних систем, приклад Сінгапуру складається з трьох основних елементів а саме:

Розумні датчики руху [17]

Датчики Інтернету речей забезпечують основу даних, які інтелектуальні системи управління транспортом аналізують, щоб підвищити ефективність дій. Інтелектуальні системи управління дорожнім рухом використовують такі інтегровані датчики, як:

- Мітки радіочастотної ідентифікації (RFID);
- Мітки автоматичної ідентифікації та збору даних (AIDC);
- Датчики температури;
- Датчики якості повітря.

Підключений відеомоніторинг

Одним з основних технологічних аспектів інтелектуальних систем управління дорожнім рухом є системи відеодетекції з інтегрованою периферійною

обробкою. Рішення для підключеного відеомоніторингу в сфері безпеки дорожнього руху називаються системами управління дорожніми інцидентами (ТІМ). ТІМ дозволяє міським планувальникам отримувати інформацію в режимі реального часу про умови дорожнього руху і реагувати на інциденти за допомогою відеозаписів у форматі HD, виявлення і розпізнавання зображень [17].

Підключені системи світлофорів

На відміну від звичайних світлофорів, інтелектуальні системи світлофорів інтегрують вищезгадані датчики і підключені технології відеомоніторингу для обліку часу очікування на перехресті, швидкості транспортних засобів і/або пішохідного трафіку. Інтелектуальні світлофорні системи включають процеси штучного інтелекту (ШІ) і машинного навчання (МН), що дозволяють використовувати “машинний зір” - оптичне розпізнавання символів (OCR) і навчання з підкріпленням [17].

Враховуючи географічні та демографічні особливості Сінгапуру, рішення про впровадження автоматизованої системи управління дорожнім рухом було неминучим. В результаті її впровадження місто отримало низку значних покращень, зокрема покращилося реагування на надзвичайні ситуації, зменшилися затори на дорогах та мінімізувалися шкідливі викиди в атмосферу [17].

Український досвіт інтеграції технологій розумного міста

Спираючись на світовий досвід, Україна почала впроваджувати ініціативи "розумного міста" у 2015 році. Наразі низка систем "розумного міста" функціонує в кількох українських містах, зокрема в Києві, Івано-Франківську, Львові, Мукачевому, Дрогобичі, Запоріжжі, Полтаві, Тернополі та Харкові, а також у Маріуполі, де впроваджувалась система "Безпечне місто". Варто зазначити, що позиція Києва на 82-му місці в глобальному Індексі розумних міст станом на 2021 рік є кількісним орієнтиром для оцінки прогресу країни в цій сфері.

Незважаючи на таке широке впровадження, українські муніципалітети часто демонструють вибіркове включення елементів "розумного міста", що свідчить про нюанси в підходах до цифровізації міст. Однак, незважаючи на ці різноманітні впровадження, Україна демонструє помітний прогрес у цифровізації та

автоматизації процесів, що свідчить про ширшу тенденцію до технологічної інтеграції в міському ландшафті.

Прикладом може слугувати додаток "Дія", який демонструє успіхи України у сфері надання цифрових послуг. Завдяки цій платформі багато державних послуг, які раніше надавалися офлайн, перейшли на онлайн-платформи, що підвищило їхню доступність та ефективність. Крім того, "Дія" сприяє залученню громадян до процесів управління, сприяючи демократії участі завдяки таким функціям, як голосування за зміни в політиці та ініціювання петицій.

Також вартий уваги, мобільний додаток “Київ Цифровий”, розроблений для оптимізації послуг громадського транспорту. Окрім своєї функціональної корисності, Київ Цифровий” відображає стратегічну відповідь на виклики міської мобільності, надаючи в режимі реального часу оновлення про стан транспорту та забезпечуючи можливість онлайн-продажу квитків. Зокрема, адаптація додатку до умов воєнного часу підкреслює його динамічний характер, а оновлення включають функції для попередження користувачів про потенційні загрози, такі як ракетні удари.

1.2 Ідентифікація потенційних загроз для інформаційного середовища smart city

Розумні міста через особливості у своїй структурі можуть та будуть стикатись з низькою ризиків. Однак нові переваги супроводжуються новими вразливостями, які створюють ризики для національної та економічної безпеки, громадського здоров'я, безпеки та функціональності критично важливих інфраструктур. Глобальне зростання кіберзагроз, спрямованих на системи операційних технологій (ОТ), у поєднанні з їх інтеграцією в системи "розумного міста", розширює сферу атак і збільшує потенційні збитки від порушень. Зловмисники використовують ці системи для крадіжки даних, атак з вимогами викупу та інших кібервторгнень, що потенційно може порушити роботу міських служб, спричинити фінансові збитки, скомпрометувати дані громадян, підірвати

довіру громадськості до цих технологій та завдати фізичної шкоди інфраструктурі, можливо, навіть поставити під загрозу життя людей. Громадам, які впроваджують "розумні" технології, вкрай важливо враховувати ці ризики у своїх комплексних стратегіях управління ризиками.

Розширена та взаємопов'язана поверхня атаки

Інтеграція більшої кількості раніше розрізнених інфраструктурних систем в єдине мережеве середовище розширює площу цифрових атак для кожної взаємопов'язаної організації.

Ця розширена поверхня атаки збільшує можливості для зловмисників використовувати вразливість для початкового доступу, переміщатися між мережами і спричиняти каскадні, міжгалузеві порушення роботи інфраструктури або іншим чином загрожувати конфіденційності, цілісності та доступності даних, систем і мереж організації. Наприклад, зловмисники, які отримують доступ до мережі датчиків Інтернету речей місцевих органів влади, можуть отримати доступ до систем оповіщення про надзвичайні ситуації, якщо ці системи взаємопов'язані.

Крім того, в результаті інтеграції більшої кількості систем і посилення зв'язку між підмережами, мережеві адміністратори і співробітники служби безпеки можуть втратити видимість колективних системних ризиків. Ця потенційна втрата видимості включає компоненти, що належать і експлуатуються постачальниками, які надають свою інфраструктуру як послугу для підтримки інтеграції.

Вкрай важливо, щоб власники систем були в курсі та контролювали топологію мережі, що розвивається, а також осіб/постачальників, відповідальних за систему в цілому та кожен сегмент. Невизначеність щодо ролей та обов'язків може погіршити стан кібербезпеки системи та можливості реагування на інциденти. Громади, які впроваджують технологію "розумного міста", повинні оцінювати та управляти цими ризиками, пов'язаними зі складною взаємодією [18].

Ризики з боку ланцюга постачання ІКТ та постачальників

Громади, які розбудовують інтелектуальні інфраструктурні системи, часто покладаються на постачальників, які закуповують та інтегрують апаратне та програмне забезпечення, що пов'язує операції інфраструктури через з'єднання для

передачі даних. Вразливості в ланцюгах постачання ІКТ, або навмисно створені суб'єктами кіберзагроз для зловмисних цілей, або ненавмисно створені через неналежні практики безпеки, можуть сприяти цьому:

- крадіжці даних та інтелектуальної власності,
- втрату довіри до цілісності системи "розумного міста",
- збій системи чи мережі через порушення доступності операційної технології.

Постачальники ІКТ, що надають технології "розумного міста", повинні застосовувати цілісний підхід до безпеки, дотримуючись практики розробки безпечних за задумом і безпечних за замовчуванням програмних продуктів. Програмні продукти, розроблені відповідно до цих практик, зменшують навантаження на місцеві юрисдикції з обмеженими ресурсами і підвищують базовий рівень кібербезпеки в мережах "розумних" міст.

Ризик від одного постачальника "розумного міста" може бути набагато вищим, ніж в інших ланцюгах постачання ІКТ або інфраструктурних операціях, з огляду на зростаючу взаємозалежність між технологіями та базовими або життєво важливими послугами. Організації повинні ретельно розглядати ризики від кожного постачальника, щоб не наражати громадян, бізнес та громади на потенційно ненадійне обладнання та програмне забезпечення, а також на навмисне використання вразливостей ланцюга постачання як вектора атаки.

Це передбачає ретельну перевірку постачальників з національних держав, пов'язаних з кібератаками, або тих, які підпадають під дію національного законодавства, що вимагає від них передавати дані іноземним спецслужбам. Незаконний доступ, отриманий через вразливий ланцюжок постачання ІКТ, може призвести до деградації або порушення роботи інфраструктури, а також до компрометації або крадіжки конфіденційних даних, отриманих в результаті роботи комунальних служб, зв'язку з аварійними службами або технологій візуального спостереження.

Постачальники ІТ-послуг для "розумних" міст також можуть мати доступ до величезних обсягів конфіденційних даних з різних громад для підтримки інтеграції

інфраструктурних послуг, включаючи конфіденційну державну інформацію та інформацію, що ідентифікує особу (PII), що може стати привабливою мішенню для зловмисників. Агрегація конфіденційних даних може надати зловмисникам інформацію, яка може виявити вразливі місця в критичній інфраструктурі та поставити громадян під загрозу [18].

Автоматизація інфраструктурних операцій

Розумні міста можуть досягти ефективності за рахунок автоматизації операцій, таких як очищення стічних вод або управління дорожнім рухом. Автоматизація зменшує потребу в прямому людському контролі над цими системами. Автоматизація також може забезпечити кращу узгодженість, надійність і швидкість стандартизованих операцій. Однак автоматизація може також створювати нові вразливості, оскільки збільшує кількість віддалених точок входу в мережу (наприклад, датчиків Інтернету речей і віддалених точок доступу). Обсяг даних і складність автоматизованих операцій - в тому числі залежність від сторонніх постачальників для моніторингу та управління операціями - можуть зменшити видимість системних операцій і потенційно перешкоджати реагуванню на інциденти в режимі реального часу.

Автоматизація інфраструктурних операцій у середовищі "розумного міста" може вимагати використання датчиків і виконавчих механізмів, що збільшує кількість кінцевих точок і мережевих з'єднань, вразливих до компрометації. Інтеграція ШІ та складних цифрових систем може призвести до появи нових векторів атак і додаткових вразливих мережевих компонентів. Покладання на систему штучного інтелекту або інші складні системи може знизити загальну прозорість роботи мережевих пристроїв, оскільки ці системи приймають і виконують оперативні рішення на основі алгоритмів, а не людських суджень.

Вразливості кіберфізичних систем

Інтеграція IT- та OT-систем у розумних містах створює складний кіберфізичний ландшафт, в якому фізична інфраструктура є вразливою до кібератак. Така конвергенція вимагає підходу до безпеки, який враховує як кібер, так і фізичні загрози, щоб запобігти інцидентам, які можуть призвести до фізичної

шкоди або перебоїв у роботі критично важливих сервісів. Виклик ускладнюється різноманітністю технологій "розумного міста" і потенціалом каскадних ефектів через взаємопов'язані системи, що вимагає стратегії глибокого захисту і безперервного моніторингу як IT-, так і OT-середовищ.

Інтероперабельність застарілих систем

Інтеграція передових цифрових технологій із застарілими застарілими системами може створити нові потенційні вектори для атак, що призводить до неузгодженості політик безпеки і вразливостей. Безпека розумних міст ставиться під загрозу через відсутність універсальних стандартів для пристроїв Інтернету речей, що призводить до появи нових вразливостей з кожним пристроєм, доданим до мережі. Забезпечення сумісності при збереженні високих стандартів безпеки вимагає ретельного балансу, з акцентом на модернізацію або заміну застарілих систем, які не можуть відповідати сучасним вимогам безпеки.

1.3 Оцінка впливу внутрішніх та зовнішніх факторів на інформаційне середовище smart city

Розвиток інфраструктури та інформаційної екосистеми розумного міста є багатогранним і тривалим процесом, що характеризується складним характером і значними витратами часу. Цей процес, який часто триває роками, підкреслює складну взаємодію безлічі чинників, що формують траєкторію розвитку міста. Як правило, наукові дослідження та відповідні стандарти поділяють ці впливи на внутрішні та зовнішні.

Зсередини діють чинники притаманні самому місту та його особливостям, його місцезнаходження та тип організації. Ця внутрішня динаміка охоплює цілий спектр міркувань, включаючи існуючу інфраструктуру міста, інституційні рамки та соціально-економічні структури. Розуміння цих внутрішніх факторів є ключовим, оскільки вони лежать в основі фундаментальних елементів, на яких будуються ініціативи "розумного міста". Такі фактори, як ефективність існуючих систем, адаптивність управлінських структур і готовність населення сприймати

технологічні досягнення, сприяють формуванню траєкторії розвитку "розумного" міста.

І навпаки, зовнішні чинники походять з ширшого контексту, що охоплює регіональну, національну і навіть міжнародну сфери. Ці зовнішні впливи виходять за межі міста, охоплюючи політику, правила та соціально-економічні тенденції, що формуються на державному та міжнародному рівнях. Такі фактори можуть включати урядові директиви, спрямовані на розвиток міст, механізми фінансування інфраструктурних проектів та міжнародні стандарти впровадження "розумного міста". Крім того, значний вплив мають світові тенденції розвитку технологій, екологічної стійкості та практики міського планування, які формують стратегічний напрямок і пріоритети ініціатив "розумного міста".

Рис.1.4.Зовнішні та внутрішні чинники впливу на розвиток розумного міста

Внутрішні фактори

Вплив громадян

Цей фактор стосується участі громадян або мешканців у прийнятті рішень з питань міської політики, а не лише як бенефіціарів простих рішень з питань міської

політики, які можуть безпосередньо підтримати їхні інтереси. Громадяни або мешканці висловлюють свої побажання та шукають шляхи їх вирішення; це також пов'язано з поняттям мешканців [10]. Для сталого розвитку міст необхідне планування та впровадження планової міської політики, але різні групи, такі як громадяни та громадянське суспільство, повинні брати участь у формулюванні та впровадженні такої міської політики [11].

Таким чином, активізація участі громадян має важливе значення для зміцнення демократії та підвищення ефективності міської політики. Міське планування в епоху смарт-технологій має бути розширене і трансформоване, щоб відрізнятися від існуючого міського планування. Розвиток ІКТ призвів до змін у суспільстві та поведінці людей у різних сферах.

У процесі розвитку розумного міста стверджується, що розширення участі громадян у формі висхідних, експериментальних інновацій, платформ з відкритим вихідним кодом і живих лабораторій з'явилося як новий міський план [12]. Найбільшою перевагою розумного міста є перетворення процесу прийняття політичних рішень під керівництвом уряду на процес прийняття політичних рішень під керівництвом громадян. Громадянам необхідно активно втручатися в практику соціальної справедливості та екологічної справедливості в місті за допомогою дорадчих груп, дебатів, бюджетів громадської участі та громадянських петицій.

Адміністрація

З точки зору міської політики, лідерство місцевого урядування має великий вплив на успіх або провал політики. Статистично виявлено, що саме роль міської адміністрації може нести критичний рівень впливу на реалізацію проектів які входять в склад реформації міста в розумне.

Ймовірність підвищення рівня якості "розумного" міста залежить від специфічних для країни змінних. Серед них, як стверджується, лідерство впливає на політичний рівень "розумного" міста, політичні ризики та рівень корупції. Для того, щоб зменшити затримки у впровадженні "розумних" міст, політики, які відіграють провідну роль, повинні знайти способи зменшити залежність шляху від

впровадження технологій [14]. Важливу роль в виборі потенційного голови на виконання проекту також грає його кваліфікація та сфера діяльності.

У контексті розвитку "розумних" міст роль, яку традиційно відігравали керівники інформаційних служб, зміщується в бік залучення сторонніх фахівців, які мають безпосередній досвід у розвитку "розумних" міст або впровадженні їхніх різних компонентів. Такий підхід підкреслює необхідність використання зовнішньої експертизи в галузі ІКТ, а також навичок у стратегічному плануванні, фінансовому управлінні, розподілі ресурсів, навчанні персоналу і забезпеченні стандартизації та інтероперабельності систем. Ці елементи мають вирішальне значення для аналітичних, стратегічних та операційних потреб успішного створення інфраструктури розумного міста.

Іфраструктура

Основою концепції розумного міста є розвиток ІКТ, таких як бездротовий зв'язок, великі дані (big data) та Інтернет речей (IoT). Розвиток нових технологій дозволяє реалізувати речі, які були неможливі в містах минулого. Розумні технології, такі як цифрові пристрої та інтернет-мережі, безперервно вивчалися, і були досягнуті різні інновації та послуги, які були розроблені незалежно, а потім з'єднані один з одним .

Зокрема, такі міські концепції, як цифрове місто, що з'явилися на початку обговорення ефективного вирішення міських проблем на основі ІКТ, були майже повністю замінені концепцією розумного міста, яка спрямована на управління інтегрованими містами. Іншими словами, вирішення міських проблем за допомогою ІКТ є основним завданням у побудові "розумного" міста. Розвиток цифрових технологій впливає на різні сфери міста (зокрема, відбуваються великі зміни в міському управлінні та розвитку), і що велика кількість даних, які генеруються різними системами ІКТ, є основним фактором розумних міст.

Хоча технологічна інфраструктура є важливим фактором розумного міста, ефект технологічної інфраструктури може бути меншим, якщо не створена людська інфраструктура. Наприклад, навіть якщо побудувати електростанцію, яка виробляє електроенергію, вона стане марною без людської інфраструктури, яка зможе її

обслуговувати. Побудова людської інфраструктури важлива так само, як і технологічна інфраструктура. Ось чому нам потрібно навчати людей будувати розумне місто, щоб ефективніше використовувати новітні технології.

Зовнішні фактори

Стандарти

У сфері розвитку розумних міст встановлені стандарти відіграють ключову роль як зовнішній фактор, що суттєво впливає як на стратегічний напрямок, так і на операційну ефективність цих міських середовищ. Стандарти, за своєю природою, слугують орієнтирами якості, сумісності та безпеки в складній екосистемі "розумних" міст. Вони гарантують, що різні технологічні компоненти і системи можуть безперешкодно взаємодіяти, тим самим підвищуючи ефективність і зручність користування міськими послугами.

Крім того, стандарти кібербезпеки спрямовані на боротьбу з безліччю загроз, з якими стикаються "розумні" міста, забезпечуючи основу для надійних заходів безпеки, які захищають цілісність даних, конфіденційність користувачів і надійність системи. Це має вирішальне значення в епоху, коли міська інфраструктура стає все більш взаємопов'язаною і залежить від збору та аналізу величезних обсягів даних.

Прийняття міжнародних і національних стандартів також сприяє приведенню ініціатив розумного міста у відповідність до найкращих світових практик, що дозволяє містам залучати інвестиції, стимулювати інновації та підвищувати свою конкурентоспроможність на світовій арені. Крім того, стандарти відіграють вирішальну роль у дотриманні нормативних вимог, допомагаючи містам орієнтуватися в складних правових та етичних питаннях, притаманних використанню цифрових технологій у публічному просторі.

По суті, розробка та впровадження стандартів як зовнішній фактор не просто керує технічними аспектами проектів "розумного міста", але й формує стратегічне бачення, забезпечуючи стійкість, безпеку та відповідність цих ініціатив ширшим суспільним цілям.

Політичний напрямок

Слідуючи за течією епохи розумних міст, уряди країн світу рішуче налаштовані на розвиток "розумних" міст. 26 листопада 2013 року в Брюсселі, Бельгія, відбулося засідання Європейської Комісії, яка ініціювала запит на участь у створенні "Зобов'язань щодо розумного міста та громади". Вони також зазначили, що Європейське інноваційне партнерство (ЄІП) необхідне, і що ЄІП буде зосереджене на ефективних рішеннях проблем, з якими стикаються європейські міста, "розумні" міста і громади. Європейська Комісія також оголосила, що планує інвестувати приблизно 200 мільйонів євро в "розумні" міста і громади в бюджеті програми досліджень та інновацій "Горизонт 2020" на 2014-2015 роки. Як результат, у Нідерландах, Іспанії та Сполученому Королівстві (Великобританія) вже існують добре розвинені розумні міста.

У Китаї сподіваються, що урбанізація сприятиме зростанню внутрішнього попиту та майбутньому зростанню. З 2012 року ця країна є домом для найбільшого у світі бізнесу в галузі "розумних міст", який очолював міський департамент сільського будівництва. Станом на 2015 рік він інвестував загалом 78 мільярдів доларів. Для цього в серпні 2013 року, після того, як у січні було оголошено про 90 демонстраційних майданчиків, було додано ще 103 майданчики. Японія також прагне експортувати "розумні" технології за кордон. Очікується, що до 2020 року це дасть економічний ефект у розмірі 3,2 трильйона ієн і створить понад 60 000 робочих місць.

У Кореї до 2020 року "розумні" міста будуть побудовані в міжнародних містах Чхонгра і Сонгдо, а також у місті неба Йонджонг-Скай, зосередившись на п'яти сферах: транспорті, запобіганні злочинності, навколишньому середовищі, управлінні об'єктами та наданні міських послуг. Крім того, місто Сонгдо буде побудоване як високотехнологічне бізнес-місто з конвергенцією ІКТ через Інтегрований операційний центр міста Сонгдо, який отримав інвестиції на загальну суму 16,5 млрд. корейських вон станом на 2014 рік [29].

Розумні міста оцінюються як нові двигуни зростання у відповідь на рецесію і вирішення існуючих міських проблем в руслі четвертої промислової революції.

Ця тенденція була природним чином досягнута завдяки політичним намірам і розглядається як ключовий зовнішній фактор розвитку розумних міст.

Зусилля уряду щодо побудови "розумного" міста інтерпретуються переважно як воля центрального уряду (політична воля центрального уряду). Як показано на Рисунку 4, політичний порядок денний центрального уряду стикається з місцевою владою в регіоні, де буде створено місто, що пов'язано з політичною волею місцевої влади. Навіть якщо центральний уряд має сильну волю до створення "розумного міста", бувають випадки, коли вона суперечить самоврядним законам або нормативним актам місцевих органів влади, а також випадки, коли виникають обмеження законів і нормативних актів центрального уряду. Політичний порядок денний уряду завжди слід розглядати разом з політичною волею органів місцевого самоврядування.

Рис.1.5. Конфлікти волі, правові та інституційні обмеження.

Інвестиції

З розвитком "розумних" міст зростає роль зацікавлених сторін, на яких вони прямо чи опосередковано впливають. Якщо міста, засновані на міському плануванні, були продуктом розвитку, орієнтованого на центральну владу, то розумні міста є продуктом поєднання різних децентралізованих зацікавлених

сторін. Реалізація проекту розумного міста і формулювання бачення розумного міста залежать від інтеграції зацікавлених сторін, а їх тісна співпраця є невід'ємною частиною досягнення взаємовигідних кінцевих результатів [19].

Як показано в Таблиці 1 нижче, зацікавлені сторони, що оточують "розумне місто", можна розділити на прямі та непрямі зацікавлені сторони. Прямими зацікавленими сторонами є громадяни та міська влада, державні службовці, відповідальні за надання послуг та розбудову інфраструктури "розумного міста", а також місцеві підприємства. Громадяни є найбільш прямими бенефіціарами послуг розумного міста. Міська влада та керівники міських органів управління є головними дійовими особами у розбудові "розумних" міст та наданні послуг громадянам. Місцеві підприємства в розумному місті можуть отримати пряму вигоду від створення нових прибутків завдяки використанню інфраструктури розумного міста. Непрямі зацікавлені сторони включають постачальників технологій і додатків для "розумних" міст, розробників інтегрованих систем, а також постачальників і операторів інфраструктурних послуг. Вони надають технології та інфраструктурні послуги, пов'язані з розумним містом, в процесі створення продуктів і послуг розумного міста з доданою вартістю.

Таблиця 1.1

Тип	Інвестор
Прямі зацікавлені сторони: місто як замовник	Громадяни, міська влада, державні менеджери з розбудови інфраструктури та надання послуг, місцеві підприємства
Непрямі зацікавлені сторони: сприятливе місто як замовник	Постачальники технологій і додатків, системні інтегратори, постачальники інфраструктурних послуг та оператори

Таким чином, розумні міста з'явилися як засіб вирішення існуючих міських проблем завдяки четвертій промисловій революції. Розумні міста розвиваються в різних країнах і визнані новим двигуном зростання економіки. Уряди усвідомлюють це і демонструють політичні наміри щодо розвитку розумних міст. Реалізація такої політики вимагає гармонізації та інтеграції зацікавлених сторін

"розумних" міст. Четверта промислова революція, політичні зобов'язання щодо "розумних" міст і зацікавлені сторони є ключовими зовнішніми елементами побудови "розумних" міст, які потребують ретельного вивчення.

Висновки першого розділу

Поява «розумних міст» є трансформаційною еволюцією в сучасному міському розвитку. Ця парадигма використовує передові технології Інтернету речей для автоматизації основних міських процесів, пристосованих до конкретних потреб і контекстуальних впливів кожного міста. Впровадження таких технологій, однак, створює значні проблеми з точки зору безпеки даних. Оскільки ці системи за своєю суттю обробляють величезні обсяги персональних даних, вони стають першочерговими мішенями для кіберзагроз.

Відповідно, проектування та розвиток інфраструктури «розумних» міст повинні включати проактивне планування безпеки. Вкрай важливо, щоб ці системи були розроблені на основі найсучасніших протоколів інформаційної безпеки. Інтегруючи надійні заходи безпеки з самого початку, міста можуть захиститися від потенційних порушень, забезпечуючи цілісність і конфіденційність даних громадян, одночасно підтримуючи сталий розвиток «розумного» міського середовища.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА SMART CITY

2.1 Роль IoT у захисті інформаційного середовища smart city

Концепція Інтернету речей (IoT) є фундаментальною складовою розвитку розумних міст. IoT охоплює ідею оснащення електронних об'єктів вбудованими датчиками для збору даних і реагування на них через мережу. Ці розумні пристрої, які варіюються від побутових приладів до загальноміських інфраструктурних систем, є невід'ємною частиною покращення життя в місті за допомогою технологій.

Однак підключення цих пристроїв до мережі також створює нові виклики для безпеки. Розумні пристрої за своєю природою збирають дані про своє оточення і користувачів, що робить їх привабливими цілями для кібератак. Різні дослідження та звіти підкреслюють вразливість цих пристроїв, особливо щодо порушення конфіденційності та несанкціонованого доступу. Поширеною точкою входу для зловмисників є мережевий маршрутизатор. Скомпрометувавши маршрутизатор, зловмисник потенційно може отримати контроль над усіма підключеними інтелектуальними системами та пристроями, що дозволить йому отримати доступ до персональних даних, відстежувати розмови та маніпулювати функціоналом системи, спрощена модель підключення IoT девайсів зображена на рис. 2.1.

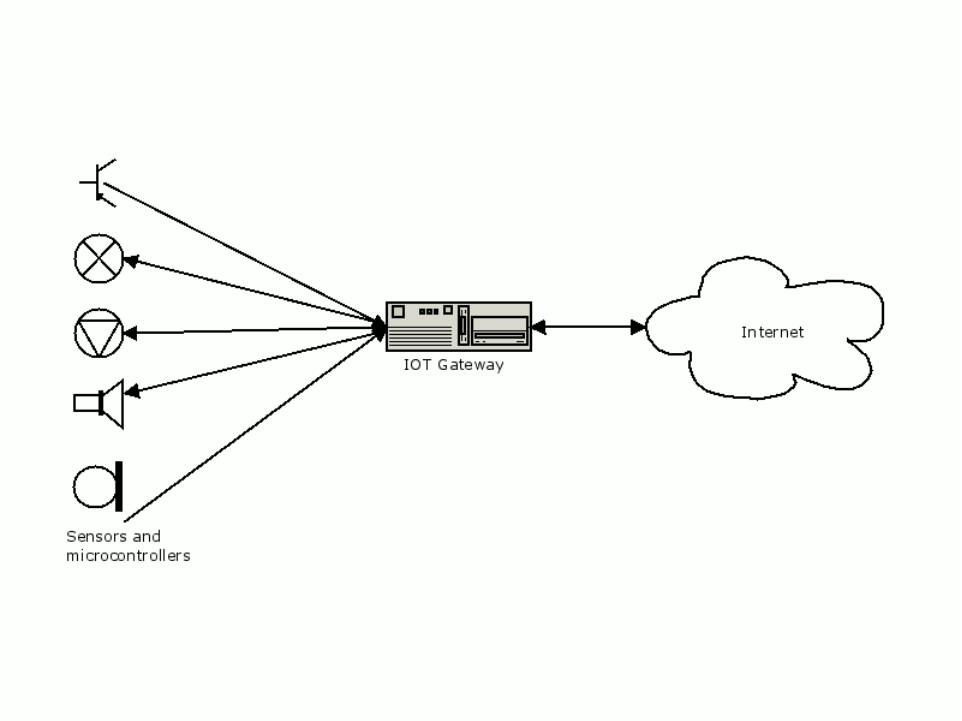

Рис.2.1. модель створення IoT мережі

Можливість того, що інфраструктура розумного міста може стати заручником хакерів, які вимагають викуп, викликає все більше занепокоєння, яке отримує все більше визнання. Залежність розумних пристроїв від з'єднань Wi-Fi, які можуть бути відносно легко зламані людиною з помірними навичками хакерства, посилює цю вразливість. Таке порушення може дозволити несанкціонований доступ до консолі управління пристроєм, персональних даних та прикладних систем.

Для користувачів і адміністраторів "розумних" пристроїв і систем дуже важливо поцікавитися, які заходи безпеки застосовуються на них. Це включає в себе питання про те, чи пропонують пристрої автентифікацію і який тип автентифікації використовується, можливість змінювати імена користувачів і паролі, наявність служби підтримки, обсяг збору персональних даних, чи був у виробника досвід витоку даних, шифрування збережених даних і частоту оновлення програмного забезпечення. Вирішення цих питань є життєво важливим для захисту приватності та безпеки окремих осіб і ширшої інфраструктури розумного міста від потенційних кіберзагроз .

Імплементація розумного пристрою в інформаційне середовище розумного міста не передбачає автоматичну імплементацію знань про безпеку комунікацій і даних, з цього моменту починаються проблеми. Неправильна установка смарт-пристрою або з неповною конфігурацією здатна вплинути не тільки на внутрішню мережу, до якої він підключений, але і безпосередньо загрожувати персональним даним громадян, які мають інтерфейс з цим пристроєм. Нещодавнє дослідження загроз для смарт-пристроїв свідчить, що більшість атак були спрямовані на цифрові відеореєстратори, IP-камери - 63%, тоді як 20% атак були спрямовані на мережеві пристрої, включаючи роутери та DSL-модеми. Китай, В'єтнам і Росія увійшли до трійки країн-лідерів за кількістю атак на смарт-пристрої, кожна з яких має велику кількість "заражених" смарт-пристроїв. З часом кількість атак різко зросте, і причина цього, проста: Смарт-пристрої є крихкими і вразливими для цифрових злочинців.

Переважна більшість "розумних" пристроїв працюють під управлінням операційних систем на базі Linux, тобто ядра Linux, що полегшує їх атаку, оскільки зловмисники можуть написати загальний шкідливий код, який одночасно націлений на величезну кількість "розумних" пристроїв від різних виробників. У світі вже існує понад 5 мільярдів "розумних" пристроїв, на більшості з яких не встановлені засоби захисту, а їхні виробники зазвичай не випускають оновлення безпеки, нові прошивки або патчі. Це означає, що в експлуатації знаходяться мільйони вразливих "розумних" пристроїв, деякі з яких можуть бути вже скомпрометовані.

“Розумних міст не існує, але є розумні міста в очах громадськості” ця думка пов’язана з тим, що пересічний користувач не може знати рівень захищеності свого смарт-пристрою, як і не може знати рівень захисту своїх персональних даних. Нещодавній аналіз показав, що в розвинених країнах розроблена статистика щодо рівня безпеки смарт-пристроїв та вразливостей безпеки після віртуальної атаки шляхом сканування зон IP-адрес, здійсненої зовнішніми факторами, і в декількох випадках показала вразливості та доступ у внутрішню мережу.

Смарт-пристрої використовують і передають значну кількість персональних даних, пов'язаних з їх вузьким приватним функціоналом, з одного боку, вони надходять від їх користувачів, з іншого боку, стосуються тих же користувачів, таких як контактна інформація, дані геолокації, фінансові операції, пошукові запити і різні функції користувача. Крім того, смарт-пристрої можуть зберігати або реєструвати дані в режимі реального часу з багатьох датчиків, таких як мікрофони, датчики паркування, номерні знаки та інші пристрої, що використовуються для роботи з тією метою, для якої вони були встановлені.

Хоча розробники сервісів хочуть надавати нові та інноваційні послуги, ці послуги можуть становити серйозні ризики для конфіденційності та репутації користувачів смарт-пристроїв, смарт-пристрої не завжди відповідають європейському законодавству про конфіденційність, причина полягає в тому, що постачання смарт-пристроїв може здійснюватися через Інтернет, а конкретний пристрій може не відповідати законодавству країни в якій розгортається проект розумного міста.

Атаки на смарт-пристрої будуть збільшуватися в майбутньому, оскільки їх технологія розвивається, а вартість придбання такого пристрою значно знижується. Також зменшується складність встановлення смарт-пристрою, але, на жаль, не існує автоматизованої моделі захисту, помилково вважаючи, що необхідні налаштування безпеки були активовані виробником. Незаконний доступ до таких смарт-пристроїв може призвести до економічної та соціальної катастрофи. Наприклад, несанкціонований доступ до смарт-пристрою, який контролює кількість води, що прокачується насосом, може призвести до пошкодження насоса, зміни частоти його роботи, пошкодження або затоплення резервуару для води або навіть до відключення насоса, що призведе до припинення водопостачання міста. Існує багато способів скомпрометувати розумний пристрій. Щоб поставити під загрозу безпеку смарт-пристрою, не обов'язково спочатку порушувати його безпеку, а потім внутрішню мережу. Запущені вразливі служби, створені віруси-бекдори або мережа контролюється програмами моніторингу IP-пакетів (сніфферами). Віруси дистанційного керування можуть бути встановлені або у

внутрішню мережу користувачем помилково або навмисно, або в якийсь момент, коли мережа скомпрометована, також такі віруси можуть бути встановлені шляхом певного порушення роботи смарт-пристрою, щоб забезпечити доступ до внутрішньої мережі, де підвищити права з можливостями адміністратора або користувача, який має підвищені дозволи, що дозволяють встановлювати додатки. Немало важливою проблемою для IoT мереж є атаки типу “man in the middle” оскільки розумні девайси спілкуються між собою за допомогою простих сигналів Wi-Fi та Bluetooth такий тип трафіку дуже легко перехопити зловмиснику та модифікувати його в деяких випадках, приклад подібної атаки зображено на рис. 2.2.

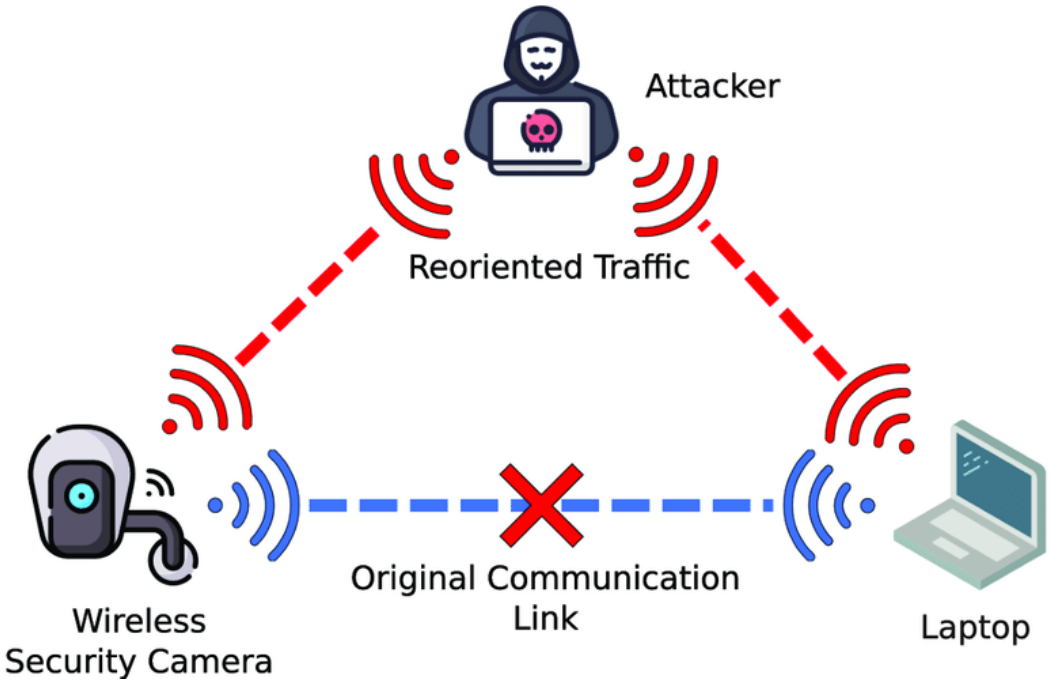

Рис.2.2. Модель атаки людина посередині

Отже, роль Інтернету речей у захисті інформаційного середовища розумного міста є парадоксальною. Хоча пристрої Інтернету речей пропонують потенціал для покращення міського життя, їхні вразливі місця у сфері безпеки створюють значні проблеми. Для зменшення цих ризиків необхідний комплексний підхід, що включає надійні заходи безпеки, регулярні оновлення та прозору політику конфіденційності. Розробка і впровадження суворих стандартів безпеки, а також

інформування користувачів і адміністраторів про потенційні загрози і заходи захисту є важливими кроками на шляху до захисту інформаційного середовища "розумних" міст. Крім того, посилення співпраці між виробниками, міськими планувальниками та експертами з кібербезпеки може підвищити стійкість "розумних" міст до кіберзагроз. Зрештою, захист інформаційного середовища "розумних" міст за допомогою Інтернету речей вимагає узгоджених зусиль для вирішення багатогранних проблем, пов'язаних з технологіями, безпекою і конфіденційністю.

2.2 Використання системи Zero Trust для підвищення захисту

Сучасна проблематика розподілених мереж

Цифрова трансформація змінила світ, спричинивши появу нових технологій, нових культурних парадигм і нових бізнес-моделей. В інформаційну епоху дані постійно надходять на підприємство і виходять з нього з усіх можливих джерел. Кінцеві точки множаться. Працівники працюють на місці, вдома і в кав'ярні.

На жаль, все, що пов'язане з Інтернетом, може бути зламано. Масштабні витоки даних стали звичним явищем за останнє десятиліття. Це відбувається в кожній галузі. Світовий бренд спортивного одягу мав 150 мільйонів облікових записів, що належали дочірній компанії, викрадених в результаті витоку даних. Акції компанії впали майже на 4% [20]. Тим часом, прямі збитки від величезного витоку даних в американській готельній групі, де було скомпрометовано півмільярда записів клієнтів, сягнули 600 мільйонів доларів [21]. Одразу після цього витоку сайт у форматі "запитання-відповідь" підтвердив, що його системи було зламано. За кілька тижнів до цього хакери отримали доступ до персональних даних 29 мільйонів акаунтів однієї з найбільших соціальних мереж [22].

Щодня до цього клубу приєднується ще одна організація - ті, кого зламали, і ті, хто тільки збирається це зробити. Accenture та Ponemon Institute підтверджують, що кіберзлочинність "зростає, займає більше часу на розслідування і обходиться організаціям дорожче". Опитавши сотні провідних компаній, вони виявили, що

середня вартість кіберзлочинів для організацій минулого року зросла на 12% до $13 млн [23]. Порівняно з серединою 2018 року кількість повідомлень про порушення зросла на 54%, а кількість викритих записів - на 52%, що робить 2019 рік "найгіршим роком за всю історію" [24].

Поверхня атаки зростає з кожним днем. Дві третини працівників використовують власні пристрої для роботи, а деякі з них - більше одного (мобільний телефон, планшет, персональний ноутбук, тощо) [25]. Цю тенденцію "приносьте свій власний пристрій" (BYOD) неможливо зупинити, і вона вимагає нових заходів безпеки для управління цими незліченними кінцевими точками. Крім того, кінцеві точки можуть знаходитися в корпоративній мережі або за її межами. У будь-якому випадку, підприємство несе за них відповідальність. Є категорії працівників які працюють виключно з відкритих мереж, кафе або коворкінгу. Розробники можуть створювати власні віртуальні машини для тестування додатків які мають вихід до інтернет. Підприємство повинно захищати бізнес-дані від витоку в споживчі додатки, захищати інформацію у відкритих мережах, підтримувати конфіденційність і дотримання нормативних вимог. Воно повинно мати можливість визначити, чи можна довіряти конкретному пристрою в будь-який момент часу.

На додаток до BYOD, Інтернет речей (IoT) створює мільярди нових кінцевих точок і передає величезні обсяги інформації. Зі збільшенням обсягу даних зростають і можливості для їх компрометації. Якщо пристрої Інтернету речей не захищені належним чином, вони слугують ідеальними точками входу до решти мережі - особливо, якщо вони знаходяться в межах моделі безпеки по периметру. Підприємство більше не існує ізольовано. Часи замкнутих локальних мереж давно минули. Сучасні організації працюють у хмарі та поза нею. Оскільки хмарні обчислення стають нормою, інфраструктура підприємств стає все більш складною і розподіленою. Незалежно від того, чи є хмарні обчислення публічними, приватними або гібридними, вони включають в себе нові види розгортання додатків, мікросервісів, контейнеризацію та безсерверні функції. Як захистити

систему, яку за самою своєю природою ми не можемо обнести стіною (або навіть пристойним парканом)?

Класична стратегія периметра довіряє тим, хто вже знаходиться всередині мережі, і припускає, що загрози є зовнішніми. До користувачів застосовують політику "довіряй, але перевіряй", надаючи їм широкий доступ, якщо вони вважаються "надійними". Захист включає периметр навколо всіх можливих точок доступу до екосистеми підприємства, включаючи мережі, брандмауери, VPN, шлюзи, кінцеві точки і центри обробки даних. Однак все це не допомагає, коли зловмисники вже знаходяться всередині мережі. Середній час перебування загрози в корпоративній мережі становить 100 днів; загроза потрапляє в систему і чекає більше трьох місяців, перш ніж почати діяти.13 Традиційна система безпеки не має інструментів, необхідних для того, щоб викорінити цих зловмисників до того, як вони зможуть завдати шкоди.

Додамо до цього той факт, що 53% порушень спричинені простими людськими помилками працівників підприємства, і стане зрозуміло, що давати користувачам свободу дій, коли вони опиняються всередині периметра, - погана ідея [26]. Зловмисні інсайдерські загрози, такі як незадоволені працівники, корпоративне шпигунство або іноземні урядові агенти, також повинні бути під захистом. Все повинно контролюватися на предмет підозрілої активності. Традиційні підходи також не можуть ефективно захистити кордони за межами периметра. Часто вони навіть не можуть визначити, як поводитися з пристроями BYOD всередині нього.

Саме в цей момент ми можемо звернути свою увагу на систему Zero Trust, яка вирішує вищезазначену проблематику надаючи організаціям нові шляхи в будівництві та оптимізації поточної інфраструктури.

Система Zero Trust

Модель мережевої безпеки Zero Trust працює за принципом "ніколи не довіряй, завжди перевіряй". У цій моделі користувачі та кінцеві точки проходять безперервну автентифікацію і отримують доступ лише до певних, заздалегідь визначених додатків і даних. Крім того, для підтримки привілеїв доступу необхідна

періодична повторна автентифікація. Вдосконалені механізми виявлення загроз активно моніторять мережу, виявляючи аномальні або потенційно зловмисні дії. Завдяки комплексним технологіям управління корпоративною інформацією (EIM), критичні дані централізовані та захищені за допомогою багаторівневої системи безпеки, що простягається від центру підприємства до всіх кінцевих точок. Захист є повним від усіх векторів атак, як зовнішніх, так і внутрішніх. Схема візуалізації принципів EIM зображена на рис. 2.3.

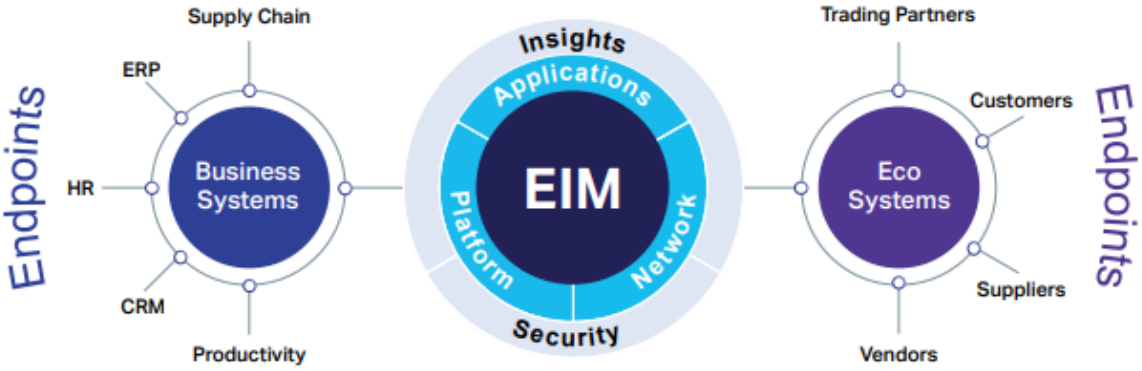

Рис.2.3. EIM в центрі підприємства

Zero Trust полягає на 3 основні стовпи:

1. Давайте розберемося, хто такий користувач.

2. Розуміння кінцевої точки, яка використовується для доступу, та її статусу безпеки.

3. Застосуємо умовну політику, яка визначає доступ.

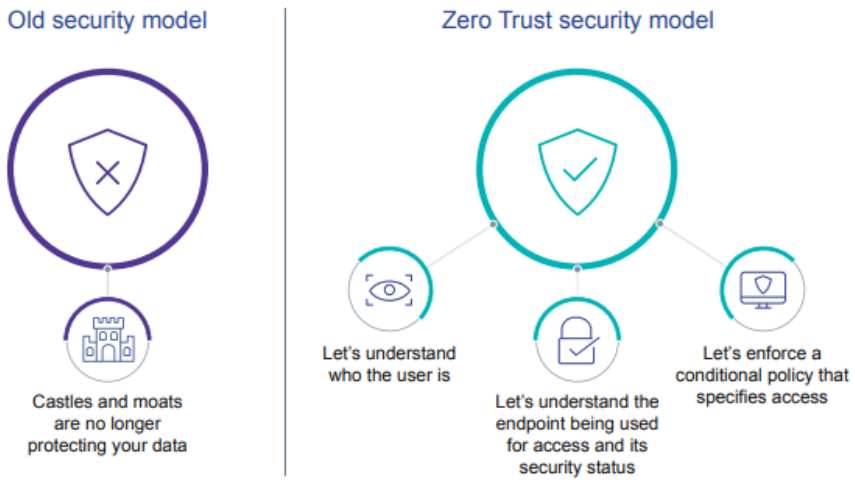

Рис.2.4. Візуалізовна різниця між старим підходом до безпеки та **Zero Trust**

Тепер, ми можемо заглибитись далі в її суть. Розуміння того, хто є користувачем, передбачає технологію, що лежить в основі моделі нульової довіри: Управління ідентифікацією та доступом (IAM). Перш ніж надати доступ до обладнання та додатків компанії, IAM здійснює автентифікацію та авторизацію кожного користувача. Система IAM включає автоматизоване управління життєвим циклом як внутрішніх, так і зовнішніх користувачів, комплексне управління ідентичностями, управління привілейованим доступом та інтегровані можливості багатофакторної автентифікації (MFA). Вона зупиняє розповсюдження ідентифікаційних даних до третіх осіб, централізуючи та захищаючи ідентичності. Однак захист ідентичностей - це лише початок. Один з найпоширеніших способів, яким зловмисники обходять корпоративні протоколи безпеки, - це кінцеві точки. Всі межі є вразливими - сервери, робочі станції, стаціонарні комп'ютери, ноутбуки, планшети, мобільні пристрої. Ось чому система безпеки Zero Trust повинна розуміти кожну унікальну кінцеву точку та її статус безпеки.

Мікросегментація лежить в основі успішного захисту кінцевих точок і, власне, всього підходу до безпеки за принципом нульової довіри. Він вимагає від підприємств сегментації на основі користувачів, їхнього місцезнаходження, чутливості даних та інших категорій. Після цього організації отримують детальну інформацію про трафік і можуть запровадити кілька рівнів моніторингу, перевірки

та контролю доступу на основі інформації про те, хто, що, де, коли, чому і як намагається отримати доступ до захищеної поверхні.

З мікросегментацією змінюється весь вектор загроз. Ніхто не може отримати все. Належна сегрегація запобігає тому, щоб більшість даних навіть не потрапляли під приціл хакерів. Єдиний спосіб, яким зловмисники можуть дістатися до них - це індивідуально, а це складно, оскільки вони повинні спочатку визначити кожну окрему точку входу. Крім того, технології виявлення загроз пильно стежать за незвичною поведінкою з будь-якого джерела, на будь-якому рівні.

Але якщо (або коли) зловмисникам вдається досягти успіху, цільова кінцева точка оснащена технологією виявлення та усунення загроз, яка швидко ізолює, усуває та очищає загрозу. Точно знаючи, хто є кожним користувачем і статус кожної кінцевої точки, технології нульової довіри дозволяють підприємству ефективно впроваджувати політики умовного доступу - також відомі як "доступ з найменшими привілеями" - щоб обмежити доступ кожного користувача лише до необхідних йому ресурсів.

Найменші привілеї зменшують ризик ненавмисного або зловмисного витоку даних, чи то внутрішніми користувачами, чи зловмисниками, які використовують викрадені облікові дані. Як і у випадку з мікросегментацією, ніхто не може мати все. Щоб ефективно впровадити політику найменших привілеїв/умовного доступу та мікросегментування, підприємство має детально оцінити свої дані та політику управління ними. Дані слід класифікувати на основі таких міркувань, як рольовий доступ, толерантність до ризиків, чутливість даних та регуляторні вимоги.

Можливі перешкоди у процесі імплементації

Подолання застарілих систем

Більшість корпоративних технологічних середовищ несуть на собі тягар застарілих додатків, мереж і протоколів, які не були побудовані з урахуванням сучасних потреб. Переробка цих систем вимагає значних зусиль, ресурсів та інвестицій - і, як правило, чим вони старіші, тим більший "технічний борг" вони накопичили. Якщо говорити конкретно про потреби кібербезпеки, то більшість застарілих корпоративних додатків не мають концепції найменших привілеїв.

Наприклад, багато застарілих моделей автентифікації забезпечують єдиний вхід, що не відповідає стандарту нульової довіри. Вони не можуть поєднуватися з іншими технологіями, такими як IAM або захист кінцевих точок.

Іншим прикладом є pear-to-pear (P2P), популярні наприкінці 1990-х років, які також мають тенденцію працювати всупереч принципу нульової довіри. У Windows 10, яка використовується більшістю працівників підприємств, P2P може дозволити несанкціоноване переміщення, що може призвести до витоку конфіденційних даних, якщо не вимкнути спільний доступ до Windows Update. Технологія mesh-мереж покладається на P2P-зв'язок, що робить її ще одним потенційним вразливим місцем. Її модель довіри базується на ключах або паролях; вона не має можливості динамічної автентифікації з нульовою довірою. Як показали останні хакерські атаки, захист доступу користувачів до корпоративних середовищ лише за допомогою ключів чи паролів приречений на невдачу. Зловмисникам дуже легко обійти ці протоколи і отримати необмежений доступ.

Експлуатація кінцевих точок та Інтернет речей

Поверхня атаки збільшилася, головним чином через стрімке зростання кінцевих точок та Інтернету речей (IoT). IoT є основною проблемою для галузей, які вже використовують величезну кількість підключених пристроїв у своєму повсякденному житті, а також для галузей, де ці зміни неминучі. Однією з таких галузей є охорона здоров'я, яка налічує понад 100 мільйонів пристроїв Інтернету речей по всьому світу [27]. У США кожне лікарняне ліжко має від 10 до 15 підключених пристроїв; однак лікарні втратили близько 30% своїх пристроїв, що робить їх відкритими для кібератак [28].

Підприємства, які вирішують проблему експлуатацій кінцевих точок, можуть звернутися до хмари як до союзника з нульовою довірою. Критично важливі дані можуть бути вилучені з кінцевих точок і поміщені в хмару. Зловмисники не зможуть отримати інформацію з кінцевої точки, якщо її там не буде з самого початку. Підключення до хмари також може замінити підключення до штаб-квартири (наприклад, для віддалених співробітників), забезпечуючи кращий захист

і прозорість трафіку. Через хмару можна забезпечити нульову довіру без встановлення брандмауера перед кожним ресурсом.

Чому система Zero Trust актуальна для розумних міст

Таким чином, архітектура нульової довіри спрямована на розробку складних і великих мереж - підхід, який стає більш застосовним до складних середовищ, якими є розумні міста. Саме такі системи потребують складних середовищ з нульовою довірою, щоб вони могли ефективно справлятися з різноманітними та об'ємними мережевими взаємодіями. На відміну від традиційної моделі безпеки, заснованої на периметрі мережі, Zero Trust функціонує на тому, що за замовчуванням не можна довіряти нікому в мережі або поза нею. Це вимагає постійної перевірки джерела кожного запиту на доступ, а отже, збільшує ймовірність несанкціонованого доступу. Нагальна потреба у впровадженні нульової довіри у розвиток розумних міст ставить на сторожі конфіденційні дані та інфраструктуру від будь-яких кіберзагроз через складність та величезну взаємопов'язаність цих цифрових міських екосистем.

2.3 Аналіз та порівняння сучасних методів захисту IoT у контексті інформаційного середовища smart city

Розумні міста особливо вразливі до різних загроз безпеці через розгалужену мережу взаємопов'язаних пристроїв і систем. Ці загрози включають витік даних, несанкціонований доступ, атаки на відмову в обслуговуванні тощо. Складність екосистеми Інтернету речей у розумних містах, що включає численні пристрої та потоки даних, посилює ці ризики, роблячи ландшафт загроз у розумних містах одночасно унікальним і складним.

Для захисту від цих загроз інженери та інші спеціалісти інформаційної безпеки відповідальні за захист системи концентруються на оновлення та впровадження нових стандартів та політик захисту, аналітиці сучасних загроз IoT, використання штучного інтелекту (ШІ) в якості адаптивного аналізу поведінки в мережі (Behavior Analyst), blockchain для безпеки IoT. Ці методи спрямовані на

захист цілісності даних, забезпечення конфіденційності та підтримання загальної безпеки мереж Інтернету речей у розумних містах.

Політики та методики

Для мітігації потенційних загроз в IoT мережах розробники використовують схему зондування на основі політик для IoT під назвою RealAlert, в якій достовірність як даних, так і пристроїв IoT оцінюється на основі історії повідомлень та контексту, в якому дані збираються, використовуючи правила політики. Результати експериментів показали, що схема RealAlert може точно оцінити довіру до сенсорних вузлів, а також до даних в IoT. Однак така система є дуже ресурсо затратною для процесу зберігання та обробки даних, що в свою чергу підвищить рівень необхідних інвестицій.

Threat intelligence

У контексті IoT розвідка загроз (Threat intelligence) може надходити з різних джерел, включаючи спеціалізовані фірми з кібербезпеки, галузеві консорціуми та державні установи. Вона охоплює потоки даних в режимі реального часу, звіти і бази даних, які детально описують поточну діяльність, пов'язану з кіберзагрозами. Використовуючи цю інформацію, системи безпеки Інтернету речей можуть впроваджувати більш ефективні заходи безпеки, такі як вдосконалені системи виявлення вторгнень (IDS) і моделі предиктивного аналізу загроз, які передбачають і протидіють атакам на основі спостережуваних закономірностей. Таким чином, розвідка загроз дозволяє організаціям приймати обґрунтовані рішення щодо безпеки, підвищуючи стійкість мереж Інтернету речей до мінливого ландшафту кіберзагроз.

Штучний інтелект

Для ефективної роботи систем виявлення вторгнень (IDS) необхідно зменшити кількість потоків, пов'язаних з IoT. Таким чином інженери почали використовувати засоби машинного навчання для виявлення аномалій в мережі та виявлення хибно позитивних спрацювань. У 2021 році проводились чисельні експерименти з використанням цього рішення. В наслідок чисельних спроб та

варіацій, запропонована IDS досягла точності 99,7%, використовуючи набори даних термостата, GPS-трекера, гаражних воріт і Modbus за допомогою класифікатора голосування [19].

Blockchain

Blockchain не є новою технологією в мережевій безпеці однак він має потенціал для використання його в мережі розумного міста. Важливо зазначити що blockchain часто йде на противагу системі ZTA оскільки пропонує більш сталий та закритій периметр мережі. Технологія blockchain пропонує децентралізований підхід до безпеки IoT, забезпечуючи прозорість, цілісність даних і захист від несанкціонованого доступу. Використовуючи blockchain, розумні міста можуть створити безпечний і незмінний запис транзакцій і обміну даними між пристроями. Цей метод особливо корисний для управління ланцюгом поставок і безпечних систем голосування, де цілісність і прозорість мають першорядне значення. Однак масштабованість і ресурсо затратність технологій blockchain залишаються проблемами для широкого застосування IoT.

Висновки другого розділу

Підсумовуючи, захист екосистеми Інтернету речей у розумних містах потребує багатогранного підходу, використовуючи комбінацію традиційних і передових методів безпеки. Хоча кожен метод має свої сильні сторони та обмеження, ефективна інтеграція цих технологій має важливе значення для захисту від загроз, що розвиваються. Оскільки ініціативи «розумного міста» продовжують зростати, зростатиме потреба в інноваційних і масштабованих рішеннях безпеки, які можуть адаптуватися до складної та динамічної природи середовищ Інтернету речей.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА SMART CITY

3.1 Визначення ключових аспектів для захисту інформаційного середовища smart city

В попередніх розділах неодноразово аналізувались ризики розумних міст, що є потенційними загрозами.

В розділі 1.1 попередньо досліджувались шари розумного міста, з яких аспектів складається розумне місто. В цьому пункті ми проаналізуємо, що саме в вищезазначених складових рівнях розумних міст є найбільш вразливою їх точкою та на що варто зосередити увагу у процесі побудови інфраструктури безпеки розумних міст.

Рівень послуг та додатків

Як зазначалось в розділі 1.1, рівень додатків присвячений точкам взаємодії користувачів/громадян з можливостями розумного міста. Ці послуги охоплюють широкий спектр, включаючи розумні транспортні системи, які направляють користувачів на оптимальні маршрути, програми спільного використання автомобілів і велосипедів, системи доступності парковок, ініціативи з прозорості уряду та участі громад, функції розумної економіки для підвищення гнучкості ринку праці та регіональної конкурентоспроможності, послуги розумного життя для обміну інформацією в режимі реального часу, дистанційний моніторинг здоров'я та послуги електронної охорони здоров'я. По суті, ці додатки слугують інтерфейсом між цифровою інфраструктурою міста та його мешканцями, обробляючи величезні обсяги даних для надання персоналізованих послуг. Однак саме на цьому рівні взаємодії є найбільше вразливостей, зважаючи на його доступність і безпосередню взаємодію з кінцевими користувачами. Конфіденційність та цілісність є ключовими пріоритетами для захисту на цьому рівні.

Принцип цілісності на рівні додатків розумних міст гарантує, що дані, на основі яких приймаються рішення і надаються послуги, є точними, повними і незмінними, за винятком випадків, коли вони були змінені несанкціонованим чином. Цей принцип має першорядне значення в таких контекстах, як розумний транспорт і моніторинг здоров'я, де маніпуляції з даними можуть призвести до катастрофічних наслідків, включаючи неправильний напрямок руху транспортних засобів або неправильні медичні рекомендації. Тому збереження цілісності даних - це не лише збереження точності інформації, але й нерозривно пов'язане з фізичною безпекою та благополуччям мешканців міста.

З іншого боку, конфіденційність має вирішальне значення для захисту приватності даних громадян, зібраних і оброблених додатками "розумного міста". З точки зору користувачів, які взаємодіють з функціями розумної економіки або беруть участь в урядових ініціативах через цифрові платформи, впевненість у тому, що їхня особиста інформація залишається приватною, є життєво важливою. Порушення конфіденційності не лише підриває довіру до ініціатив "розумного міста", але й наражає людей на ризики крадіжки персональних даних, фінансового шахрайства та інших форм кіберексплуатації.

Збереження цілісності та конфіденційності в додатках "розумного міста" пов'язане з певними труднощами, насамперед через складність і різноманітність цифрової екосистеми. Неоднорідність в взаємодії пристроїв і платформ, задіяних у сервісах "розумного міста", ускладнює впровадження єдиних заходів безпеки. Інтероперабельність цих систем, хоча і має важливе значення для безперебійного надання послуг, також відкриває безліч векторів для потенційних атак. Крім того, динамічний характер даних "розумного міста", що характеризується їх генеруванням і обробкою в режимі реального часу, вимагає надійних, адаптивних протоколів безпеки, здатних реагувати на загрози в режимі реального часу. Масштабованість цих рішень є ще одним критично важливим фактором, оскільки цифрова інфраструктура міст продовжує розширюватися і розвиватися.

Рівень технологій

Рівень технологій присвячений можливостям збору інформації які вже потім буде оброблюватись додатками. На цьому рівні, як правило, оперують IoT девайси та інші пристрої в якості кінцевих точок. Пристрої Інтернету речей за своєю природою призначені для роботи у взаємопов'язаному середовищі, безперервно передаючи та отримуючи дані. Цей взаємозв'язок, хоча і має вирішальне значення для операційної ефективності, ненавмисно створює безліч вразливостей у сфері безпеки. Основна вразливість пов'язана з тим, що багато з цих пристроїв розробляються з акцентом на функціональність і економічну ефективність, часто за рахунок надійних заходів безпеки. Як наслідок, ці пристрої часто не мають необхідних протоколів шифрування, безпечних методів автентифікації та регулярних оновлень програмного забезпечення, необхідних для захисту від складних кіберзагроз.

Більше того, широке розгортання пристроїв Інтернету речей у різних секторах - від "розумних" домашніх приладів до промислових систем управління - загострює ситуацію з ризиками. Багато з цих пристроїв розгортаються в середовищах з мінімальним наглядом за безпекою і часто залишаються з паролями за замовчуванням або з невиправленою прошивкою, що робить їх першочерговими цілями для кібер атак. Простота та однотипність цих вразливостей дозволяє зловмисникам використовувати велику кількість пристроїв з мінімальними зусиллями, полегшуючи виконання розподілених атак на відмову в обслуговуванні (DDoS), витоку даних та шпигунства. На мікрорівні компрометація пристрою Інтернету речей може призвести до несанкціонованого доступу до особистої інформації, втручання в приватне життя і фінансових втрат для окремих осіб. На макрорівні експлуатація слабких місць у захисті пристроїв Інтернету речей, розгорнутих на об'єктах критичної інфраструктури, може призвести до катастрофічних наслідків, в тому числі перебоїв у наданні основних послуг, компрометації конфіденційних даних і підриву національної безпеки.

Рівень пристроїв та датчиків

Цей рівень як зазначалось відповідає за процес комунікації між девайсами збору інформації. Загрози цього шару подібні загрозам фізичного рівня в мережевій моделі OSI. Однак цей рівень також має вразливості, подібні до тих, що спостерігаються на фізичному рівні OSI, представляючи спектр проблем безпеки, які потенційно можуть поставити під загрозу цілісність операцій "розумного" міста. На рівні пристроїв і датчиків основним способом зв'язку є сигнали, які можуть бути перехоплені, модифіковані та підслухані зловмисниками. Простота і повсюдність цих сигналів роблять їх привабливою мішенню для кібератак, спрямованих на порушення нормального функціонування пристроїв збору інформації. Можливість зловмисників проникнути на цей рівень може призвести до маніпулювання даними в самому їхньому джерелі, тим самим порушуючи цілісність інформації, що обробляється наступними рівнями інфраструктури розумного міста.

У контексті розумного міста, де інфраструктура взаємопов'язана і сильно залежить від точних даних, маніпуляції з входами датчиків можуть призвести до масштабних збоїв у роботі. Порушення безпеки на цьому фундаментальному рівні може призвести до каскадних збоїв у різних міських службах, включаючи транспорт, громадську безпеку та управління комунальними послугами.

3.2 Визначення вимог до систем моніторингу які використовуються для захисту інформаційного середовища smart city

Дефініція моніторингу мережі

Термін "моніторинг мережі" означає роботу системи, яка постійно стежить за комп'ютерною мережею в пошуках повільних або несправних систем і при виявленні 3 збоїв повідомляє про них адміністратора мережі електронною поштою, месенджером або іншими засобами сповіщення. Ці завдання є частиною завдань управління мережею. Моніторинг необхідний для того, щоб більш ефективно діагностувати і вирішувати проблеми, коли вони виникають, і, таким чином,

скорочувати тривалість непрацюючих сервісів. Система моніторингу мережі відстежує проблеми, викликані активним і пасивним мережевим обладнанням, кінцевими пристроями або мережевими з'єднаннями. Невдалі запити (наприклад, якщо з'єднання не вдається встановити, закінчується таймаут або повідомлення не було доставлено) зазвичай викликають реакцію з боку системи моніторингу. Як реакція, може бути надісланий сигнал тривоги системному адміністратору або автоматично активована система захисту від збоїв, яка тимчасово виводить з експлуатації проблемний елемент до вирішення проблеми.

Активний моніторинг передбачає виконання мережевих запитів і аналіз їх результатів, в той час як пасивний моніторинг збирає і аналізує мережевий трафік. Активний моніторинг звітує про зібрані вимірювання за допомогою надсилання та отримання мережевих пакетів. Система активних вимірювань має справу з такими метриками, як: корисність, маршрутизатори/маршрути, затримка пакетів, повторна спроба пакетів, втрата пакетів, нестабільна синхронізація між прибуттями, вимірювання пропускної здатності. Здебільшого вона спирається на використання таких інструментів, як команда ping, яка вимірює затримку і втрату пакетів, і traceroute, яка допомагає визначити топологію мережі. Обидва ці інструменти надсилають пробні пакети Internet Control Message Protocol (ICMP) до пункту призначення і чекають на відповідь відправника.

Пасивний моніторинг, на відміну від активного, не додає трафіку в мережу і не змінює трафік, який вже існує в мережі. Пасивні вимірювання мають справу з такою інформацією, як трафік і суміш протоколів, кількість біт (бітрейт), синхронізація пакетів і час між прибуттями. Пасивний моніторинг може бути кращим за активний, оскільки дані не додаються до мережі, але їхня подальша обробка може спричинити значні часові витрати. У реальних системах моніторингу часто використовується комбінація цих двох методів збору інформації.

Таблиця 3.1

Активний Моніторинг Мережі	Пасивний Моніторинг Мережі
Зосереджується на специфічних аспектах для аналізу продуктивності мережі.	Надає повний огляд продуктивності мережі.
Генерує невелику кількість даних.	Генерує велику кількість даних.
Використовується для виявлення та звітування про проблеми, такі як втрата пакетів, джиттер, час відгуку HTTP тощо.	Використовується для ідентифікації елементів, які споживають найбільшу кількість пропускної здатності.
Може вимірювати трафік всередині та зовні мережі.	Може вимірювати трафік лише всередині мережі.

Моніторинг, керований агентами, зменшує навантаження на мережу та обчислювальну потужність системи моніторингу мережі (Network Monitoring System). Агент - це система, встановлена в іншій системі з метою моніторингу та контролю. Агент може передавати статистичну інформацію до NMS, сповіщати про події, надавати API для керування цільовою системою. Однак не у всіх випадках є можливість встановити агента. У деяких випадках адміністраторам потрібно зібрати інформацію про мережу за допомогою якогось параметра. Найбільш очевидним є збір інформації про топологію віртуальної локальної мережі (Virtual Local Area Network) з певним номером. Якщо мережевий контролер відсутній або не підтримує таку функціональність, система моніторингу збирає інформацію про всі VLAN в рамках конфігурації мережевих пристроїв. Дані збираються через певний проміжок часу або за ініціативою пристрою, який надсилає оновлену конфігурацію до системи моніторингу. Періодичний збір даних погано підходить для оперативної роботи, а обробка події зміни конфігурації підтримується не всіма пристроями, має різну реалізацію (наприклад, вимагає не тільки застосування, але і збереження нової конфігурації).

Альтернативою є збір даних на вимогу. Такі дані збираються не постійно, а лише тоді, коли вони потрібні користувачеві. Наприклад, можна збирати дані про топологію певної VLAN у мережі: наявні на пристрої, стан портів (немає, позначені, не позначені). Цей метод відносно простий і невимогливий до мережевих ресурсів і обчислювальних потужностей пристроїв. В ідеальному

випадку запитуються і передаються тільки ті дані, які необхідні користувачеві.

Також важливо зауважити можливість використання так званих систем IDS (Intrusion detection system). IDS сиетма - це пристрій або програмний додаток, який відстежує мережу або системи на предмет зловмисної активності або порушень політики. Про будь-яку зловмисну активність або порушення зазвичай повідомляється адміністратору або збирається централізовано за допомогою системи управління інформацією та подіями безпеки (SIEM). SIEM-система об'єднує дані з різних джерел і використовує методи фільтрації тривог, щоб відрізнити зловмисну активність від хибних тривог. Типи IDS варіюються від окремих комп'ютерів до великих мереж. Найпоширенішими класифікаціями є системи виявлення мережевих вторгнень(NIDS) і системи виявлення вторгнень на основі хостів (HIDS).

Система, яка контролює важливі файли операційної системи, є прикладом HIDS, тоді як система, яка аналізує вхідний мережевий трафік, є прикладом NIDS. Також можна класифікувати IDS за підходом до виявлення. Найвідоміші варіанти - виявлення на основі сигнатур (розпізнавання поганих шаблонів, таких як шкідливе програмне забезпечення) і виявлення на основі аномалій (виявлення відхилень від моделі "хорошого" трафіку, яке часто спирається на машинне навчання). Ще одним поширеним варіантом є виявлення на основі репутації (розпізнавання потенційної загрози відповідно до оцінок репутації). Деякі продукти IDS мають можливість реагувати на виявлені вторгнення. Системи з можливістю реагування зазвичай називають системами запобігання вторгненням. Системи виявлення вторгнень також можуть служити для конкретних цілей, якщо доповнити їх спеціальними інструментами, наприклад, використовувати "honeypot" для залучення та характеристики шкідливого трафіку.

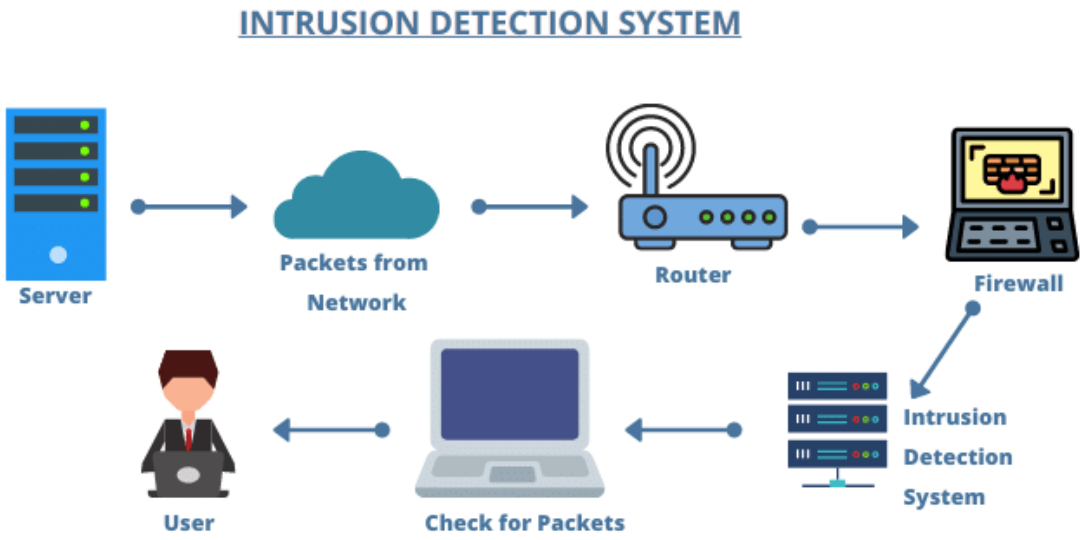

Рис.3.1. Схема імплементації системи IDS

Особливі вимоги розумних міст

На відміну від звичайного інформаційного средовища, розумні міста характеризуються вищим ступенем складності та інтеграції. Вони включають в себе широкий спектр пристроїв Інтернету речей, від камер спостереження до розумних лічильників, які вносять свій внесок у міський пул даних, але також створюють потенційні точки входу для кібератак. Крім того, взаємопов'язаний характер інфраструктури "розумного міста" означає, що вразливість в одній системі може мати каскадні наслідки для багатьох служб, посилюючи потенційний вплив кіберінцидентів. Необхідна значна кількість ресурсів для збору трафіку з усіх девайсів в мережі розумного міста. Оскільки саме постійний моніторинг та аналіз трафіку з усіх девайсів дозволить новим рішенням в сфері IDS/IPS виявляти загрози краще, враховуючи сучасний напрямок розвитку IDS/IPS, а саме інтегрування технологій Deep learning (DL) та Machine learning (ML). Це рішення має як переваги так і недоліки, до переваг можна віднести те що в потенціалі такі системи будуть автоматично виявляти та правильно реагувати на більшість сучасних загроз, але кількість навчального матеріалу для подібних систем обмежена. Розумне місто це дуже велика та комплексна система яка потребує індивідуального підходу, враховуючи це та вище згаданий недолік це робить розумне місто вразливим перед

новими атаками та на початку свого створення до моменту впровадження систем реагування на інциденти.

Більшість NIDS на основі виявлення аномалій намагаються побудувати модель, яка відображає профіль усіх можливих типів поведінки або шаблонів нормального трафіку. Це, однак, надзвичайно складно, оскільки доведено, що такі моделі мають тенденцію зміщуватися в бік домінуючого класу, тобто нормального класу, що призводить до високого рівня хибно позитивних спрацьовувань. Крім того, неможливо врахувати всі можливі нормальні спостереження, які можуть генеруватися в мережі, особливо в гетерогенному середовищі мереж IoT, що збільшує кількість хибно негативних результатів.

3.3 Розробка рекомендацій щодо захисту інформаційного середовища smart city

Провівши аналіз ризиків інформаційного середовища розумного міста, сучасних методів забезпечення захисту інформаційного середовища настільки комплексних та складних мереж, дозволяє нам зробити висновок, що існує кілька ключових технологічних векторів, які можуть значно підвищити стійкість цих цифрових екосистем до кіберзагроз. Розумні міста з їхньою складною мережею взаємопов'язаних послуг і пристроїв створюють унікальний набір викликів безпеці, які вимагають інноваційних підходів до захисту інформаційного середовища. Також спираючись на кращі практики рекомендовані світовими організаціями з кібербезпеки для забезпечення стабільного захисту проти кіберзагроз, що передбачає прийняття багаторівневої стратегії безпеки.

Муніципалітети повинні підтримувати розробку гармонізованої системи кібербезпеки

Розробка гармонізованої системи кібербезпеки дозволить операторам "розумних міст" впроваджувати загальні рекомендації. Такі рамки повинні підтримуватися муніципалітетами, які будуть виступати в ролі координатора між зацікавленими сторонами (операторами, виробниками тощо). Гармонізація

важлива для забезпечення послідовного рівня безпеки для будь-якої служби міста. Ця структура може інтегрувати відповідні стандарти безпеки та існуючі підходи до управління ризиками, враховуючи при цьому особливості міста (наприклад, соціальні аспекти, архітектуру ІКТ тощо). З цієї причини важливо розуміти існуючі підходи, що використовуються в галузі та операторами, оскільки вони знають свої потреби в безпеці та відповідні стандарти. Крім того, "розумні" міста з нижчим рівнем зрілості можуть виявити інтерес до систем, розроблених більш розвиненими муніципалітетами.

Ланцюг постачання обладнання та пристроїв IoT

Організації, відповідальні за впровадження технології "розумного міста", повинні визначити, чи потребуватимуть пристрої та обладнання Інтернету речей, які забезпечать "розумну" функціональність, підтримки сторонніх або зовнішніх сервісів. Ці організації повинні провести комплексну перевірку того, як постачаються і збираються деталі для створення продуктів. Вони також повинні визначити, як пристрої зберігають та обмінюються даними і як пристрої захищають дані в стані спокою, під час передачі та використання. Організації повинні вести реєстр ризиків, який визначає залежність від підтримки хмарних обчислень, зовнішніх компонентів та інших подібних залежностей, як власну, так і від постачальників.

Постачальники керованих послуг та хмарних сервісів

Використання хмари як допоміжного стовпа в інформаційному середовищу розумного міста - це дуже приваблива ініціатива для багатьох організацій та часто може вирішити багато питань одночасно. Однак, організації повинні встановити чіткі вимоги до безпеки для постачальників керованих послуг та інших постачальників, які підтримують впровадження та експлуатацію технологій розумного міста. Організації повинні враховувати ризики, пов'язані з укладанням контрактів зі сторонніми постачальниками, у своєму загальному плануванні управління ризиками та забезпечити включення стандартів безпеки організації в контрактні угоди із зовнішніми сторонами. Аналогічно, організації повинні ретельно переглядати угоди про надання хмарних послуг, включаючи положення

про безпеку даних та моделі розподілу відповідальності.

Планування мережевої архітектури

Як зазначалось в пункті 1.2, розширена поверхня атаки є найкритичнішим ризиком для інформаційного середовища розумного міста. Більшість відомих атак на розумні міста були успішними саме через відсутність грамотної сегментації мережевих девайсів. Згідно до цього, рекомендується слідувати наступним крокам у процесі побудови та підтримки мережі розумного міста.

Крок перший, проведення ретельного аудиту для виявлення і картографування всіх підключених пристроїв і систем в мережі розумного міста. Сюди входять не тільки пристрої Інтернету речей, а й базова інфраструктура, наприклад, сервери та мережеві пристрої, які підтримують ці технології. Після ідентифікації важливо розподілити ці активи за категоріями на основі їхньої критичності та даних, які вони обробляють. Така категоризація допомагає визначити пріоритети заходів безпеки на основі ризику та потенційних наслідків компрометації.

Крок другий, після мапування поверхні атаки необхідно здійснити сегментацію мережі. Розділивши мережу на менші, керовані сегменти, міста можуть ізолювати критичні системи і дані від менш чутливих, обмежуючи потенційне поширення кібератаки. Заходи контролю доступу повинні бути суворими, гарантуючи, що пристрої та користувачі матимуть доступ лише до тих сегментів мережі та даних, які необхідні для їхньої роботи. Цей принцип найменших привілеїв мінімізує ризик латерального переміщення зловмисників всередині мережі.

Крок третій, розширена поверхня атак вимагає безперервного моніторингу для виявлення та реагування на загрози в режимі реального часу. Розгортання передових рішень безпеки, які використовують штучний інтелект і машинне навчання, може допомогти виявити незвичайні патерни і потенційні інциденти безпеки до того, як вони розростуться. У поєднанні з надійною програмою управління вразливостями, яка включає регулярне сканування, оцінку та своєчасне застосування виправлень і оновлень, міста можуть значно зменшити вразливість до

кіберзагроз.

Рис.3.2. Приклад систем об'єднаних в середовище розумного міста

Впровадження моделі Zero Trust в розумних містах

У пункті 2.2 розглядалась система Zero Trust, її переваги та недоліки і відповідно до висновку розілу 2.2 можемо побачити, що ця система є валідною для особливостей інфраструктури розумного міста. Однак, важливо зауважити, що згідно до кращих практик, розумним містам рекомендується розглянути можливість імплементації технологій Blockchain, оскільки ці практики безумовно допоможуть підтримувати цілісність системи від сторонніх девайсів або їх вилучення. Однак такий підхід, як правило, йде в супереч ідеології Zero Trust. Обидва варіанти задовольняють різні потреби розумного міста, однак Zero Trust є більш гнучкою для розширення, що набагато більше пасує розумному місту.

В основі моделі нульової довіри лежить принцип "ніколи не довіряй, завжди перевіряй". Це вимагає впровадження надійних рішень з управління ідентифікацією та доступом (IAM), які забезпечують надійні механізми автентифікації для всіх користувачів і пристроїв, що намагаються отримати доступ до мережі. Багатофакторна автентифікація (MFA), біометрія та цифрові сертифікати є прикладами технологій, які можуть покращити процеси перевірки особи, гарантуючи, що лише авторизовані суб'єкти можуть отримати доступ до

конфіденційних даних та систем. Мікросегментація просуває сегментацію мережі на новий рівень детальності, визначаючи більш детальний контроль доступу, навіть в межах одного сегмента мережі. Цей підхід дозволяє розумним містам впроваджувати управління доступом на основі політик, які динамічно коригуються в залежності від контексту запиту на доступ, наприклад, ролі користувача, його місцезнаходження та чутливості даних, до яких надається доступ. Таким чином, мікросегментація значно зменшує поверхню атаки і обмежує потенційний вплив порушення.

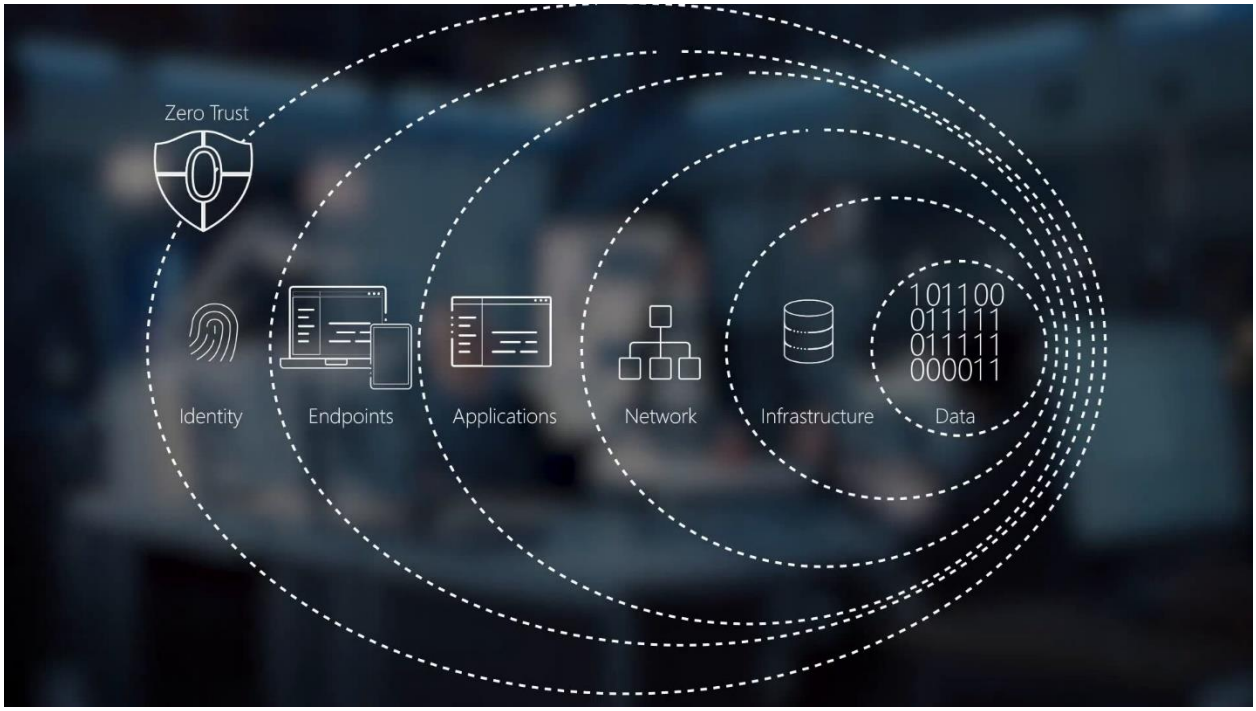

Рис. 3.3. Спрощена модель Zero Trust

Висновки третього розділу

У сучасних розумних містах, де інтеграція та взаємозв'язок IT-інфраструктур досягає високого рівня складності, розвиток гармонізованої системи кібербезпеки є ключовим елементом для забезпечення стійкості міських послуг. Муніципалітети, виконуючи роль координаторів між різними зацікавленими сторонами, повинні підтримувати імплементацію загальних кібербезпекових рамок, які адаптуються до специфіки міста. Ці рамки включають не тільки технічні стандарти, але й розглядають соціальні аспекти та архітектурні особливості ІКТ.

Крім технічних засобів захисту, таких як мікросегментація та багатофакторна автентифікація, важливе значення мають стратегічні підходи типу Zero Trust та використання блокчейн технологій. Ці технології забезпечують підвищений рівень перевірки та контролю доступу, що критично важливо для зменшення ризиків у взаємопов'язаному інформаційному середовищі. Впровадження цих систем вимагає ретельного планування та управління, а також постійного оновлення відповідно до новітніх кіберзагроз.

ВИСНОВКИ

Проведено аналіз сучасних методів захисту інформаційного середовища розумних міст.

Розглянуто шляхи та методи які використовують та які можуть бути використані для забезпечення безпеки інформації, що обробляється розумним містом.

Визначено критичні елементи розумного міста та принципи їх роботи. Розглянуто сучасні методи захисту цих елементів та запропоновано альтернативні методи що використовуються для захисту корпоративних середовищ сьогодні.

Рекомендації, розроблені на основі дослідження сучасних практик, наукових статей, та міжнародних стандартів, ці рекомендації спрямовані на підвищення рівня захисту систем розумного міста без значної інтерференції з ефективністю зазначених процесів. Розглянуто потенціал використання інших методів які можуть бути використані для захисту інформаційного середовища розумного міста.

ПЕРЕЛІК ПОСИЛАНЬ

1. Serrano, M.; Griffor, E.; Wollman, D.; Dunaway, M.; Burns, M.; Rhee, S.; Greer, C. Smart Cities and Communities: A Key Performance Indicators Framework; Special Publication (NIST SP): Gaithersburg, MD, USA, 2022. (date of access: 6.03.2024).

2. Securing the IoT System of Smart City against Cyber Threats Using Deep Learning Received 25 September 2021 ULR: https://downloads.hindawi.com/journals/ddns/2022/1241122.pdf (date of access: 6.03.2024).

3. Kumar, T.M.V. Smart Environment for Smart Cities. In Advances in 21st Century Human Settlements; Springer: Berlin/Heidelberg, Germany, 2020; pp. 1–53. (date of access: 8.03.2024).

4. Oh, I.K.; Seo, J.W.; Lee, M.K.; Lee, T.H.; Han, Y.N.; Park, U.S.; Ji, H.B.; Lee, J.H.; Cho, K.H.; Kim, K. Derivation of Security Requirements of Smart TV Based on STRIDE Threat Modeling. J. Korea Inst. Inf. Secur. Cryptol. 2020, 30, 213–230. (date of access: 8.03.2024).

5. Navarathn, P.J.; Malagi, V.P. Artificial Intelligence in Smart City Analysis. In Proceedings of the 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 13–14 December 2018; pp. 13–14. (date of access: 8.03.2024).

6. Talari, S.; Shafie-Khah, M.; Siano, P.; Loia, V.; Tommasetti, A.; Catalão, J.P. A review of smart cities based on the internet of things concept. Energies 2017, 10, 421. (date of access: 8.03.2024).

7. Bauer, M.; Sanchez, L.; Song, J. IoT-enabled smart cities: Evolution and outlook. Sensors 2021, 21, 4511. (date of access: 10.03.2024).

8. Toma, C.; Alexandru, A.; Popa, M.; Zamfiroiu, A. IoT solution for smart cities' pollution monitoring and the security challenges. Sensors 2019, 19, 3401. (date of access: 10.03.2024).

9. Thirumalaisamy, M.; Basheer, S.; Selvarajan, S.; Althubiti, S.A.; Alenezi, F.;

Srivastava, G.; Lin, J.C.W. Interaction of secure cloud network and crowd computing for smart city data obfuscation. Sensors 2022, 22, 7169. (date of access: 10.03.2024).

10. Alam, T. Cloud-based IoT applications and their roles in smart cities. Smart Cities 2021, 4, 1196–1219. (date of access: 14.03.2024).

11. Park, J.; Chung, H.; DeFranco, J.F. Multilayered Diagnostics for Smart Cities. Computer 2022, 55, 14–22. (date of access: 14.03.2024).

12. Lee, I.; Park, D.; Son, Y.; Lee, Y.; Park, T. Technology Trends of IoT-based Smart city application. J. Comput. Sci. Eng. 2018, 36, 61–68. (date of access: 14.03.2024).

13. Kumar, S.; Rathore, R.S.; Mahmud, M.; Kaiwartya, O.; Lloret, J. BEST—Blockchain-Enabled Secure and Trusted Public Emergency Services for Smart Cities Environment. Sensors 2022, 22, 5733. (date of access: 18.03.2024).

14. Asif, M.; Aziz, Z.; Bin Ahmad, M.; Khalid, A.; Waris, H.A.; Gilani, A. Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities. Sensors 2022, 22, 2604. (date of access: 18.03.2024).

15. Biswas, K.; Muthukkumarasamy, V. Securing smart cities using blockchain technology. In Proceedings of the 2016 IEEE 18th International Conference on High Performance Computing and Communications, IEEE 14th International Conference on Smart City, IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, Austrilia, 12–14 December 2016; pp. 1392–1393. (date of access: 18.03.2024).

16. Barcelona Introduces LED Streetlights That Cut Energy Costs by 1/3 URL: https://inhabitat.com/barcelona-introduces-led-streetlights-that-cut-energy-use-by-13/ (date of access: 23.02.2024).

17. What is a Smart Traffic Management System? URL: https://www.symmetryelectronics.com/blog/what-is-a-smart-traffic-management-system/ (date of access: 23.02.2024).

18. Cybersecurity Best Practices for Smart Cities URL: https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf (date of access 21.02.2024)

19. Alfouzan, F.A.; Kim, K.; Alzahrani, N.M. An efficient framework for securing the smart city communication networks. Sensors 2022, 22, 3053. (date of access: 20.03.2024).

20. Nick Statt, “Under Armour says 150 million MyFitnessPal accounts compromised in data breach,” The Verge, March 29, 2018, URL: https://www.theverge.com/2018/3/29/17177848/under-armourmyfitnesspal-data-breach-150-million-accounts-security (date of access: 25.02.2024).

21. Judy Greenwald, “Direct cyber incident losses from Marriott breach up to $600M: AIR,” Business Insurance, December 18, 2018, URL: https://www.businessinsurance.com/article/20181218/NEWS06/912325732/Direct-cyber-incident-losses-from-Marriott-breach-up-to-$600-million-AIR-Worldwi (date of access: 25.02.2024).

22. Russel Brandom, “Facebook hacker accessed personal details for 29 million accounts,” The Verge, October 12, 2018, URL: https://www.theverge.com/2018/10/12/17968302/facebook-hacker-personal-details-29-million-accounts (date of access: 27.02.2024).

23. Kelly Bissell, Ryan M. Lasalle and Paolo Dal Cin, “Ninth Annual Cost of Cybercrime Study,” Accenture, March 6, 2019, URL: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study (date of access: 27.02.2024).

24. Samantha Ann Schwartz, “Data breaches up 54% YOY, 2019 set to be ‘worst year on record’,” CIO Dive, August 21, 2019, URL: https://www.ciodive.com/news/data-breaches-up-54-yoy-2019-set-to-be-worstyear-on-record/561359/ (date of access: 27.02.2024).

25. Statista Research Department, “Estimated healthcare IoT device installations worldwide from 2015 to 2020,” Statista, May 26, 2016, URL: https://www.statista.com/statistics/735810/healthcare-iotinstallations-global-estimate/ (date of access: 30.02.2024).

26. Zeljka Zorz, “Healthcare’s blind spot: Unmanaged IoT and medical devices,” Help Net Security, July 22, 2019, URL: https://www.helpnetsecurity.com/2019/07/22/healthcare-iot/ (date of access:

30.02.2024).

27. Meera Narendra, “Human error remains the main cause of data breaches,” PrivSec Report, June 20, 2019, URL: https://gdpr.report/news/2019/06/20/human-error-remains-the-cause-of-databreaches/ (date of access: 4.03.2024).

28. Deyan G., “41 Stunning BYOD Stats and Facts to Know in 2019,” TechJury, April 17, 2019, URL: https://techjury.net/stats-about/byod/ (date of access: 30.02.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)