Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: Аналіз стандартів захисту даних у розумних містах

Виконав: студент (ка) IV курсу, групи СБ-42

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Блозва Вікторія Сергіївна
підпис (прізвище та ініціали)

Керівник Деркач М.В.
підпис (прізвище та ініціали)
Нормоконтроль Дроздова Т.В.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Блозві Вікторії Сергіївні
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз стандартів захисту даних у розумних містах

Керівник роботи Деркач Марина Володимирівна, кандидат технічних наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «02» 05 2025 року № 4/7-361.

2. Термін подання студентом завершеної роботи 27.06.2025

3. Вихідні дані до роботи Нормативно-правові вимоги у сфері захисту персональних даних.

4. Зміст роботи (перелік питань, які потрібно розробити)
Проаналізувати архітектуру та загрози Smart City.
Дослідити міжнародні стандарти захисту даних.
Розглянути кейси впровадження стандартів у містах.
Використати Shodan для виявлення вразливих пристроїв.
Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Мета і завдання роботи; Поняття Smart City та його інфраструктура;
Обробка і зберігання даних; Методи та технології захисту даних;
Міжнародні стандарти захисту даних; Огляд прикладів застосування стандартів;
Компоненти системи Shodan; Ілюстрації інтерфейсу Shodan;
Підготовка до пошуку та стратегія його проведення; Пошук пристроїв відеоспостереження;
Пошук пристроїв мережевого обладнання; Пошук зі "smart" веб-інтерфейсом;
Усунення вразливостей ip-камери;
Усунення вразливостей маршрутизатора;
Усунення вразливостей Smart WiFi;
Висновки;

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С.Ю, к.т.н., доц. кафедри МТ		

7. Дата видачі завдання 29.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01 – 30.01	Виконано
2.	Підбір джерел для аналізу стандартів захисту даних у Smart City	01.02 – 07.02	Виконано
3.	Опрацювання нормативних актів та міжнародних стандартів	08.02 – 18.02	Виконано
4.	Аналіз інформаційної архітектури Smart City та її загроз	19.02 – 29.02	Виконано
5.	Аналіз прикладів впровадження стандартів у світових розумних містах	01.03 – 10.03	Виконано
6.	Використання Shodan для виявлення вразливих пристроїв	11.03 – 24.03	Виконано
7.	Оформлення розділу «Основи Захисту Даних У Розумних Містах»	25.03 – 02.04	Виконано
8.	Оформлення розділу «Стандарти Захисту Даних У Системах Smart City»	03.04 – 20.04	Виконано
9.	Оформлення розділу «Аналіз Впровадження Стандартів У Розумних Містах»	21.04-30.04	Виконано
10.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	01.05 – 10.05	Виконано
11.	Оформлення кваліфікаційної роботи	11.05 – 05.06	Виконано
12.	Нормоконтроль	26.06.2025	Виконано
13.	Перевірка на плагіат	26.06.2025	Виконано
14.	Попередній захист кваліфікаційної роботи	26.06.2025	Виконано
15.	Захист кваліфікаційної роботи	27.06.2025	Виконано

Студент _____ Блозва В.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Деркач М.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз стандартів захисту даних у розумних містах // Кваліфікаційна робота ОР «Бакалавр» // Блозва Вікторія Сергіївна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-42 // Тернопіль, 2025 // С. 73, рис. – 19, табл. – 4, кресл. – -, додат. – 1.

Ключові слова: Smart City, стандарти безпеки, ISO/IEC 27001, Shodan, кіберзахист.

У кваліфікаційній роботі досліджено питання інформаційної безпеки у цифровій інфраструктурі розумного міста. Проведено аналіз архітектури Smart City, визначено основні загрози кібербезпеки, а також досліджено міжнародні стандарти захисту даних, зокрема ISO/IEC 27001, ISO/IEC 27701 та NIST SP 800-53. Розглянуто приклади впровадження стандартів у Барселоні, Торонто та Таллінні. За допомогою сервісу Shodan здійснено пошук вразливих пристроїв у міських мережах. Запропоновано рекомендації з посилення стандартів захисту в національних Smart City-проєктах. Робота має прикладне значення для проєктування безпечних міських цифрових систем.

ABSTRACT

Data Protection Standards in Smart Cities // Bachelor's Qualification Thesis // Blozva Viktoriia // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group SB-42 // Ternopil, 2025 // P. 73, fig. – 19, tab. – 4, drawing – 1, appendix – 1

Keywords: Smart City, security standards, ISO/IEC 27001, Shodan, cybersecurity.

This thesis explores data protection issues within the digital infrastructure of smart cities.It analyzes Smart City architecture, identifies key cybersecurity threats, and examines international data protection standards such as ISO/IEC 27001, ISO/IEC 27701, and NIST SP 800-53. Case studies of standard implementation in Barcelona, Toronto, and Tallinn are reviewed.The Shodan service was used to identify vulnerable devices in urban networks. Recommendations for enhancing national Smart City data protection practices are provided. The study has practical value for designing secure digital municipal systems.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IoT	—	Internet of Things
ІКТ	—	Інформаційно комунікаційні технології
LPWAN	—	Low-Power Wide-Area Network
DoS	—	Denial of Service
NAT	—	Network Address Translation
VPN	—	Virtual Private Network
SMB	—	Server Message Block
FTP	—	File Transfer Protocol
PII	—	Personally Identifiable Information
ISMS	—	Information Security Management System
TLS	—	Transport Layer Security
IAM	—	Identity and Access Management
CVE	—	Common Vulnerabilities and Exposures
NVD	—	National Vulnerability Database
API	—	Application Programming Interface
KSI	—	Keyless Signature Infrastructure
HTTP	—	Hypertext Transfer Protocol

ВСТУП

Сьогодні концепція «розумного міста» (Smart City) стрімко набуває популярності у світі, і багато міст впроваджують цифрові рішення для підвищення якості та ефективності надання міських послуг. Розумне місто передбачає інтеграцію сучасних інформаційно-комунікаційних систем у міську інфраструктуру задля оптимального управління ресурсами та покращення якості життя населення. Така модель розглядається як засіб розв'язання викликів, спричинених урбанізацією, і як шлях до створення сталого й комфортного міського середовища. Незважаючи на світові тенденції, в Україні рівень впровадження технологій Smart City дещо низький, оскільки реалізація таких проєктів потребує значних фінансових вкладень, складної координації та високого рівня технологічної експертизи. Крім того, впровадження таких систем створює нові виклики для кібербезпеки міської інфраструктури. Smart City стає потенційною ціллю для кібератак, що створює ризики несанкціонованого доступу до даних, витоку конфіденційної інформації та порушення роботи критичних сервісів.

В умовах війни ці ризики значно зростають: атаки на цифрову інфраструктуру чи витоки даних можуть прямо загрожувати державній, муніципальній та особистій безпеці. Це підкреслює актуальність надійного захисту інформації в розумних містах саме зараз.

Забезпечення кібербезпеки Smart City значною мірою залежить від дотримання належних стандартів захисту даних. Постає потреба у розробці, впровадженні та вдосконаленні як міжнародних, так і національних стандартів безпеки інформації, адаптованих до специфіки розумних міст, що дозволить мінімізувати кіберризики та підвищити довіру до цифрових міських сервісів.

Метою роботи є дослідження ефективності застосування стандартів кібербезпеки в системах Smart City.

Для досягнення цієї мети передбачено виконання таких **завдань**:

- Проаналізувати концепцію та основні принципи забезпечення захисту даних у розумних містах.

- Дослідити сучасні міжнародні та національні стандарти кібербезпеки і захисту даних.
- Оцінити практичне впровадження стандартів захисту даних у проєктах розумних міст.

Об’єкт дослідження: інформаційні системи та технології розумного міста в аспекті забезпечення їх кібербезпеки.

Предмет дослідження: стандарти захисту даних і механізми їхнього застосування в інфраструктурах Smart City.

Практичне значення: результати роботи (виявлені проблеми та запропоновані рекомендації) можуть бути використані органами влади та фахівцями для підвищення рівня захищеності даних при плануванні та реалізації Smart City-рішень.

РОЗДІЛ 1 ОСНОВИ ЗАХИСТУ ДАНИХ У РОЗУМНИХ МІСТАХ

1.1 Інформаційна інфраструктура розумного міста

Розумне місто – це комплексна система, що використовує інформаційно-комунікаційні технології (ІКТ), Інтернет речей (IoT) та штучний інтелект для покращення управління міськими сервісами та інфраструктурою.

Рисунок 1.1 – Приклад розумного міста

Центральним елементом таких систем є *інформаційна інфраструктура розумного міста*, що охоплює мережу сенсорів, пристроїв і платформ обробки даних, які поєднані між собою [1].

Вона є сукупністю цифрових технологій, які збирають, передають, аналізують дані та управляють ними для ефективної оптимізації міського середовища та покращення якості життя мешканців.

Ця інтегрована система формує «нервову систему» міста, забезпечуючи безперервну взаємодію між фізичними об'єктами, цифровими платформами та людьми.

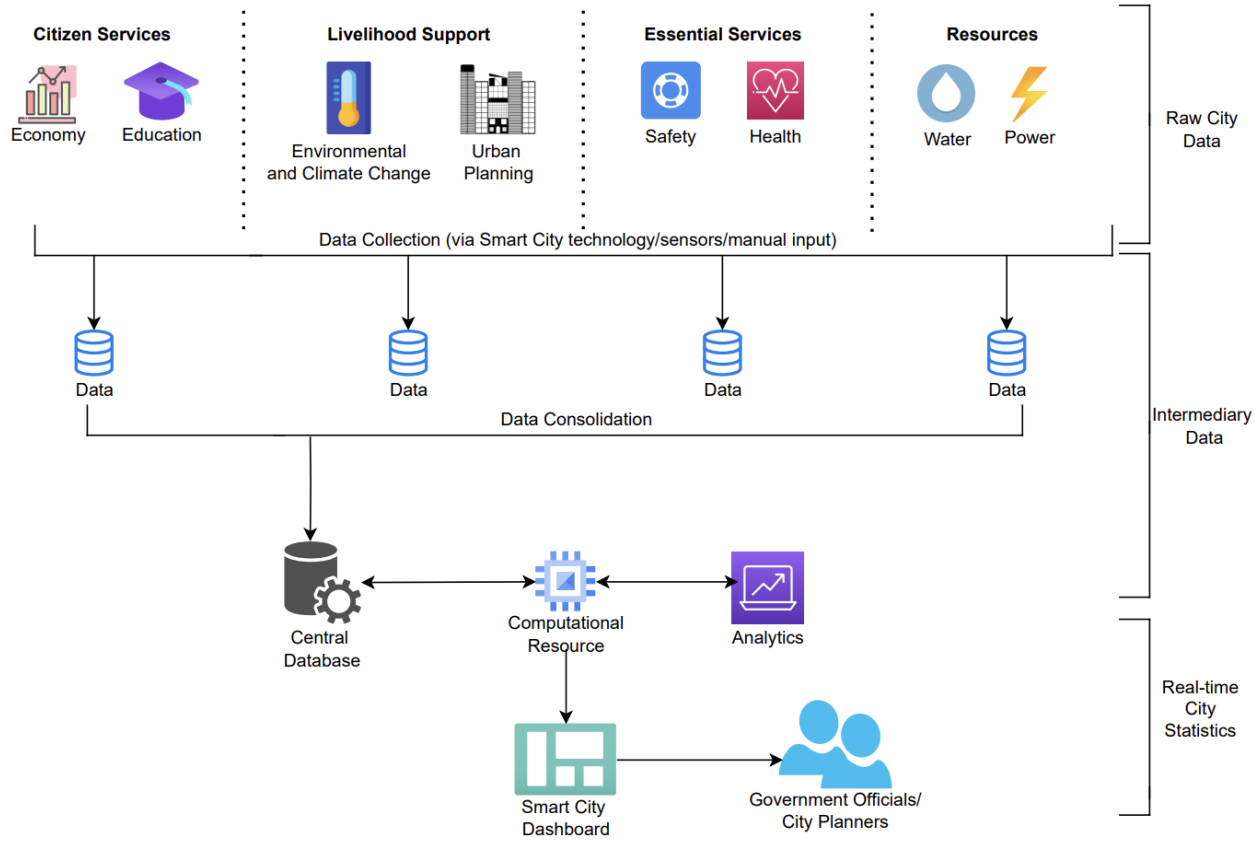


Рисунок 1.2 – Інфраструктура розумногно міста

Її головними елементами є системи моніторингу та управління: різноманітні сенсори, відеокамери та інші датчики, що призначені для збору даних про стан міських об'єктів, таких як дорожня мережа, мости, комунікації, системи енерго- та водопостачання.

Вони є первинними джерелами даних у розумних містах, забезпечуючи збір інформації в реальному часі для широкого спектру застосунків. Функція цих сенсорів полягає у тому, щоб надати місту «відчуття» навколишнього середовища та динамічно реагувати на зміни [2]. Різноманітність типів таких пристроїв відображає різноманітність потреб міського середовища.

До прикладу: смарт-лічильники використовуються для моніторингу споживання води, газу та електроенергії, дозволяючи оптимізувати використання ресурсів та виявляти аномалії.

Датчики трафіку та відеокамери, розміщені на дорогах та світлофорах, збирають дані про транспортні потоки, затори та аварії, що сприяє оптимізації руху та підвищенню безпеки дорожнього руху [3].

Екологічні датчики моніторять якість повітря, рівень шуму, температуру та вологість, допомагаючи міським службам реагувати на зміни навколишнього середовища.

Датчики рівня відходів повідомляють про заповненість сміттєвих баків, оптимізуючи маршрути збору, а також датчики паркування, що передають інформацію про наявність вільних місць, дозволяючи водіям швидко їх знаходити та зменшуючи затори.

Сенсори відіграють не лише роль первинних пристроїв збору даних, а також формують критичний рівень усього ланцюга функціонування розумного міста, оскільки від точності та своєчасності зібраної ними інформації залежить ефективність подальших процесів аналізу, прогнозування та управління міськими ресурсами [4].

Не менш важливою складовою цієї інфраструктури є також системи комунікацій та обміну даними. Вони використовують як дротові, так і бездротові мережі, включаючи мобільний зв'язок стандартів 4G/5G, Wi-Fi та технології LPWAN для забезпечення надійного з'єднання між датчиками, виконавчими пристроями та серверами.

Надійне та доступне мережеве покриття є критично важливим для безперебійної передачі інформації між усіма компонентами інфраструктури.

Наступним елементом виступають інтелектуальні системи аналізу даних. Зібрана інформація обробляється за допомогою алгоритмів штучного інтелекту та інструментів для роботи з великими даними. Ці системи здатні інтерпретувати інформацію, виявляти приховані закономірності, прогнозувати потреби та ефективно сприяти прийняттю рішень щодо управління міськими ресурсами. Крім аналізу, ці платформи забезпечують надійне зберігання величезних обсягів накопичених даних.

Завершальним елементом є платформи управління містом – цифрові інформаційні системи, які слугують єдиною точкою взаємодії для міської влади та мешканців з міськими службами. Вони консолідують дані від різних підсистем, таких як транспорт, житлово-комунальне господарство та безпека, забезпечуючи комплексний моніторинг і централізоване керування ними.

Таким чином, інформаційна інфраструктура розумного міста є багатокомпонентною та динамічною системою [5].

Ця складна взаємодія всіх елементів дозволяє розумному місту не лише «відчувати» та «розуміти» свої потреби, а й активно реагувати на них, оптимізуючи послуги та підвищуючи якість життя громадян.

1.2 Обробка та зберігання даних у системах Smart City

Ефективна обробка та надійне зберігання даних є ключовими для реалізації потенціалу розумного міста як інтелектуальної та динамічної системи, адже саме ці процеси забезпечують перетворення інформації на цінні відомості.

Ці процеси формують основу для прийняття рішень та надання інноваційних міських послуг, враховуючи величезні обсяги, високу швидкість та різноманітність даних, що генеруються в розумних містах.

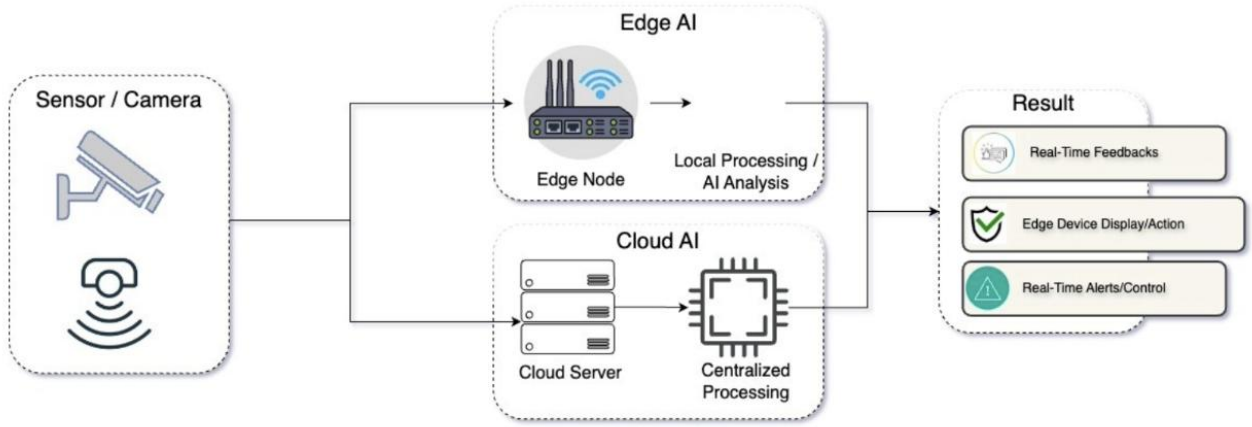


Рисунок 1.3 – Приклад методів обробки даних штучним інтелектом

Обробка даних у реальному часі є необхідною для забезпечення миттєвої реакції на події та динамічну адаптацію операцій у розумних містах. Віднедавна цей процес може реалізуватися за допомогою передових механізмів таких як штучний інтелект та машинне навчання. Вони беруть участь в аналізі масивних обсягів даних, розпізнаванні закономірностей, прогнозній аналітиці та автоматизованому прийнятті рішень.

Зберігання величезних обсягів даних, що генеруються розумними містами, вимагає гнучких, масштабованих та надійних рішень. Для цих цілей застосовуються хмарні обчислення, які надають масштабовані можливості та централізоване зберігання даних, забезпечуючи гнучкість ресурсів та економію на масштабі [6].

Хмарні рішення ідеально підходять для великомасштабної аналітики та довгострокового зберігання даних. Водночас, периферійні обчислення (Edge Computing) дозволяють обробляти дані ближче до джерела їх генерації (наприклад, на самих датчиках або локальних шлюзах). Це значно зменшує затримку, заощаджує пропускну здатність та покращує швидкість реагування для критично важливих застосунків.

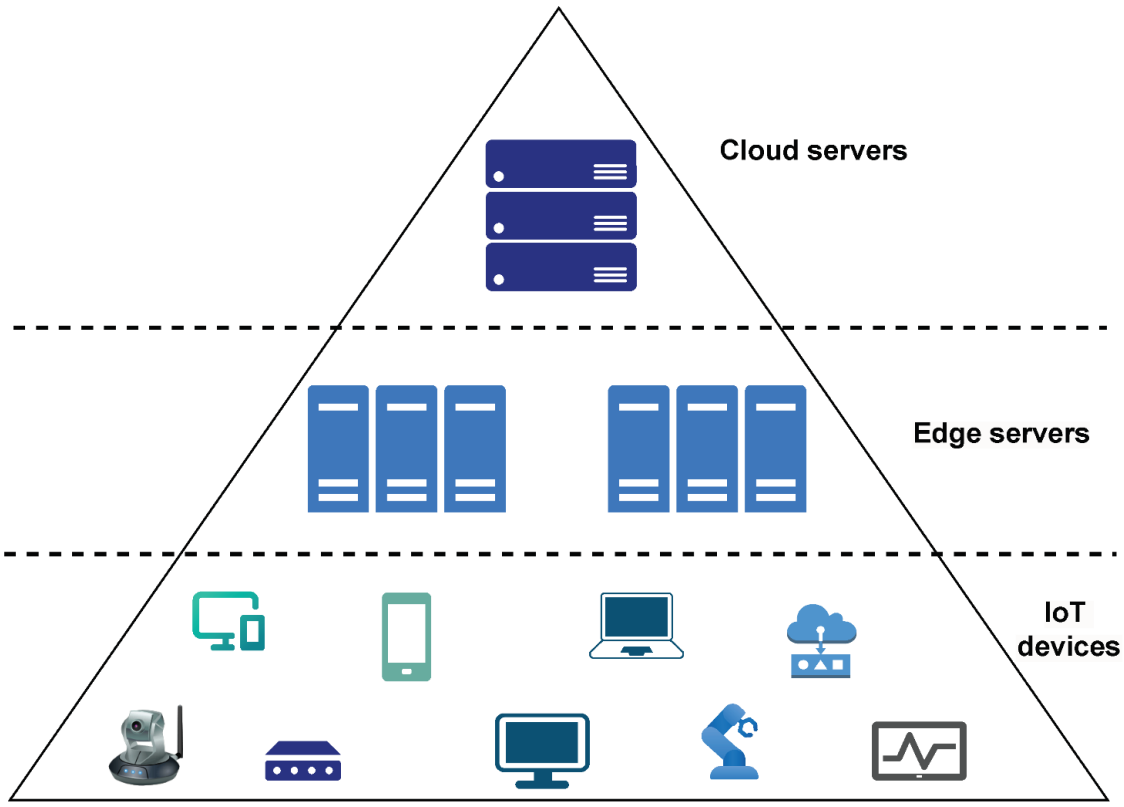


Рисунок 1.4 – Принцип роботи Edge Computing

Для управління та обробки великих обсягів даних від численних джерел також широко використовуються розподілені бази даних, які забезпечують високу доступність та стійкість до відмов, ефективно розподіляючи навантаження. Конвергенція хмарних та периферійних обчислень призводить до

створення гібридних архітектур, що оптимізують використання ресурсів та підвищують швидкість обробки даних у реальному часі.

Попри це, управління даними великих обсягів може створити значний виклик. Він часто описується як «3 В» великих даних (Big Data).

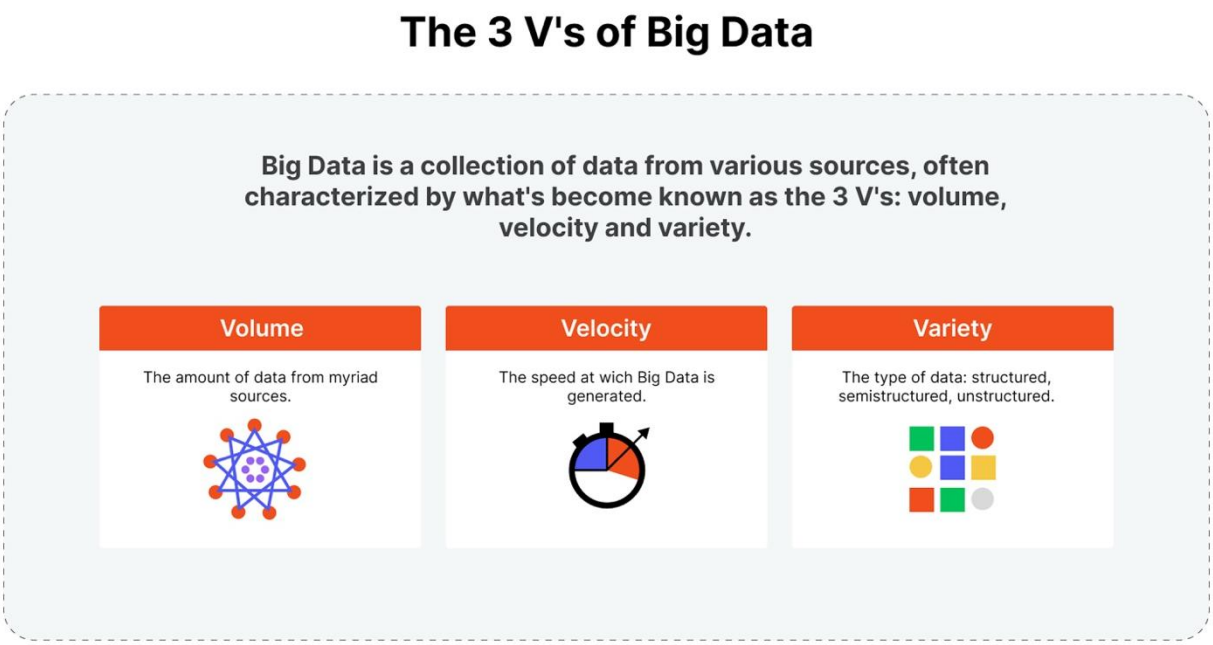


Рисунок 1.5 – Поняття «3 В» у великих обсягах даних

Обсяг (Volume). Розумні міста, з їхніми мільйонами сенсорів, камер та інших пристроїв, генерують астрономічні та постійно зростаючі обсяги даних. Управління такими масивними потоками інформації, що можуть вимірюватися у петабайтах та навіть зетабайтах, вимагає значних обчислювальних потужностей та ресурсів для зберігання, а також значних інвестицій у відповідну інфраструктуру.

Швидкість (Velocity). Дані в розумних містах створюються, збираються та передаються у реальному або майже реальному часі, формуючи безперервний та динамічний потік інформації. Ця висока швидкість вимагає, щоб дані оброблялися та аналізувалися з аналогічною швидкістю, тобто миттєво або з мінімальною затримкою, для забезпечення своєчасного прийняття рішень. Затримки в обробці можуть призвести до втрати актуальності даних для критично важливих міських сервісів.

Різноманітність (Variety). Дані, що надходять у розумному місті, походять з багатьох різних джерел і представлені у різноманітних форматах [7]. Це можуть бути структуровані дані (наприклад, показники лічильників), неструктуровані дані (наприклад, відеозаписи з камер, текстові повідомлення із соціальних мереж), а також мультимедійні файли. Ця неоднорідність значно ускладнює їх інтеграцію, стандартизацію та подальший аналіз, оскільки вимагає застосування різних інструментів та підходів до обробки.

Враховуючи ці характеристики об'ємної кількості даних, ретельне планування інфраструктури та застосування передових технологій є необхідністю для забезпечення її ефективності та масштабованості.

Окрім забору та обробки даних, належне управління ними (Data Governance) відповідає за функціонування та формування довіри до розумних міст.

Рисунок 1.6 – Принципи Data Governance

Ця концепція охоплює систему політик, процесів та стандартів, що гарантують цілісність, безпеку та відповідність даних регуляторним вимогам.

Основні принципи управління даними, як ілюструє Рисунок 1.6, включають: *володіння даними (Ownership)*, *доступність (Accessibility), захищеність (Security), якість даних (Quality) та знання (Knowledge [7]).*

Прозорість даних забезпечує зручний доступ жителів до інформації про міські послуги, сприяючи підвищенню довіри та заохочуючи інновації. Без належного управління навіть технічно захищені системи можуть зіткнутися з ризиками порушень конфіденційності та, як наслідок, втрати громадської довіри.

Проте, зростаючий обсяг та чутливість даних у розумних містах значно підвищують ризики несанкціонованого доступу, витоків інформації та зловживання даними, включно з прихованим спостереженням та профілюванням громадян.

Це зумовлює нагальну необхідність впровадження комплексних заходів безпеки та забезпечення конфіденційності на всіх етапах життєвого циклу даних. Взаємопов’язана природа інфраструктури розширює її поверхню атаки, роблячи розумні міста привабливою мішенню для кібератак, а компрометація одного компонента може призвести до каскадних відмов у пов'язаних системах, спричиняючи широкомасштабні збої та втрату громадської довіри.

Для ефективного пом'якшення цих ризиків необхідна імплементація багаторівневих стратегій, що узгоджуються з принципами Data Governance.

Наприклад: застосування наскрізного шифрування даних під час передачі та зберігання, що забезпечує конфіденційність інформації від перехоплення та несанкціонованого доступу або впровадження надійних механізмів автентифікації та контролю доступу, які гарантують, що лише авторизовані особи та системи можуть взаємодіяти з даними [7].

Ефективна безпека та конфіденційність також нерозривно пов'язані з іншими принципами управління даними. Так, забезпечення *Якості (Quality)* даних допомагає уникнути неточностей, які можуть мати критичні наслідки для прийняття рішень у міському управлінні, а *Доступність (Accessibility)* контролюється для гарантування, що дані доступні лише авторизованим користувачам за потреби та у належний час. *Знання (Knowledge)* про потік даних

та їх використання є важливим для визначення відповідальності та впровадження ефективних заходів безпеки.

Таким чином, безпека та конфіденційність є невід'ємними компонентами комплексної системи управління даними, що є основою для функціонування та довіри до розумних міст.

1.3 Огляд прикладів застосування стандартів захисту даних у розумних містах

Захист даних у розумних містах є не лише питанням відповідності нормативно-правовим актам, а й практичного впровадження принципів безпеки, прозорості та підзвітності у цифрову інфраструктуру. Барселона, Торонто і Таллінн демонструють різні моделі реалізації політик захисту персональних даних у межах смарт-урбаністики. Барселона, як частина ЄС, активно використовує інструменти на основі GDPR і відкритих платформ; Торонто адаптує федеративний і провінційний підхід на базі PIPEDA і MFIPPA, фокусуючись на посткризовому управлінні конфіденційністю після проєкту Sidewalk Labs; Таллінн вирізняється системним використанням цифрових інфраструктур, зокрема X-Road та блокчейн-аудиту, які забезпечують повну простежуваність доступу до даних. [9]

1.3.1 Барселона

Барселона як місто-член ЄС суворо дотримується GDPR і додатково застосовує іспанський Закон про захист даних (LOPDGDD). Відповідно до національного регулювання, зокрема положень LOPDGDD, міські політики захисту приватності базуються на цифрових правах громадян та принципах добросовісності та пропорційності. Однією з ключових технологічних платформ є Sentilo — відкрита IoT-архітектура для збору та обробки даних від приблизно 10 000 сенсорів у міській інфраструктурі. Це рішення забезпечує стандартизовані протоколи для передавання, форматування й шифрування даних. Усі підключені

пристрої проходять верифікацію відповідно до політики відкритого коду, затвердженої муніципалітетом. [9]

Крім того, Барселона бере участь у проєкті IRIS (EU Horizon2020), який спрямований на інтеграцію систем моніторингу безпеки. Інструмент Cisco Cyber Vision застосовується для виявлення мережевих аномалій у реальному часі, що особливо актуально для критичної інфраструктури міста, наприклад, транспортних вузлів. Барселона також активно розвиває Zero Trust як концепцію кібербезпеки, при якій кожна транзакція перевіряється незалежно від джерела.

1.3.2 Торонто

Торонто, як одне з найбільш цифрово активних міст Канади, підпорядковується вимогам PIPEDA на федеральному рівні та MFIPPA на провінційному. Ці акти формують базу для міських політик захисту даних. У 2022 році муніципалітет ухвалив «Protection of Privacy Policy», що передбачає ризик-орієнтований підхід, вбудовування приватності в системи на етапі проєктування (privacy by design), а також посади відповідальних осіб, таких як CISO. [11]

Найбільший вплив на політику приватності в Торонто справив проєкт Sidewalk Labs, який зіштовхнувся з критикою через відсутність прозорих механізмів управління даними. Після його закриття міська влада впровадила низку заходів, які передбачають незалежний нагляд за ініціативами зі збору даних і обов’язкове публічне обговорення проєктів. Нові правила також вимагають проведення оцінки впливу на конфіденційність перед впровадженням будь-яких цифрових сервісів.

1.3.3 Таллінн

Естонія є прикладом глибокої цифрової трансформації на рівні держави. З 2019 року діє Personal Data Protection Act (PDPA), гармонізований з положеннями GDPR. У місті Таллінн муніципальні сервіси діють відповідно до опублікованих

умов захисту даних, які визначають дозволені основи для обробки персональної інформації.

Таллінн активно використовує інфраструктуру X-Road, яка забезпечує повне шифрування при обміні даними між системами. Усі транзакції підписуються цифровими сертифікатами, а історія доступів фіксується у захищеному реєстрі. Системи захисту інтегрують апаратне та програмне шифрування, а також використовують блокчейн KSI для аудиту дій з персональними даними. Це дозволяє виявляти будь-які несанкціоновані дії або спроби змін у записах навіть з боку адміністратора. [12]

Завдяки суворій нормативній базі та технічному захисту, Таллінн гарантує повну підзвітність і прозорість обробки даних, що робить його одним із лідерів цифрового управління у світі.

У першому розділі було розглянуто загальні засади функціонування інформаційної інфраструктури розумного міста, особливості обробки та зберігання даних, а також практичні приклади реалізації стандартів захисту інформації у провідних Smart City-проєктах.

Узагальнено, що ключовими компонентами цифрової архітектури розумного міста є сенсори, системи зв’язку, аналітичні платформи та сервіси управління. Особливу увагу приділено сенсорним мережам, які формують основу оперативного збору даних у міському середовищі.

Також з’ясовано, що ефективність цифрового управління залежить від інтеграції рішень на базі хмарних технологій, периферійних обчислень і принципів Data Governance. Обробка великих масивів даних у режимі реального часу є необхідною умовою забезпечення стабільності та безпеки міської інфраструктури.

Огляд міжнародних кейсів (Барселона, Торонто, Таллінн) показав, що успішна імплементація стандартів захисту даних ґрунтується на поєднанні правових механізмів, технологічних платформ і прозорих політик приватності.

Отримані висновки закладають основу для подальшого моделювання системи захисту даних Smart City, що буде розглянуто у наступному розділі.

1.4 Загрози інформаційній безпеці в Smart City

Системи Smart City стикаються з широким спектром кіберзагроз. Їх можна класифікувати за характером впливу та векторами атаки.

Нижче наведено основні типи загроз, актуальні для розумних міст, та їх детальний опис.

Шкідливе програмне забезпечення (malware): віруси, трояни, черв'яки та програми- вимагачі, які можуть проникати в міські мережі та пристрої. Malware здатний пошкоджувати або шифрувати дані, порушувати роботу систем і надавати хакерам несанкціонований доступ.

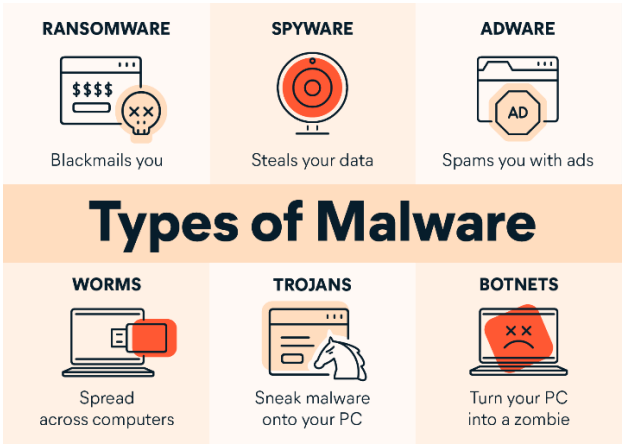


Рисунок 1.7 – Типи шкідливого програмного забезпечення

Особливо руйнівною формою є *ransomware* – програми, що шифрують дані або блокують системи, вимагаючи викуп.

У розумних містах уже були прецеденти таких атак: так, у 2018 році вірус-вимагач паралізував IT-системи міста Атланта (США), змусивши відключити муніципальні сервіси (наприклад, суди) і завдавши багатомільйонних збитків. Подібно, низка інших муніципалітетів (наприклад, округ Матануска-Сусітна на Алясці) постраждали від атак шифрувальників, витративши значні кошти на відновлення систем. [9]

Malware може проникнути через заражені електронні листи, носії даних або використовуючи вразливості в застарілому ПЗ. Його наслідки – крадіжки конфіденційної інформації (трояни можуть збирати паролі, дані кредитних

карток, тощо), виведення з ладу цілих сервісів міста та багато інших збитків для технологічних систем.

DDoS-атаки (розподілені атаки відмови в обслуговуванні): масове надсилання трафіку або запитів на міські сервіси з метою перевантажити їх і зробити недоступними для легітимних користувачів.

У Smart City з його високою залежністю від доступності онлайн-сервісів DDoS становить серйозну загрозу.

Зловмисники можуть використати армії зламаних IoT-пристроїв (ботнети) для генерації потужного трафіку. В результаті міські веб-портали, системи «розумних» світлофорів чи навіть канали зв'язку екстрених служб можуть вийти з ладу через перевантаження.

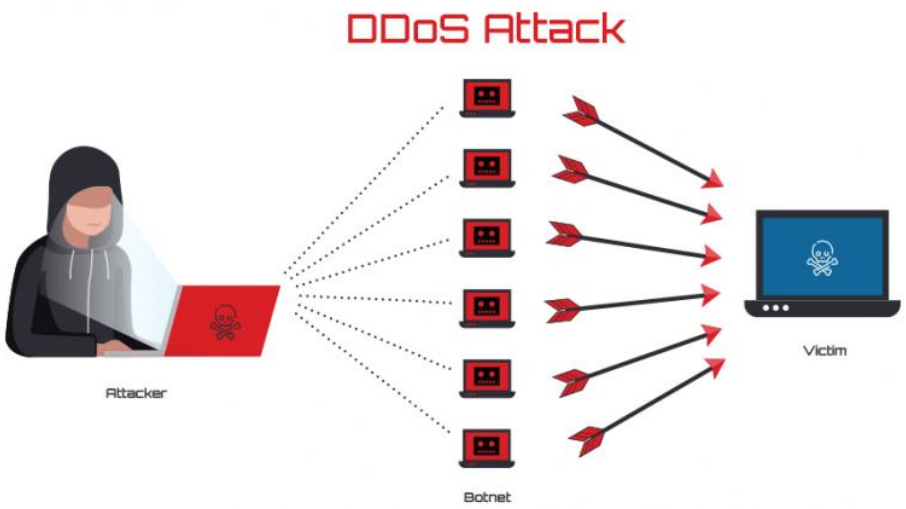


Рисунок 1.8 – Принцип реалізації DDoS-атаки

Дослідження відзначають, що складність і масштаб міських мереж робить їх вразливими до великих DDoS-атак, які здатні спричинити масові збої в роботі послуг і поставити під загрозу громадську безпеку. Мотиви таких атак варіюються: від хуліганства чи протестів до спроб здирництва (вимагають гроші за припинення атаки) чи політичного тиску.

Фішинг та соціальна інженерія: методи обману людей для отримання несанкціонованого доступу.

Рисунок 1.9 – Принцип реалізації фішингової атаки

Фішингові атаки зазвичай реалізуються через підроблені електронні листи або сайти, які маскуються під офіційні. Метою є переконати користувача розкрити свої облікові дані, відкрити шкідливий вкладений файл або перейти за небезпечним посиланням.

В умовах Smart City фішинг часто націлений на посадовців чи адміністраторів систем: один невдалий клік працівника мерії по шахрайському листу і зловмисники отримують пароль від внутрішньої мережі.

Соціальна інженерія може набувати й інших форм – наприклад, телефонні дзвінки, де шахрай видає себе за IT-фахівця і випитує конфіденційні дані. Це надзвичайно поширений вектор атаки: за оцінками, значна частина успішних зламів починається саме з фішингу. Наслідком може стати непомітне проникнення у мережу міста, крадіжка облікових записів і подальше розгортання атак (установлення malware, крадіжка даних і т.д.). Тому навчання користувачів розпізнавати такі хитрощі – життєво необхідне.

Компрометація IoT-пристроїв: розумні міста покладаються на тисячі IoT-ґаджетів: від камер спостереження і «розумних» світлофорів до сенсорів моніторингу довкілля та паркових ліхтарів з інтернет-з'єднанням.

Багато з цих пристроїв мають слабкі місця у безпеці. Наприклад: обмежені ресурси не дозволяють реалізувати складне шифрування, прошивки можуть рідко оновлюватись, а заводські паролі іноді не змінені. Хакери використовують ці вразливості, щоб захопити контроль над пристроями або вивести їх з ладу.

Зламаний IoT-пристрій може стати плацдармом для проникнення глибше в мережу міста або частиною ботнету для здійснення DDoS. При цьому компрометація може лишитися непоміченою. Наприклад: захоплений «розумний» лічильник продовжує начебто нормально працювати, але непомітно передає дані злочинцям чи виконує їх команди.

Потенційні загрози від IoT-компрометацій різноманітні: від підробки показників (що може зашкодити рішенням міста) до використання камер спостереження для таємного стеження за мешканцями. З 2019-го року фахівці зафіксували значне зростання атак на IoT (зростання було на 300% протягом року) що підкреслює актуальність цієї загрози.

Атаки на критичну інфраструктуру: об’єкти на кшталт енергомереж, систем водопостачання, транспортних систем, систем управління дорожнім рухом та інші операційні технології (OT) дедалі більше діджиталізовані та під’єднані до міських мереж.

Це відкриває перед зловмисниками можливість дистанційного втручання, яке раніше було неможливим. Кібернапад на такі системи може призвести до фізичних наслідків: відключення електроенергії на значній території, зупинки громадського транспорту, порушення роботи лікарень чи аварії на промислових об’єктах.

Враховуючи взаємозв’язок інфраструктури, атака в одній сфері може спричинити доміно-ефект на інші. З найбільш відомих прикладів є: атака на електромережу в Україні (2015–2016 рр.), яка залишила сотні тисяч людей без світла; злам системи водоочистки у Флориді (2021), коли зловмисник спробував змінити хімічний склад води, що могла отруїти містян.

У контексті Smart City такі атаки особливо небезпечні, оскільки місто покладається на автоматизацію. Якщо оператори покладаються на систему «розумної» електростанції, а вона скомпрометована, то аварія може статись за

лічені години. Тому критичну інфраструктуру часто виділяють як окремий пріоритет кіберзахисту.

Витоки даних (data breaches): неавторизоване отримання конфіденційної або чутливої інформації з систем. Дані – це стратегічний об'єкт розумних міст, що охоплює інформацію про громадян (особисті записи, фінансові дані, медичні картки), бізнес (комерційні таємниці) і саму інфраструктуру. Така концентрація чутливої інформації зумовлює високий рівень інтересу з боку зловмисників, які можуть переслідувати як фінансові, так і шпигунські цілі.[9]

Витоки можуть статися як результат успішної хакерської атаки (злам бази даних, встановлення шпигунського ПЗ), так і через банальну помилку (незахищене сховище в хмарі, втрачений незашифрований ноутбук чиновника, тощо). Наслідки є досить масштабними: зловмисники можуть оприлюднити або продати персональні дані тисяч мешканців, що порушує приватність і може призвести до шахрайств (наприклад, оформлення кредитів на чуже ім'я).

Для міста це загрожує юридичними позовами, штрафами за недотримання законів про захист даних, а головне – підривом довіри громадян до цифрових сервісів. Часто, після великих витоків людям доводиться масово змінювати документи, паролі, остерігатися цільового фішингу тощо.

Загрози приватності мешканців: окрема категорія, пов'язана не стільки з цілеспрямованими атаками, скільки з ризиками надмірного стеження та збору даних у Smart City.

Міста впроваджують тисячі камер відеоспостереження, системи розпізнавання обличь, трекери руху транспорту і громадян – усе це робиться задля безпеки та ефективності, але водночас породжує ризик масового спостереження.

Без належних політик і контролю міська влада чи оператори можуть зловживати такими даними, порушуючи право людей на приватне життя.

Наприклад: об'єднання даних з камер і з мобільних додатків може дозволити відстежувати пересування конкретної особи по місту. Якщо такі дані потраплять у чужі руки або використовуватимуться непрозоро, це становить загрозу демократії і довірі до влади.

Вже зараз громадяни багатьох міст висловлюють занепокоєння стосовно того, як використовуються їхні дані – чи не продаються вони третім сторонам, чи надійно зберігаються. Таким чином, навіть без зовнішнього втручання, сам характер Smart City як «всевидячої» мережі може загрожувати приватності, якщо не впроваджено чітких рамок і технічних засобів захисту.

Потенційні наслідки згаданих загроз для функціонування міста та добробуту мешканців надзвичайно серйозні.

По-перше, кібератаки можуть спричинити дестабілізацію критичних сервісів: відключення електроенергії, хаос на дорогах через збій світлофорів, недоступність екстреного виклику, параліч платіжних систем транспорту. Усе це напряму впливає на повсякденне життя і безпеку громадян. [8]

По-друге, місто може зазнати значних фінансових втрат: як прямих (оплата викупу при ransomware, витрати на відновлення IT-систем), так і непрямих (втрачений 7 прибуток бізнесів через простої інфраструктури, зниження інвестиційної привабливості).

Для прикладу, дослідження Deloitte показало, що вже у 2018 році середнє сукупнерічне фінансове навантаження від кіберінцидентів для великих міст складало близько €2,8 млн, а один-єдиний атлантський інцидент з ransomware обійшовся місту приблизно у €14,5 млн.

По-третє, наслідком атак може бути фізична небезпека та шкода здоров'ю людей. Якщо кібератака порушує роботу лікарні, систем оповіщення про надзвичайні ситуації чи систем водо- або газопостачання, це створює пряму загрозу життю.

По-четверте, страждає довіра населення до цифрових рішень. Великі витоки даних чи випадки стеження підривають готовність мешканців користуватися smart-сервісами, люди відчувають себе вразливими і менш захищеними. Це може гальмувати впровадження нових ініціатив (жителі будуть проти, скажімо, нових сенсорів або камер).

Нарешті, іміджеві втрати: місто, яке пережило масштабний кіберінцидент, стикається з репутаційним ударом у очах інвесторів, туристів, самих мешканців.

Підсумовуючи, кіберзагрози у Smart City – це не абстрактна IT-проблема, а реальний фактор ризику для стабільності роботи міста, економічного розвитку і якості життя громади. Саме тому кібербезпека повинна стати невід’ємною частиною планування і управління розумними містами, з акцентом на проактивне виявлення й нейтралізацію загроз до того, як вони реалізуються.

РОЗДІЛ 2 СТАНДАРТИ ЗАХИСТУ ДАНИХ У СИСТЕМАХ SMART CITY

2.1 Інформаційна безпека та захист даних

Розбудова Smart City – «розумного міста», що ґрунтується на цифрових технологіях та мережах датчиків, висуває інформаційну безпеку на рівень критично важливого пріоритету.

Інфраструктура Smart City покладається на безперервний потік даних. Якщо ці дані або системи будуть скомпрометовані, наслідки можуть бути масштабними: від ризиків для національної безпеки та економічних втрат до загроз здоров'ю та життю людей.

Наприклад, успішна кібератака може призвести до зупинки критичних міських сервісів, значних фінансових втрат, витоку конфіденційних даних громадян і навіть підірвати довіру мешканців до «розумних» систем. [14]

2.1.1 Ключові принципи та компоненти інформаційної безпеки

Для захисту даних і систем Smart City використовуються базові принципи інформаційної безпеки, відомі як тріада CIA: конфіденційність, цілісність та доступність.

Рисунок 2.1 – CIA-тріада

Дотримання цих принципів дозволяє забезпечити довіру до «розумних» міських сервісів та стабільність їхньої роботи.

Розглянемо кожен із принципів детальніше.

Конфіденційність (Confidentiality) Конфіденційність означає захист даних від несанкціонованого доступу та розголошення.

У контексті Smart City це стосується як персональної інформації мешканців (дані про здоров'я, переміщення, послуги), так і службових даних міста (наприклад, ключі доступу до систем керування інфраструктурою) [15]. Лише уповноважені особи та системи повинні мати доступ до таких даних. Забезпечується конфіденційність, зокрема, такими методами:

•*Шифрування даних*. Данні шифруються як при зберіганні (наприклад, бази даних міста, архіви відео з камер), так і під час передавання мережею, аби зловмисник не міг їх прочитати у разі перехоплення. Сильне шифрування гарантує, що навіть при перехопленні трафіку чи викраденні носія інформації зловмисник не отримає відкриті дані.

•*Контроль доступу.* Впроваджуються суворі механізми автентифікації та авторизації, аби лише довірені користувачі та пристрої мали доступ до систем Smart City. Це означає обов'язкову перевірку особи та надання мінімально необхідних прав доступу кожному акаунту. Жорсткий контроль доступу у поєднанні з обліком дій користувачів допомагає запобігти як зовнішнім вторгненням, так і внутрішнім загрозам, коли хтось з персоналу перевищує свої повноваження.

Завдяки зазначеним заходам конфіденційність гарантує, що критично важлива інформація міста не потрапить до чужих рук – це зберігає приватність громадян і запобігає потенційному шантажу чи саботажу, що може бути здійснений на основі викрадених даних.

Цілісність (Integrity). Цілісність означає точність, повноту й достовірність інформації, а також захищеність її від несанкціонованих змін або знищення. У «розумному місті» рішення приймаються на основі даних сенсорів та інформаційних систем, тому надзвичайно важливо, щоб ці дані були правильними і не спотвореними зловмисниками.

Порушення цілісності може мати серйозні наслідки: скажімо, якщо хакер змінить показники датчика якості повітря або дорожні дані, місто може зробити неправильні висновки і дії (не запустити очищувачі повітря або неправильно скоригувати трафік), що нашкодить мешканцям.

Зокрема, однією з основних практик є використання *хеш-функцій.* Цей підхід передбачає обчислення контрольної суми (хешу) для важливих файлів, таких як журнали безпеки чи прошивки пристроїв. У разі передачі або повторного зчитування даних, система здійснює повторне хешування та порівнює результат із початковим значенням. Найменша невідповідність сигналізує про порушення цілісності, що дозволяє негайно виявити спробу підробки або пошкодження.

Крім того, для гарантування автентичності джерела та незмінності повідомлень застосовуються *цифрові підписи.* Ця технологія базується на механізмах асиметричної криптографії, де приватний ключ використовується для підпису даних, а відкритий для їх перевірки. Таким чином, будь-яке несанкціоноване втручання в структуру повідомлення буде негайно виявлене через невідповідність підпису. Наприклад, при оновленні програмного забезпечення для смарт-лічильників, система приймає лише ті файли, які мають дійсний цифровий підпис від офіційного постачальника, що унеможливлює встановлення шкідливих модифікацій.

Ще одним важливим елементом захисту цілісності є *система контролю версій та резервного копіювання*. Завдяки фіксації кожної зміни в даних з інформацією про час та автора змін, забезпечується можливість аудитів та швидкого виявлення помилкових або злочинних втручань. У випадку втрати даних унаслідок кібератаки, наявність резервних копій дозволяє оперативно відновити систему до стабільного стану, мінімізуючи шкоду для міської інфраструктури.

Забезпечуючи цілісність, Smart City гарантує, що його рішення базуються на надійних та автентичних даних. Це підвищує ефективність роботи служб і довіру громадян до цифрових сервісів, адже вони можуть бути впевнені:

інформація (скажімо, про якість води чи про баланс на транспортній картці) є точною і не була потай змінена.

Доступність (Availability). Доступність полягає в тому, щоб інформація та функції систем були доступні уповноваженим користувачам тоді, коли це потрібно, без неприйнятних затримок чи простоїв. Місто не може «стати розумним», якщо його сервіси не працюють тоді, коли вони потрібні мешканцям або службам – без надійної доступності всі інші вигоди Smart City втрачають сенс.

Для забезпечення доступності інформаційних систем у Smart City застосовується низка технічних та організаційних заходів.

Насамперед, ідеться про формування *відмовостійкої інфраструктури*, яка передбачає дублювання та резервування критичних вузлів. Зокрема, серверні кластери, альтернативні канали зв'язку та джерела безперебійного живлення забезпечують мінімізацію часу простою в разі виходу з ладу окремих компонентів. Відомо, що великі центри обробки даних можуть мати географічно рознесені дублікати, що дозволяє оперативно передавати критичні функції резервному сегменту інфраструктури в умовах надзвичайної ситуації, наприклад, стихійного лиха або кіберінциденту. Додатково застосовується балансування навантаження між декількома обчислювальними вузлами, що запобігає перевантаженню окремих елементів системи.

Значну загрозу для доступності становлять *DDoS-атаки*, спрямовані на блокування сервісів шляхом перевантаження мережевого трафіку. У відповідь на це муніципальні IT-служби впроваджують багаторівневий захист, що включає файрволи, інтелектуальні фільтри трафіку та спеціалізовані DDoS-мітігаційні сервіси. Останні можуть бути як локальними, так і хмарними, де трафік спрямовується через захищені вузли, які нейтралізують атаки без шкоди для основної інфраструктури. Таким чином, навіть у разі масштабної атаки міські сервіси здатні залишатися функціональними, хоча й із тимчасовим зниженням швидкодії.

Крім технічних заходів, важливим аспектом є *організація процесів аварійного відновлення.* Регулярне створення *резервних копій даних* дозволяє

зберігати не лише їхню цілісність, але й забезпечувати швидке відновлення функціонування критичних служб у разі збоїв. Кожна така служба повинна мати задокументований план реагування на інциденти, що визначає алгоритм дій у разі відключення або порушення безпеки. Завдяки цьому досягається висока швидкість переключення на резервні ресурси і підтримується безперервність надання послуг населенню навіть у складних обставинах.

Отже, принцип доступності забезпечує безперебійну роботу міських цифрових сервісів, надаючи авторизованим користувачам можливість отримати потрібну інформацію чи послугу саме тоді, коли вона їм необхідна. Це особливо важливо для систем реального часу (транспорт, безпека), де навіть хвилини простою неприпустимі.

2.1.2 Методи та технології захисту даних у Smart City

Для забезпечення інформаційної безпеки розумних міст застосовується цілий спектр методів і технологій, які дозволяють вибудувати надійну та стійку цифрову інфраструктуру.

В основі таких рішень лежить принцип «безпечного за задумом» (secure by design), що передбачає вбудований захист на всіх рівнях – від кінцевих пристроїв до хмарних сервісів.

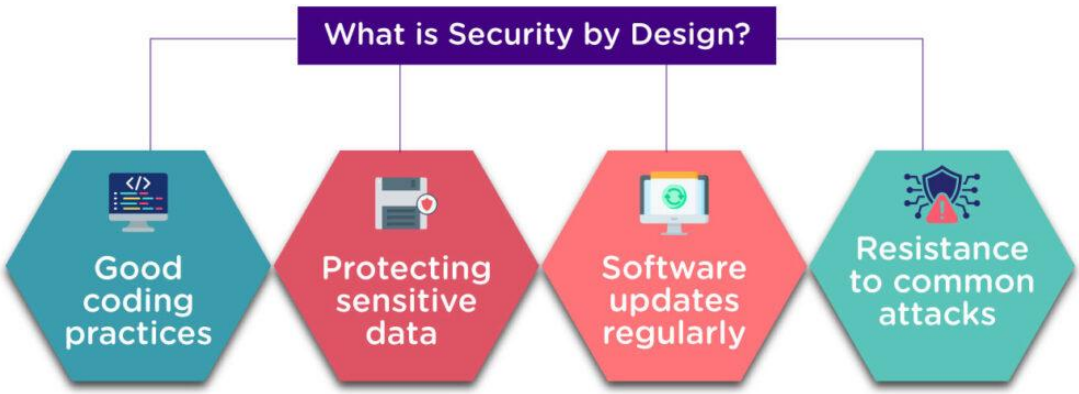


Рисунок 2.2 – Принцип “secure-by-design”

Нижче подано детальний аналіз ключових технологічних компонентів системи захисту в Smart City. [15]

Шифрування є базовим інструментом забезпечення конфіденційності, автентичності й цілісності даних у цифрових інфраструктурах міста. Існують два основні типи шифрування: симетричне та асиметричне.

Симетричне шифрування характеризується високою швидкодією і зазвичай використовується для захисту даних у спокої – наприклад, у базах даних муніципальних служб або відеоархівах систем спостереження.

Асиметричне шифрування є основою для побудови захищених каналів зв'язку (TLS/SSL) і широко застосовується у комунікації між IoT-пристроями та хмарними платформами.

Управління ідентифікацією та доступом (IAM). Інфраструктура Smart City охоплює тисячі користувачів і пристроїв, тому ефективне управління ідентифікацією та доступом (IAM) є критично важливим.

Сучасні системи IAM поєднують автентифікацію, авторизацію, аудит та управління життєвим циклом облікових записів.

Автентифікація дедалі частіше реалізується за допомогою багатофакторної перевірки (MFA), що значно знижує ризики компрометації облікових даних. *Принцип найменших привілеїв (Least Privilege)* застосовується для обмеження доступу користувачів і систем лише до тих ресурсів, які є необхідними для виконання функціональних обов'язків.

Мережева безпека є фундаментом захисту цифрової інфраструктури міста. Вона базується на принципах сегментації, контролю трафіку та виявлення вторгнень.

Міжмережеві екрани (фаєрволи) контролюють трафік між критичними компонентами, тоді як IDS/IPS-системи (Intrusion Detection and Prevention Systems) виконують моніторинг та блокування підозрілої активності у реальному часі.

Для ізоляції важливих підсистем (на кшталт систем водопостачання або мереж енергопостачання) застосовується сегментація мережі, у тому числі за

допомогою VLAN, VPN і ACL. Такий підхід мінімізує ризики латерального розповсюдження загроз у разі проникнення в одну з зон.

Наприклад, навіть при компрометації вузла системи паркування, зловмисник не отримає доступ до мережі обробки медичних даних.

Моніторинг трафіку і поведінковий аналіз мереж (NBA) дозволяють виявляти аномалії, які можуть вказувати на атаки типу DDoS, брутфорс або експлуатацію вразливостей.

Ці засоби інтегруються у загальну систему безпеки міста і дозволяють оперативно ізолювати загрози.

Безпека IoT-пристроїв. IoT-пристрої є вразливим елементом цифрової екосистеми розумного міста через свою масовість, гетерогенність і обмеженість ресурсів. Для захисту IoT-компонентів впроваджуються такі заходи:

- Цифрові сертифікати: пристрої отримують унікальні ідентифікатори та сертифікати PKI для автентифікації.
- Підписані оновлення прошивок: прошивки оновлюються через захищений канал, з обов'язковою верифікацією цифрового підпису.
- Сегментація мереж IoT: ізоляція IoT-зон від загальної IT-мережі з обмеженим маршрутом даних.
- Вбудовані захисти: використання TPM/SE для захисту ключів і запуску тільки перевіреного коду (Secure Boot).

Такі заходи значно підвищують стійкість IoT-інфраструктури до атак та сприяють загальній кіберстійкості міста.

Безпека хмарних сервісів. Оскільки багато функцій Smart City реалізуються через хмарні платформи (зберігання даних, аналітика, візуалізація), безпека хмарного середовища є надзвичайно важливою.

Основні напрямки захисту включають:

- Шифрування даних у хмарі (включно з підходом BYOK).
- Контроль конфігурацій та доступу на основі ролей та MFA.
- Моніторинг активності та журналювання дій адміністраторів.
- Використання WAF, CASB, SIEM для управління безпекою.
- Резервне копіювання та мультихмарні стратегії для відмовостійкості.

Правильна інтеграція хмарних сервісів у систему міської безпеки дозволяє забезпечити відповідність стандартам і законодавству, а також захистити критичні цифрові активи від сучасних загроз.

Загалом, захист даних у Smart City вимагає комплексного підходу, що поєднує технологічні рішення, нормативну відповідність. Тільки такий синергетичний підхід дозволяє забезпечити сталий розвиток розумної міської інфраструктури в умовах динамічного кіберсередовища.

2.2 Міжнародні стандарти захисту даних

Міжнародні стандарти захисту даних набувають ключового значення для побудови довіри та забезпечення безпеки Smart City. Вони визначають найкращі практики управління інформаційною безпекою і приватністю, які є актуальними для міських проєктів по всьому світу. [16]

Застосування таких стандартів у Smart City допомагає гарантувати конфіденційність, цілісність і доступність даних громадян, сприяє дотриманню правових вимог та підвищує рівень довіри мешканців до цифрових сервісів.

Зокрема, широко використовуються стандарти сімейства ISO/IEC а також рамкові документи NIST (National Institute of Standards and Technology).

Усі ці стандарти мають спільну мету – зменшити кіберризики організації та пом’якшити наслідки кібератак шляхом впровадження системного підходу до захисту даних.

У контексті Smart City це означає захистити персональні дані мешканців, гарантувати стійкість критичних сервісів (транспорт, енергомережі, відеоспостереження тощо) та забезпечити безперебійну роботу міської цифрової інфраструктури навіть під час інцидентів.

Далі розглянемо три основні міжнародні стандарти: ISO/IEC 27001, ISO/IEC 27701 та NIST SP 800-53, їх структуру, вимоги та приклади застосування у розумних містах.

2.2.1 Аналіз стандарту ISO/IEC 27001

Стандарт ISO/IEC 27001 є базовим міжнародним нормативним документом у сфері управління інформаційною безпекою. Він визначає вимоги до створення, впровадження, функціонування, моніторингу та постійного вдосконалення Системи управління інформаційною безпекою (ISMS — Information Security Management System) у межах будь-якої організації. Його універсальність забезпечує адаптивність до будь-якого сектора, включаючи муніципальні структури, операторів міських сервісів, а також цифрові платформи в рамках концепції Smart City. [17]

Структурно стандарт ISO/IEC 27001:2022 містить сім обов'язкових розділів (4–10), які охоплюють фундаментальні елементи управлінського циклу (PDCA — Plan-Do-Check-Act), а також додаток Annex.

Оновлений додаток Annex A до стандарту ISO/IEC 27001:2022 містить 93 контрольні заходи інформаційної безпеки, згруповані у чотири категорії: організаційні, фізичні, технологічні та пов'язані з персоналом [ISO/IEC 27002:2022. Guidelines for information security controls].

Ці контролі не є універсальними до застосування, але підлягають відбору на основі оцінювання ризиків, що властиві конкретній міській IT-інфраструктурі, згідно з підходом "заяви про застосовність" (Statement of Applicability).

У контексті цифрового міського середовища доцільним є розгляд наступних контрольних заходів, які мають безпосередню релевантність до критичних міських сервісів.

A.5.18 – Access to information. Встановлення правил і технічних механізмів для обмеження доступу до інформації тільки для уповноважених осіб.

Приклад впровадження: у муніципалітеті функціонує система управління зверненнями громадян, у якій зберігаються персональні дані (ПІБ, адреса, ІПН). Доступ до цієї системи має бути обмежено за принципом "необхідності знання" (need-to-know). Контроль A.5.18 вимагає, щоб:

- було впроваджено ролеву модель доступу (наприклад, лише співробітники відділу персоніфікованого обслуговування можуть бачити ІПН);

- використовувався механізм автентифікації з 2FA;
- велися журнали доступу з метою аудиту.

Таким чином, реалізація контролю запобігає витоку даних унаслідок помилки персоналу або компрометації облікового запису.

A.8.10 – Monitoring activities. Забезпечення постійного спостереження за інформаційною системою з метою виявлення інцидентів безпеки.

Приклад впровадження. Центр ситуаційного реагування міста обробляє відеопотоки з тисяч камер, які встановлені на перехрестях. Застосування контролю A.8.10 означає:

- використання SIEM-системи для моніторингу мережевих з'єднань, ідентифікації підозрілої активності (спроби отримати несанкціонований доступ до камер);
- налаштування автоматичних оповіщень у разі виявлення критичних подій (наприклад, раптове відключення 100 камер з однієї підмережі — потенційна атака).

Контроль гарантує оперативне виявлення порушень безпеки в режимі реального часу.

A.7.4 – Physical security monitoring. Запобігання фізичному доступу до IT-інфраструктури сторонніми особами.

Приклад впровадження. У рамках розвитку транспортної системи місто встановлює кіоски поповнення карток громадського транспорту. Ці пристрої містять мережеві адаптери, зчитувачі банківських карт, SIM-модулі для передачі даних. Застосування A.7.4 передбачає:

- облаштування камер відеонагляду на місцях розміщення кіосків;
- запровадження сигналізації при відкритті технічного люку;
- регулярні перевірки фізичної цілісності корпусів пристроїв (для виявлення втручання, зокрема встановлення стороннього обладнання — скімінгу).

Упровадження цього контролю знижує ризик компрометації даних через фізичний саботаж.

2.2.2 Аналіз стандарту ISO/IEC 27001

Стандарт ISO/IEC 27701:2019 є офіційним розширенням до ISO/IEC 27001 та ISO/IEC 27002, орієнтованим на побудову системи управління конфіденційною інформацією (Privacy Information Management System, PIMS).

Його ключовим завданням є формалізація процедур, політик та технічних засобів для захисту персонально ідентифікованої інформації (PII) в умовах цифрової трансформації суспільства.

Уперше серед стандартів ISO він системно охоплює питання приватності, а не лише інформаційної безпеки, що робить його надзвичайно релевантним у контексті нормативного реагування на виклики, зумовлені впровадженням Загального регламенту ЄС про захист даних (GDPR).

На відміну від ISO/IEC 27001, який фокусується на захисті інформаційних активів загалом, ISO/IEC 27701 доповнює цю систему положеннями, що стосуються прав суб’єктів даних, правомірності обробки персональних даних, а також визначає відповідальність контролерів і обробників інформації.

Важливо, що стандарт не функціонує автономно: його впровадження можливе виключно на базі сертифікованої ISMS, побудованої за ISO/IEC 27001, з відповідними доповненнями в частині оцінювання ризиків і реалізації заходів безпеки для PII [ISO/IEC 27701:2019. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines].

Таким чином, ISO/IEC 27701 забезпечує інтеграцію принципів приватності в загальну систему управління інформаційною безпекою, створюючи основу для формування відповідної політики організації щодо конфіденційної інформації на всіх етапах її обробки.

2.2.3 Аналіз стандарту NIST SP 800-53

Стандарт NIST Special Publication 800–53, Revision 5 («Security and Privacy Controls for Information Systems and Organizations») розроблений Національним

інститутом стандартів і технологій США (National Institute of Standards and Technology, NIST) як систематизований каталог заходів захисту для інформаційних систем державного та приватного секторів.

Уперше опублікований для застосування у федеральних агенціях США, він швидко набув глобального значення, ставши де-факто еталоном для формування політик кібербезпеки в критичних IT-системах.

Актуальна редакція Rev. 5 (2020 р.) є наймасштабнішою з усіх і містить понад 1100 контрольних вимог, об'єднаних у 20 функціональних сімейств контролів. До таких сімейств належать:

- AC (Access Control) – управління доступом.
- SI (System and Information Integrity) – цілісність даних та систем.
- SC (System and Communications Protection) – захист комунікацій.
- PT (Personally Identifiable Information Processing and Transparency) – обробка PII та прозорість.
- інші – що охоплюють політики (PL), безперервність (CP), навчання (AT), фізичну безпеку (PE) тощо.

Відмінною рисою NIST SP 800-53 є високий рівень деталізації: кожен контроль супроводжується конкретним описом, критеріями виконання та можливими варіантами реалізації.

Таким чином, стандарт не лише визначає вимоги, а й виконує роль методичного довідника, який дозволяє організаціям самостійно адаптувати механізми захисту до свого контексту ризиків, типу даних та технічної архітектури.

2.3 Інформаційна безпека та захист даних

Розбудова Smart City в Україні неможлива без узгодження цифрових ініціатив з вимогами національного законодавства у сфері інформаційної безпеки та захисту персональних даних. На відміну від міжнародних стандартів, які мають рекомендаційний характер, українські нормативні акти встановлюють

обов’язкові правила щодо обробки, зберігання та захисту даних в інформаційно-комунікаційних системах.

Цей розділ присвячено аналізу ключових законів, технічних регламентів та стандартів, які визначають правові рамки функціонування цифрової міської інфраструктури в Україні. Особливу увагу зосереджено на аспектах, що мають критичне значення для реалізації концепції Smart City.

2.3.1 Аналіз Закону України “Про захист персональних даних”

Закон “Про захист персональних даних” №2297-VI, прийнятий 1 червня 2010 року, – основний акт, що регулює збір і обробку персональних даних в Україні.

Він встановлює базові поняття (персональні дані, володілець та розпорядник даних, третя особа тощо) та принципи обробки: законність і справедливість, конкретна мета, пропорційність (необхідність і ненадмірність даних), точність, зберігання не довше, ніж це потрібно для мети, захищеність даних і дотримання прав суб’єктів.

Закон зобов’язує отримувати згоду суб’єкта даних на обробку, крім випадків, визначених законом (наприклад, виконання державних функцій або укладення угоди з суб’єктом). Ці підстави схожі до передбачених європейськими директивами.

Визначено права суб’єктів даних: знати про місцезнаходження їхніх даних, отримувати інформацію про мету та осіб, яким передаються дані, доступ до своїх даних, вимагати виправлення або знищення неточних чи незаконно отриманих даних тощо.

Володільці персональних даних (у контексті міста це можуть бути міські адміністрації, комунальні підприємства, центри надання адмінпослуг і т.д.) мають низку обов’язків. Один із ключових: забезпечити належний захист даних.

Закон прямо зобов’язує володільців та розпорядників вживати необхідних організаційних і технічних заходів для запобігання несанкціонованому доступу, витоку або втрати персональних даних. Це означає, що всі міські інформаційні

системи, які містять ПД громадян (реєстри мешканців, електронні квитки, системи “розумного” відеоспостереження з розпізнаванням обличь і т.д.), повинні бути захищені. Наприклад, шляхом контролю доступу, шифрування, аудиту дій персоналу.

Закон містить вимоги повідомляти суб’єктів у разі збору їхніх даних про мету і права, а також регулює транскордонну передачу даних: передача дозволена в країни, які забезпечують належний рівень захисту, або за згодою суб’єкта.

Для сфери Smart City Закон “Про захист ПД” є базовим – всі міські сервіси повинні йому відповідати. На практиці це означає, що впроваджуючи, наприклад, міський мобільний додаток чи портал е-звернень, міська влада повинна: по-перше, визначити чітку мету збору даних (і не виходити за її межі), по-друге, отримати згоду користувачів або мати іншу законну підставу, по-третє, гарантувати реалізацію прав мешканців (надати їм доступ до своїх даних, можливість видалити акаунт тощо), і по- четверте, подбати про безпеку технічної інфраструктури.

Також відповідно до закону міські володільці даних повинні реєструвати бази даних, що містять чутливі персональні дані (здоров’я, біометрія, дані про дітей), та призначати відповідального за захист даних підрозділ або особу.

Важливим питанням для Smart City є обробка зображень громадян системами відеоспостереження – такі дані теж підпадають під закон як персональні, тому їх використання (наприклад, передача поліції чи іншим органам) повинно відбуватися в межах закону.

Закон 2010 року застарів, і в 2021–2023 рр. тривала робота над новою редакцією, щоб наблизити його до GDPR. Станом на кінець 2024 р. парламент прийняв за основу новий законопроєкт №8153 “Про захист персональних даних”, який може найближчим часом замінити чинний закон.

У цьому проєкті враховано сучасні вимоги: введено поняття “контролер” і “процесор” замість “володільця/розпорядника” для синхронізації з термінологією ЄС, розширено перелік прав суб’єктів (додано право на забуття, на перенесення даних, на заперечення, на обмеження обробки тощо),

деталізовано принципи (впроваджено принципи прозорості, підзвітності, мінімізації, які прямо запозичені з GDPR) , посилено вимоги до згоди і умов її дійсності, запроваджено вимогу проведення оцінок впливу на захист даних (DPIA) для ризикових обробок та обов'язок повідомляти про витоки даних регулятора протягом 72 годин і суб'єктів – якщо порушення може спричинити значний ризик.

Для Smart City ухвалення такого закону означатиме суттєве підвищення планки відповідальності: міста муситимуть більш серйозно інвестувати в захист даних, призначати фахівців і виконувати нові процедури.

Підсумовуючи, чинний Закон України "Про захист персональних даних" задає мінімально необхідні рамки для захисту приватності в міських проєктах, але має ряд недоліків (застаріла термінологія, слабкий контроль і санкції).

Міста, які прагнуть відповідати найкращим практикам, вже зараз орієнтуються на GDPR та готуються до нової редакції закону. На перехідному етапі важливо дотримуватися чинних норм (щоб не порушувати права громадян) і паралельно впроваджувати принципи "privacy by design": закладати захист даних у дизайн кожного нового Smart City-сервісу. Це допоможе безболісно адаптуватися до майбутньої більш суворої регуляції та уникнути репутаційних ризиків.

2.3.2 Інші нормативні акти та стандарти: кібербезпека, роль ДССЗЗІ, національні стандарти (ДСТУ)

Окрім закону про персональні дані, екосистема нормативних актів, що стосується Smart City, включає законодавство про кібербезпеку, підзаконні акти щодо технічного захисту інформації та національні стандарти, гармонізовані з міжнародними. [18; 19]

Закон "Про основні засади забезпечення кібербезпеки України" (2017) заклав фундамент державної політики у цій сфері. Для міських органів він важливий тим, що визначає суб'єктів та їх обов'язки.

Зокрема, суб’єктами кібербезпеки є центральні органи влади, місцева влада, об’єкти критичної інфраструктури, підприємства, громадяни та інші – всі, хто залучений до забезпечення стійкості кіберпростору держави.

Закон встановлює принципи: координація, взаємодія держави і приватного сектору, пріоритет захисту критичних об’єктів, невідворотність відповідальності за кіберзлочини.

Для Smart City доцільно визначити, чи належить його інфраструктура до критичної інформаційної інфраструктури (КІІ) згідно з цим законом.

Наприклад, системи електропостачання, міський транспорт, системи екстрених викликів, тощо можуть бути віднесені до КІІ. Тоді на них поширюються підвищені вимоги безпеки, державний моніторинг та інші заходи безпеки.

На виконання закону схвалено Стратегію кібербезпеки України та Концепцію створення державної системи захисту критичної інфраструктури.

Ці документи орієнтують зусилля на пріоритетний захист енергетики, транспорту, зв’язку. Тобто тих сфер, що утворюють основу інфраструктури Smart City.

Важливу роль у реалізації політики кібербезпеки відіграє Державна служба спеціального зв’язку та захисту інформації України (ДССЗЗІ). Це центральний орган виконавчої влади, що формує і реалізує державну політику у сфері захисту інформації та кібербезпеки.

Для міських проєктів ДССЗЗІ є методичним центром: служба видає нормативно-методичні документи з технічного захисту, здійснює державну експертизу комплексних систем захисту інформації (КСЗІ) та може проводити аудит кібербезпеки в держорганах.

Зокрема, якщо у місті створюється інформаційна система, яка обробляє персональні дані в державному реєстрі або таємну інформацію, закон “Про захист інформації в інформаційно-телекомунікаційних системах” вимагає побудови в ній КСЗІ з подальшою державною експертизою в ДССЗЗІ.

КСЗІ – це комплекс організаційних і технічних рішень, що забезпечують захист інформації від несанкціонованого доступу, і діють вони на основі національних нормативів (ДСТУ, НД ТЗІ).

Наприклад, у Києві функціонує міська система відеоспостереження, створена кілька років тому: щоб мати змогу використовувати відео з камер для потреб поліції і зберігати ці записи, було реалізовано КСЗІ та отримано Атестат відповідності від ДССЗЗІ (про це згадується у міських звітах і рішеннях ради).

Вимоги до побудови КСЗІ викладені у 8 відповідних нормативних документах ДССЗЗІ, які базуються на стандартах серії ISO 27000, але враховують українську специфіку.

Щодо національних стандартів, в Україні протягом останнього десятиліття активно проводиться гармонізація з міжнародними. Технічний комітет стандартизації ТК-20 “Інформаційні технології” прийняв низку стандартів ISO/IEC як державні стандарти України (ДСТУ).

Наприклад, діє ДСТУ ISO/ IEC 27001:2015, який є ідентичним перекладом ISO/IEC 27001:2013. Він був чинним до 2023 року і застосовувався українськими підприємствами для розбудови систем управління безпекою.

У серпні 2023 набрав чинності ДСТУ ISO/IEC 27001:2023, що відповідає оновленому стандарту ISO 27001:2022. Аналогічно, було прийнято ДСТУ ISO/IEC 27002:2015 (кодекс практик), ДСТУ ISO/IEC 27005:2015 (управління ризиками) та інші зі складу сімейства 27xxx.

Для приватності впроваджено ДСТУ ISO/ IEC 27701:2022, еквівалент ISO 27701.

Отже, вітчизняні організації, зокрема міські структури, мають змогу офіційно користуватися цими стандартами в українському перекладі та навіть проходити акредитацію/сертифікацію за ними в Україні.

Наприклад, деякі українські IT-компанії, що обслуговують міські сервіси, вже отримали сертифікати ISO 27001, видані міжнародними органами. Компанія GigaCloud (постачальник хмарних рішень для проєктів на кшталт Kyiv Smart City) стала першим українським хмарним оператором з сертифікатом ISO 27001:2013.

Суттєвим для Smart City є і законодавство про електронні комунікації – Закон “Про електронні комунікації” (2021). Він зобов’язує провайдерів телекомпослуг дотримуватися вимог кібербезпеки і захисту споживачів, а також впроваджує норми ЄС щодо конфіденційності зв’язку.

Підсумовуючи, на національному рівні Україна має базові закони і нормативні акти, що охоплюють захист персональних даних та кібербезпеку, але вони перебувають у стадії модернізації та наближення до європейських стандартів.

Паралельно країна гармонізує технічні стандарти: вже зараз Smart City-проєкти можуть керуватися українськими ДСТУ, еквівалентними ISO 27001, ISO 27701 та ін. Це полегшує інтеграцію міжнародних практик у локальний контекст. Ключовим інституційним гравцем є ДССЗЗІ, яка встановлює вимоги до захисту інформації в державних системах і контролює їх виконання.

Успішне впровадження Smart City в Україні неможливе без врахування цих нормативних вимог: від побудови КСЗІ на критичних об’єктах до дотримання всіх юридичних процедур при роботі з персональними даними мешканців.

Отже, забезпечення захисту даних та інформаційної безпеки у системах Smart City є складним, але абсолютно необхідним завданням.

Воно вимагає комплексного та проактивного підходу, що базується на: глибокому розумінні та впровадженні фундаментальних принципів інформаційної безпеки (CIA-тріади), застосуванні передових технологій та методів захисту, адаптованих до унікальних викликів IoT-середовища та хмарних платформ, а також неухильному дотриманні та гармонізації як міжнародних стандартів (ISO/IEC 27001, ISO/IEC 27701, NIST SP 800-53), так і національного законодавства, що постійно розвивається з метою наближення до європейських норм.

Лише такий багатошаровий та інтегрований підхід дозволить Smart City ефективно протистояти сучасним кіберзагрозам, забезпечити стабільність функціонування міських сервісів, захистити приватність мешканців та побудувати довгострокову довіру до "розумних" рішень.

РОЗДІЛ 3 АНАЛІЗ ВПРОВАДЖЕННЯ СТАНДАРТІВ У РОЗУМНИХ МІСТАХ

3.1 Інструменти контролю та моніторингу даних у міських інфраструктурах

У сучасних умовах розвитку Smart City та Smart Home дедалі більше пристроїв IoT під'єднані до інтернету, що підвищує ризики кібербезпеки.

Більшість IoT-пристроїв функціонує у відкритих мережах, часто з мінімальними налаштуваннями безпеки, типовими конфігураціями та застарілими прошивками, що робить їх вразливими до зовнішнього втручання.

Особливо критичною ситуація стає тоді, коли такі пристрої виконують функції, пов'язані з фізичним керуванням. Наприклад, системи освітлення, відеоспостереження, енергорозподілу, водопостачання або диспетчеризації.

Зважаючи на це, своєчасне виявлення слабких місць в інформаційній безпеці таких систем є не лише технічним, а й соціально-економічним пріоритетом.

Практика демонструє, що навіть одна уразливість у публічно доступному IoT-пристрої може стати вхідною точкою до всієї мережі або спричинити компрометацію критичної інфраструктури. У зв'язку з цим, постає потреба у системному підході до моніторингу та ідентифікації таких ризиків на ранніх етапах з використанням сучасних аналітичних інструментів і платформ.

3.1.1 Вибір Shodan як методу дослідження

Shodan часто називають «пошуковцем для хакерів», адже на відміну від традиційних пошукових систем, що індексують вебсторінки, Shodan сканує глобальний інтернет на наявність відкритих портів, активних сервісів і пристроїв, збираючи їхні банери та інші метадані.

Існують й інші пошукові системи для інтернет-пристроїв: Censys, ZoomEye, Thingful тощо. Однак для цілей даного дослідження було обрано саме Shodan. Основною причиною є зручність та функціональність Shodan: він пропонує дружній вебінтерфейс та простий у використанні API, що важливо при проведенні як інтерактивного пошуку, так і автоматизованого аналізу.

За даними порівняльних досліджень, Shodan вважається одним із найкращих інструментів в сфері кіберрозвідки IoT пристроїв завдяки наявності розвинених фільтрів пошуку та підтримки різноманітних утиліт для роботи з його даними.

Важливою перевагою Shodan для цього дослідження є наявність інтегрованих інструментів оцінки вразливостей. Зокрема, вебінтерфейс Shodan на сторінці кожного знайденого пристрою містить окрему вкладку “Vulnerabilities”, де перелічуються знайдені уразливості разом з короткими описами.

Таким чином, вибір Shodan обґрунтований його здатністю не лише знаходити IoT-пристрої, але й надавати контекстну інформацію з точки зору кібербезпеки у зручному вигляді.

Це особливо релевантно для дослідження безпеки Smart City / Smart Home, оскільки дозволяє швидко виявити у мережевому просторі пристрої міської інфраструктури чи домашніх мереж, які можуть мати критичні вразливості, і тим самим оцінити рівень загрози для цих середовищ.

3.1.2 Компоненти системи Shodan

Архітектура та принцип роботи. Shodan підтримує власну розподілену інфраструктуру сканерів, що постійно обстежують інтернет-простір у пошуках активних пристроїв. Сканування відбувається 24 години на добу а виявлені відкриті порти та відповідні служби зберігаються у внутрішній базі даних та регулярно оновлюються в режимі, близькому до реального часу.

Кожен знайдений хост (пристрій) додається до індексу разом з так званим банером (текстовою інформацією, що описує сервіс на цьому пристрої). Залежно

від типу сервісу вміст банера різниться: для вебсервера це можуть бути HTTP-заголовки, для FTP привітальне повідомлення сервера, для промислового протоколу рядок ідентифікації ПЛК, тощо.

Окрім тексту банера, Shodan фіксує і супутні метадані пристрою: географічне розташування (країна, місто, координати), належність до автономної системи чи організації (ISP/ASN), доменне ім’я або hostname (якщо визначено), тип пристрою (за наявності тегів) тощо.

Вся ця інформація структуровано зберігається і доступна через веб-інтерфейс та API для подальшого аналізу.

Результати пошуку та основні параметри. При виконанні запиту Shodan повертає список результатів – пристроїв, що відповідають критеріям. Кожен результат містить базові атрибути: IP-адресу пристрою, відкриті порти і назви сервісів на них, фрагменти банерів, які вказують на версію програмного забезпечення або тип пристрою, а також країну та інші географічні дані. Таким чином, наприклад, пошук може показати вузол з IP 192.0.2.1, на якому відкриті порти 80/HTTP та 502/Modbus, з зазначенням, що це, ймовірно, вебсервер (Apache HTTPD) певної версії та модбас-контролер; також буде вказано, що пристрій знаходиться у Франції і належить до мережі провайдера Orange.

За потреби дослідник може переглянути детальніший банер (наприклад, повні HTTP-заголовки чи протокольні відповіді) у вкладці “Details” на сторінці пристрою.

Ця вкладка містить всю зібрану сервісом інформацію про вузол: перелік всіх відкритих портів і протоколів, детальні банери кожного сервісу, дані про операційну систему (якщо визначено), назву хоста, провайдера, час останнього сканування тощо.

Окремо слід відзначити вище описану вкладку “Vulnerabilities”, що автоматично генерується сервісом на основі банерних даних пристрою.

У цій вкладці перераховані *CVE-ідентифікатори* відомих вразливостей, які потенційно впливають на даний пристрій.

Shodan аналізує версії програмного забезпечення (ПЗ) з банерів і співставляє їх з базою CVE та експлойтів. Якщо знайдено збіг, система відображає відповідний CVE, його короткий опис і оцінку небезпеки.

Важливо зазначити, що Shodan розрізняє підтверджені та непідтверджені уразливості: перші були явно перевірені (наприклад, шляхом специфічного тесту), тоді як другі є імовірними (виведеними лише на основі версії ПЗ).

Непідтверджені вразливості помічені відповідним дисклеймером і потребують ручної перевірки дослідником. Попри це застереження, вкладка з CVE є надзвичайно корисною для експрес-оцінки безпеки: вона одразу вказує, на які саме відомі уразливості слід звернути увагу при подальшому аналізі пристрою.

У контексті практичного дослідження це дозволяє зосередитися на найбільш критичних слабких місцях кожного знайденого вузла, базуючись на авторитетних джерелах (NVD, Exploit-DB тощо) про вразливості.

3.2 Пошук вразливих пристроїв за допомогою сервісу Shodan

3.2.1 Підготовка до пошуку та стратегія дослідження

Перед початком роботи із Shodan необхідно визначити чітку стратегію пошуку, аби результати були релевантними цілям дослідження. Підготовчі кроки включають формулювання пошукових запитів і вибір ключових слів, які найкраще відображають потрібні типи IoT-пристроїв у середовищах Smart City та Smart Home.

Застосування системи Shodan у дослідницьких цілях потребує розуміння базових принципів її роботи, а також синтаксису пошукових запитів. Основу методології становить комбінація ключових параметрів, які дозволяють звузити область пошуку та сфокусувати його на окремих класах пристроїв, протоколах або сервісах. Найбільш релевантні параметри для аналізу безпеки IoT-компонентів наведені у таблиці 3.1:

Таблиця 3.1 – Параметри пошуку, що релевантні до IoT пристроїв у Shodan

Параметр	Опис
port:	Пошук пристроїв, що мають відкритий вказаний порт (наприклад, port:554 — RTSP-потоки).
country:	Обмеження результатів за країною (наприклад, country:UA).
org:	Фільтр за організацією/провайдером інтернету.
city:	Обмеження результатів по місту (наприклад, city:Kyiv).
product:	Пошук пристроїв або сервісів за назвою програмного забезпечення чи прошивки (наприклад, product:MikroTik).
os:	Пошук за операційною системою (наприклад, os:Linux).
hostname:	Пошук за частиною або повним доменним ім’ям.
title:	Пошук за HTML-заголовком відповіді веб-інтерфейсу (наприклад, title:"Smart Home").
before: / after:	Фільтр за датою виявлення пристрою.
has_screenshot:true	Пошук пристроїв, для яких доступний попередній перегляд веб-інтерфейсу.

Комбінація вищенаведених операторів дозволяє побудувати комплексну стратегію дослідження вразливостей. Зокрема, шляхом поєднання фільтрів *has_vuln:true, port*:, *country:* та *device:* можливо виявити не лише окремі пристрої, але й зіставити їх із відомими вразливостями, що становлять загрозу для цілісності, конфіденційності та доступності даних у середовищі розумного міста.

У процесі дослідження планується використати цілеспрямовану комбінацію запитів, спрямованих на охоплення ключових компонентів інфраструктури розумного міста:

- Пристрої відеоспостереження (webcam), які критично важливі для безпеки та моніторингу.
- Мережеве обладнання, зокрема MikroTik, яке використовується як у побутовому, так і в муніципальному сегменті.
- Пристрої, вебінтерфейс яких містить ознаку «smart», що може свідчити про централізовані платформи або рішення з інтерфейсом управління.

Запити будуватимуться із врахуванням таких фільтрів як: *has_vuln:true* (фільтр, який обмежує вибірку лише пристроями, для яких вже знайдено відомі вразливості у CVE-базі) та *country:UA* (фільтр географічної прив'язки до України, що дозволяє оцінити стан кібербезпеки локальної інфраструктури).

Відповідно до вимог до цільових пристроїв, що були сформовані у пункті 3.2.1, було підібрано та здійснено запити з урахуванням конкретної цілі: виявити найбільш поширені типи пристроїв, які є складовими розумної інфраструктури та потенційно вразливі з точки зору кібербезпеки. Далі наведено опис та обґрунтування кожного запиту, що використовувався у рамках дослідження.

3.2.2 Пошук вразливих пристроїв відеоспостереження

У рамках практичного етапу дослідження було проведено аналіз пристроїв відеоспостереження з підтвердженими вразливостями на території України. Застосовуючи запит *webcam has_vuln:true country:UA* у пошуковій системі Shodan, було отримано вибірку мережевих пристроїв, які ідентифікуються як камери відеоспостереження та мають зареєстровані вразливості у CVE-базі.

Було ідентифіковано декілька пристроїв типу IP-відеокамер, розміщених в Україні, з відкритим мережевим доступом через Shodan. Розглянемо один з таких пристроїв.

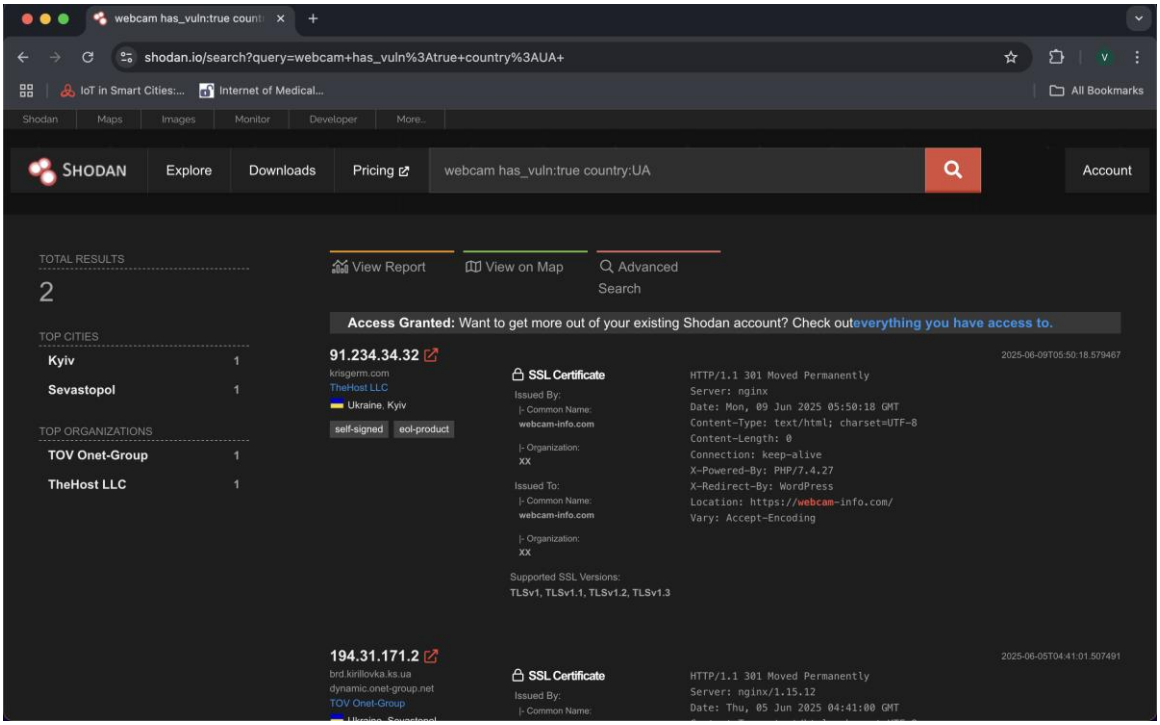


Рисунок 3.1 – Результати пошуку за запитом «webcam has_vuln:true country:UA»

На основі даних з Shodan, пристрій представляє собою мережеву IP-камеру з доступними інтерфейсами на портах 21 (Telnet), 80 та 8080 (HTTP/адмін-панелі).

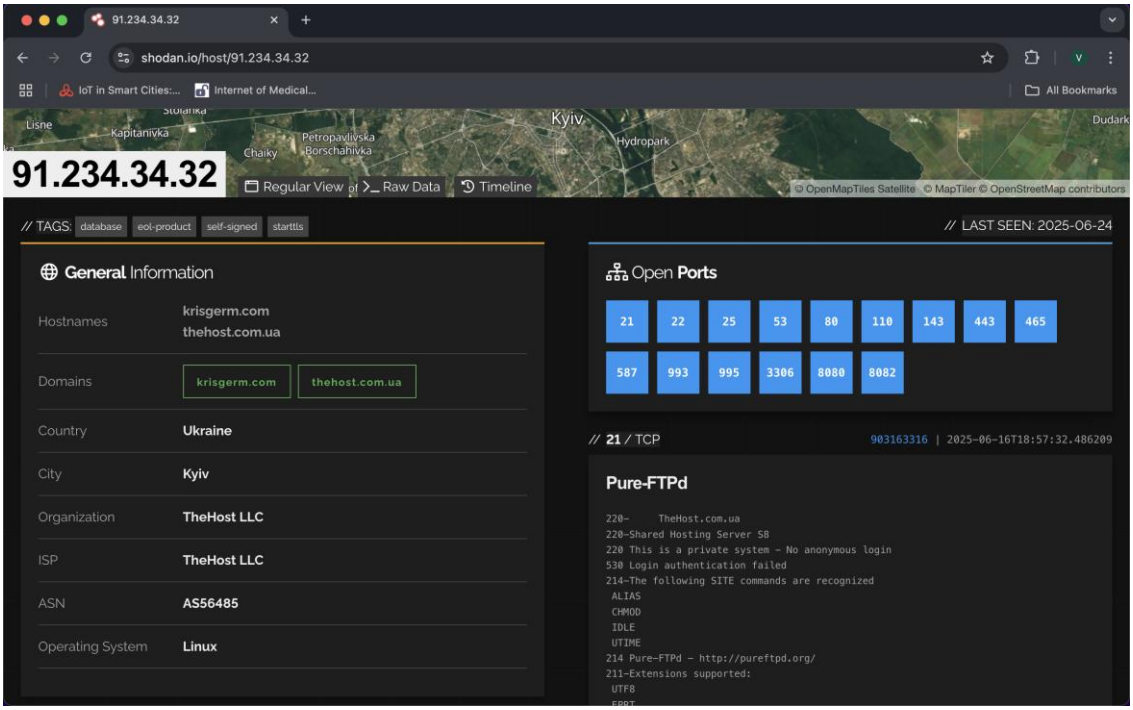


Рисунок 3.2 – Пристрій відеоспостереження з вразливістю

Відкритість порту Telnet (21) свідчить про наявність одного з найбільш вразливих протоколів, оскільки він забезпечує текстовий, нешифрований доступ до системи, що може використовуватися для атаки типу «brute force» або захоплення сесії. Порти HTTP-інтерфейсів є типовими для адміністративного доступу до пристроїв і можуть свідчити про відсутність захищеної авторизації або шифрування.

У процесі аналізу були виявлені численні уразливості, зокрема такі, що мають високу критичність з точки зору потенційного використання зловмисниками. Найбільш значущими є:

- CVE-2024-25117 (CVSS: 6.8): уразливість у бібліотеці php-svg-lib, що дозволяє виконання довільного коду (RCE) через використання спеціально сформованого параметра font-family. Уразливість може бути використана для компрометації серверного середовища, особливо в конфігураціях із PHP < 8.0.
- CVE-2023-21980 (CVSS: 7.1): уразливість у клієнтських програмах MySQL, яка за певних умов дозволяє зловмиснику отримати повний контроль над сервером MySQL. Потенційно це дає змогу змінювати, зчитувати або знищувати дані, а також запускати довільний код у контексті сервера.
- CVE-2022-31626 (CVSS: 7.5): уразливість у розширенні pdo_mysql для PHP, яка дозволяє здійснити буферне переповнення під час обробки пароля надмірної довжини, що може призвести до віддаленого виконання коду.
- CVE-2022-37454 (CVSS: 9.8): критична уразливість у реалізації SHA-3, яка дозволяє переповнення буфера, що потенційно призводить до повного обходу криптографічного захисту або запуску довільного коду.
- CVE-2021-21708 (CVSS: 8.2): уразливість у PHP-функції фільтрації, що дозволяє використання пам’яті після її звільнення (use-after-free). Це може призвести до збоїв, витоків даних або виконання довільного коду на сервері.

Наявність цих вразливостей свідчить про системне недотримання політик оновлення та відсутність належного контролю конфігурацій пристрою. Уразливості, пов’язані з PHP та MySQL, є типовими для веб-інтерфейсів відеоспостереження, в яких часто використовуються стандартні CMS або самописні панелі адміністрування.

У результаті, зловмисник може: отримати повний контроль над пристроєм або вебінтерфейсом керування, здійснити несанкціонований доступ до відеопотоку, використовувати пристрій як точку входу до внутрішньої мережі, встановити зловмисне ПЗ або включити пристрій до ботнет-мережі, таким чином, аналіз даного кейсу підтверджує високий рівень ризику при відсутності належного захисту мережевих камер.

Виявлені уразливості мають не лише локальний, а й системний характер, що робить такі пристрої потенційною ціллю для кібератак, коли звичайна IP-камера, залишена без належного захисту, може стати значною загрозою для безпеки цифрового середовища як у межах Smart Home, так і в архітектурі Smart City.

3.2.3 Пошук вразливих пристроїв мережевого обладнання

У межах практичного дослідження було проаналізовано потенційно вразливі мережеві пристрої, зокрема маршрутизатори MikroTik, які активно використовуються в інфраструктурі як «розумних будинків», так і муніципальних мереж.

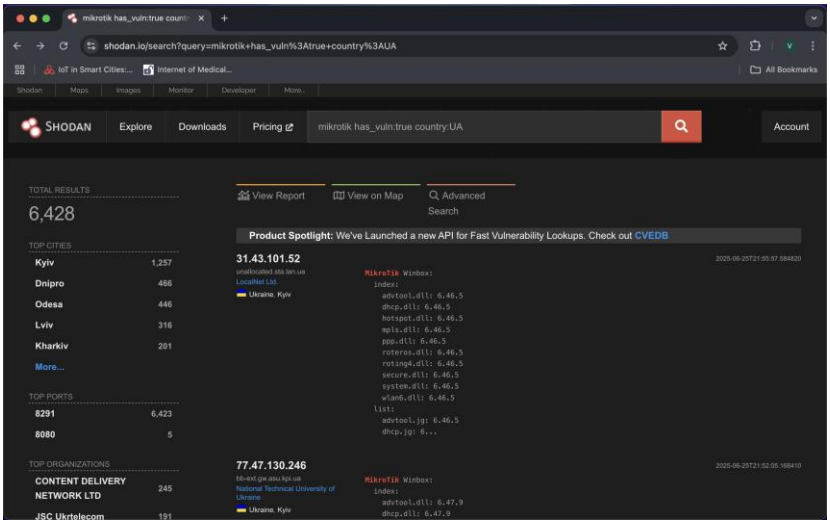


Рисунок 3.3 – Результати пошуку за запитом «mikrotik has_vuln:true country:UA»

Для цього було застосовано пошуковий запит *mikrotik has_vuln:true country:UA,* що дозволив локалізувати пристрої даного виробника з підтвердженими вразливостями в межах України.

Серед отриманих результатів для поглибленого аналізу було обрано пристрій із RouterOS версії 6.46.5, розгорнутий в одній із локальних мереж провайдера. Аналіз виконано на основі метаданих, наданих системою Shodan.

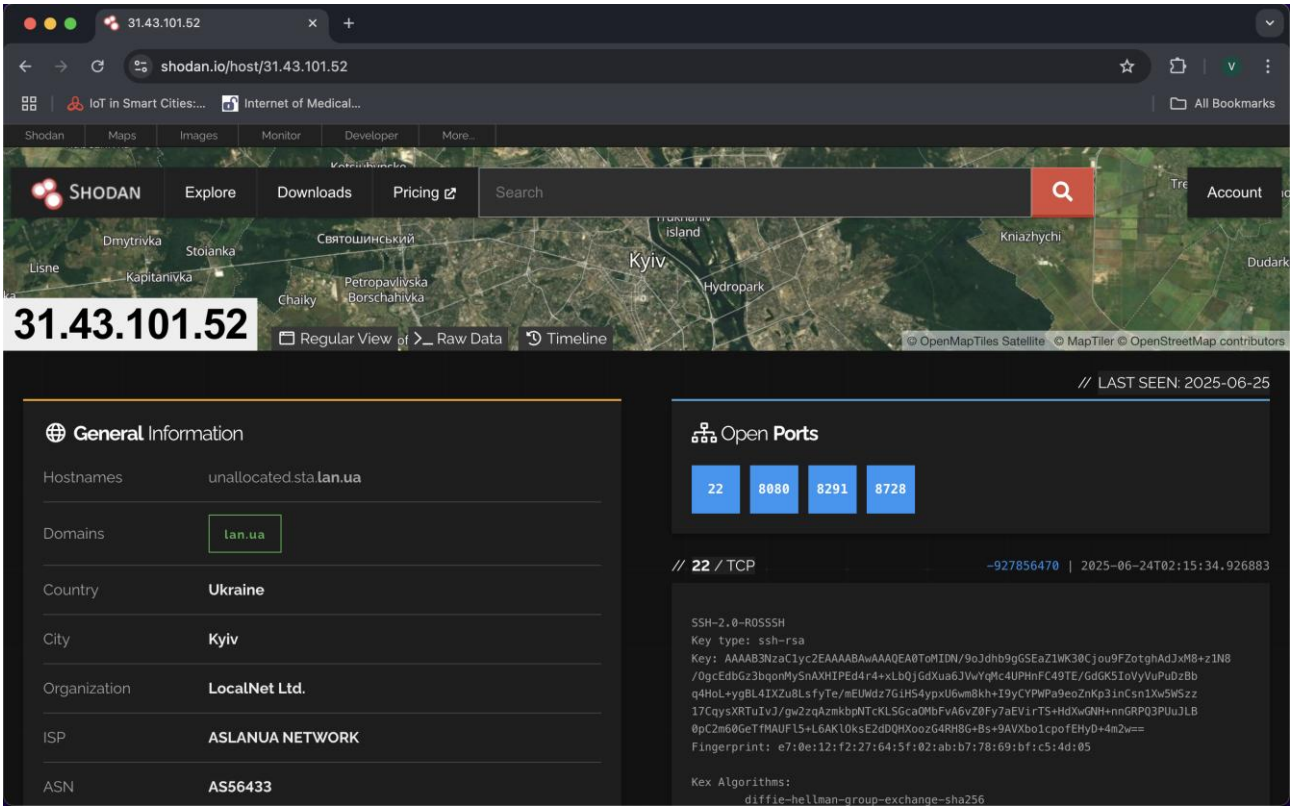


Рисунок 3.4 – Ідентифікований MikroTik RouterOS з відкритими портами

Згідно з даними, пристрій має відкриті порти: 22, 8080, 8291, 8728. Це свідчить про те, що пристрій або не має обмежень на підключення, або сконфігурований з використанням небезпечних за замовчуванням налаштувань.

У процесі аналізу Shodan виявив низку критичних вразливостей, характерних для саме цієї версії RouterOS. Найбільш небезпечні з них:

•CVE-2023-30799 (CVSS: 9.1): дозволяє зловмиснику з правами адміністратора підвищити привілеї до рівня супер-адміністратора через інтерфейс Winbox або HTTP. Як результат — можливість виконання довільного коду на маршрутизаторі.

•CVE-2023-30800 (CVSS: 7.5): вразливість, що дозволяє віддаленому користувачу призвести до аварійного завершення роботи вебінтерфейсу за

допомогою спеціально сформованого HTTP-запиту. Може використовуватись для DoS-атак.

•CVE-2022-45315 (CVSS: 9.8): поза межами читання у процесі SNMP, що дозволяє віддалене виконання довільного коду.

•CVE-2020-11881 (CVSS: 7.5): вразливість SMB-сервера, яка дозволяє віддаленому неавторизованому користувачу спровокувати крах системи шляхом надсилання модифікованих запитів.

Ці уразливості мають широкий спектр можливих наслідків: повний контроль над пристроєм (отримавши суперкористувацький доступ, зловмисник може повністю модифікувати конфігурацію, відключити маршрутизацію або змінити правила брандмауера), масове підключення до ботнету, шпигування за трафіком, дестабілізація локальної інфраструктури

Таким чином, аналіз даного пристрою MikroTik демонструє реальні та високоризикові вразливості, які можуть бути використані для атак на інфраструктурному рівні.

У контексті Smart City/Smart Home, компрометація маршрутизатора не лише відкриває шлях до інших IoT-пристроїв, але й створює серйозну загрозу функціональності та безпеці всієї цифрової екосистеми.

3.2.4 Пошук вразливих “smart” пристроїв

У рамках реалізації пошукового запиту *title:"smart" has_vuln:true country:UA* у Shodan було виявлено пристрої, вебінтерфейс яких ідентифікується як частина «розумної» інфраструктури, а саме інтерфейси з назвою "Smart Wi-Fi". Такий підхід дозволяє виявити панелі керування або шлюзи, пов’язані з інтегрованими системами у сфері Smart Home або Smart City.

Серед отриманих результатів було обрано один пристрій, розміщений на території України. Згідно з Shodan, ідентифікований пристрій працює під брендом Linksys Smart Wi-Fi.

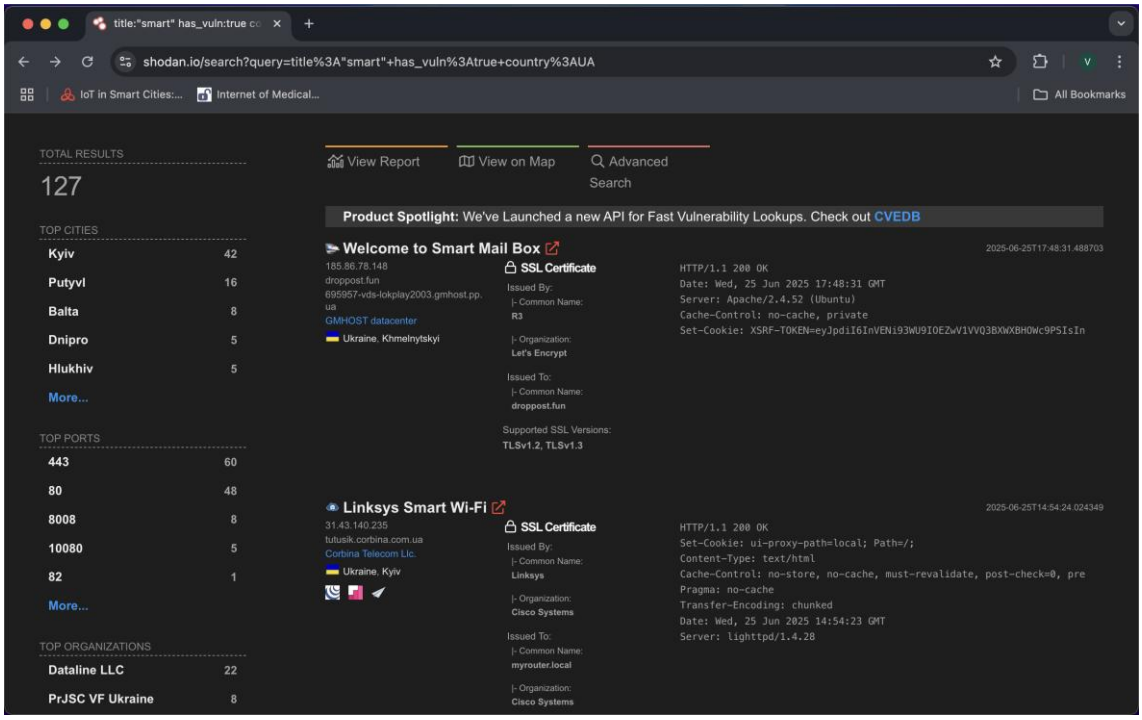


Рисунок 3.5 – Результати пошуку за запитом «title:"smart" has_vuln:true country:UA»

Відкриті порти TCP (443, 10080, 49152) свідчать про доступність адміністративного інтерфейсу ззовні.

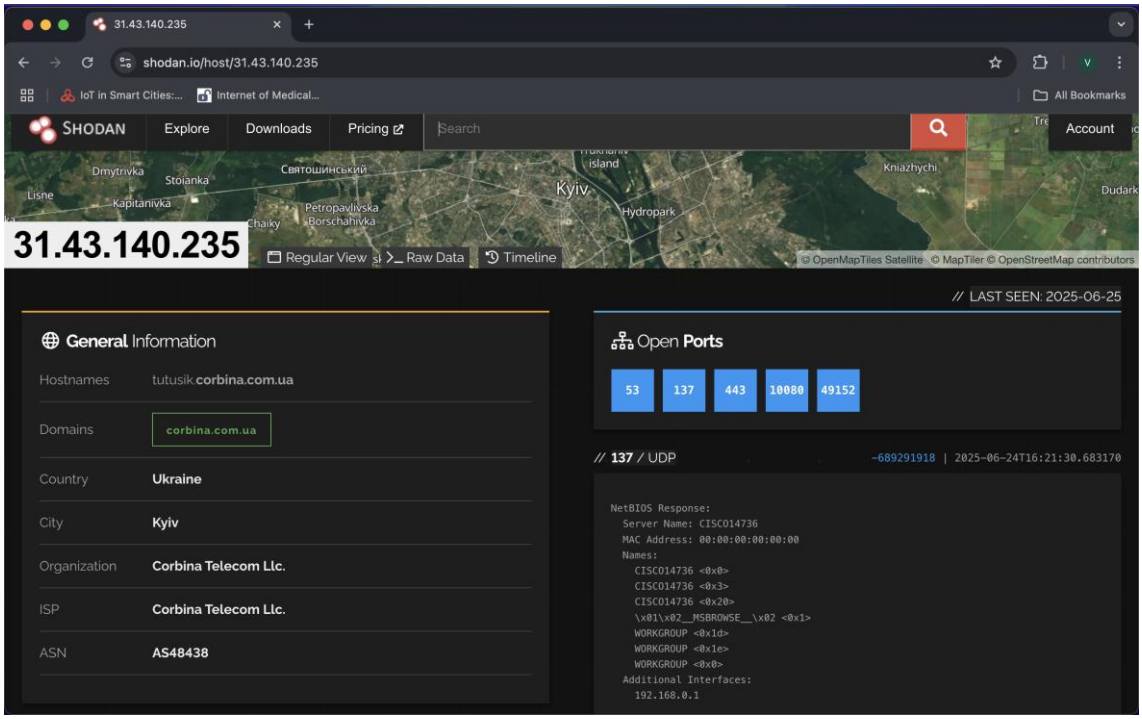


Рисунок 3.6 – Вебінтерфейс Linksys Smart Wi-Fi з вразливістю

Вебінтерфейс надає доступ до функціоналу управління маршрутизатором або шлюзом, що інтегрований до інфраструктури розумного будинку.

Найбільш небезпечні вразливості, пов’язані з цим пристроєм:

- CVE-2019-11072 (CVSS: 9.8): вразливість у lighttpd до версії 1.4.54 дозволяє відмову в обслуговуванні або виконання небажаних дій через маніпуляцію HTTP GET-запитами. Це відкриває шлях до дестабілізації роботи системи або використання ресурсу у ботнетах.
- CVE-2018-19052 (CVSS: 7.5): дозволяє обхід прав доступу через path traversal (../), що може дати змогу зловмиснику отримати доступ до файлів поза межами призначених директорій.
- CVE-2014-2323 (CVSS: 9.8): критична SQL-ін’єкція у модулі mod_mysql_vhost дозволяє виконання довільних SQL-команд через некоректну перевірку вмісту заголовка Host. Це створює потенційну загрозу для повного компрометування системи.
- CVE-2015-3200 (CVSS: 7.5): дає змогу ін’єкції логів через Basic HTTP автентифікацію, що може призвести до витоку журналів, включно з авторизаційною інформацією.
- CVE-2013-4559 (CVSS: 7.6): дає змогу підвищення привілеїв через неправильну обробку системних викликів setuid/setgid у lighttpd, що може дозволити запуск сервера з правами root.

Ці вразливості вказують на те, що пристрій використовує застарілу версію вебсервера та потенційно ненадійні механізми автентифікації, а отже, може бути використаний як точка входу в домашню або міську мережу. Зловмисник має змогу отримати повний доступ до конфігурації пристрою, здійснити несанкціоноване адміністрування, змінити маршрутизацію трафіку, а також перехоплювати або підмінювати дані, що передаються.

Таким чином, дослідження цього кейсу підтверджує важливість своєчасного оновлення прошивок та вебінтерфейсів у середовищах з розумними пристроями, а також демонструє ризики, які несе застаріле або неправильно сконфігуроване мережеве обладнання в архітектурі Smart Home.

3.3 Усунення вразливостей на основі рекомендацій NIST SP 800-53

Проведений практичний аудит пристроїв на базі Shodan показав, що низка IoT-компонентів, задіяних у середовищах Smart Home / Smart City, мають серйозні вразливості, які можуть бути використані для компрометації систем.

Для ефективного реагування використано підхід, заснований на рекомендаціях NIST SP 800-53, які описують вимоги до безпеки IT-систем.

3.3.1 Усунення вразливостей IP-камери

У процесі практичного аналізу було виявлено IP-камеру, яка функціонує з низкою серйозних порушень вимог до інформаційної безпеки. Серед основних проблем — активні відкриті порти 21 (Telnet), 80 та 8080 (HTTP), що дозволяє зловмисникам отримати доступ до адміністративного інтерфейсу пристрою без автентифікації або шифрування.

Додатково ідентифіковано низку критичних вразливостей, зокрема у компонентах PHP, MySQL та реалізації SHA-3, які відкривають можливості для віддаленого виконання коду (RCE), компрометації автентифікаційних даних і повного захоплення контролю над пристроєм.

Для впорядкування заходів з усунення таких вразливостей та приведення конфігурації до відповідності загальноприйнятим стандартам інформаційної безпеки, нижче подано узагальнену таблицю дій згідно з фреймворком NIST SP 800-53.

Запровадження перелічених заходів дозволить зменшити ризики експлуатації вразливостей IP-камер, захистити доступ до системи керування відеоспостереженням та унеможливити використання таких пристроїв як шлюзів до внутрішньої інфраструктури.

У контексті Smart City це набуває особливої актуальності, враховуючи залежність від стабільного функціонування розподілених відеоаналітичних систем.

Таблиця 3.2 – Рекомендовані заходи для усунення вразливостей IP-камери згідно з NIST SP 800-53

Напрямок безпеки	Рекомендовані заходи	Відповідність NIST SP 800-53
Шифрування каналів управління	Використання HTTPS з SSL-сертифікатом замість HTTP/Telnet	SC-12 (Cryptographic Key Establishment), SC-13 (Cryptographic Protection)
Вимкнення небезпечних сервісів	Деактивація Telnet; впровадження доступу через SSH з IP-фільтрацією	AC-17 (Remote Access), AC-4 (Information Flow Enforcement)
Оновлення прошивки та ПЗ	Впровадження оновлень для усунення CVE-2024-25117, CVE-2023-21980, тощо	SI-2 (Flaw Remediation), CM-6 (Configuration Settings)
Захист облікових даних	Зміна стандартних логінів і паролів, впровадження 2FA	IA-2 (Identification and Authentication), AC-2 (Account Management)
Аудит доступу та логування	Увімкнення логування доступу до панелі, зберігання логів на окремому сервері, інтеграція з SIEM	AU-2 (Audit Events), AU-12 (Audit Generation)

3.3.2 Усунення вразливостей маршрутизатора MikroTik

У ході практичного дослідження було ідентифіковано маршрутизатор MikroTik під керуванням RouterOS 6.46.5 із відкритими портами 22 (SSH), 8080 (HTTP), 8291 (Winbox) та 8728 (API).

Для зменшення ризику компрометації маршрутизатора пропонуються такі заходи:

Таблиця 3.3 – Рекомендовані заходи для усунення вразливостей MikroTik згідно з NIST SP 800-53

Напрямок безпеки	Рекомендовані заходи	Відповідність NIST SP 800-53
Обмеження мережевого доступу	Обмеження доступу до портів 8080, 8291, 8728 за допомогою фаєрволів та whitelist	AC-4 (Information Flow Enforcement), SC-7 (Boundary Protection)
Оновлення RouterOS	Оновлення прошивки до актуальної стабільної версії, що усуває зазначені CVE	SI-2 (Flaw Remediation), CM-6 (Configuration Settings)
Зміцнення автентифікації	Вимкнення стандартних облікових записів, впровадження SSH-ключів та складних паролів	IA-2 (User Identification and Authentication), IA-5 (Authenticator Management)
Журналювання та аудит	Активізація логування подій Winbox/API, моніторинг змін конфігурації	AU-6 (Audit Review, Analysis, and Reporting), AU-12 (Audit Generation)
Мінімізація доступних служб	Вимкнення непотрібних служб (наприклад, SMB) та обмеження SNMP лише на локальний інтерфейс	CM-7 (Least Functionality), AC-18 (Wireless Access)

Застосування наведених заходів дозволяє значно знизити ризик експлуатації маршрутизаторів MikroTik як інструменту для атак на інфраструктуру. Це критично важливо у розрізі захисту цифрових платформ, що використовуються у контексті Smart City / Smart Home.

3.3.3 Усунення вразливостей Smart Wi-Fi

У третьому прикладі було виявлено пристрій Linksys Smart Wi-Fi із застарілою версією вебсервера lighttpd, що супроводжувався низкою критичних вразливостей, включно з SQL-ін’єкцією, обходом автентифікації та можливістю запуску серверу з правами root.

Відкриті порти (443, 10080, 49152) дозволяли прямий зовнішній доступ до адміністративного інтерфейсу.

Таблиця 3.3 – Рекомендовані заходи для усунення вразливостей інтерфейсу Smart Wi-Fi згідно з NIST SP 800-53

Напрямок безпеки	Рекомендовані заходи	Відповідність NIST SP 800-53
Оновлення вебсервера	Перехід на актуальну версію lighttpd із виправленням критичних модулів	SI-2: Flaw Remediation; CM-2: Baseline Configuration
Контроль доступу	Обмеження доступу ззовні через VPN, впровадження HTTPS	IA-2: Identification and Authentication; SC-12: Cryptographic Key Establishment
Захист від атак	Інтеграція WAF, захист від SQL-ін’єкцій, path traversal	SI-10: Information Input Validation; SC-34: System Generated Alerts
Моніторинг та IDS	Виявлення вторгнень, аналіз логів доступу та конфігурацій	SI-4: System Monitoring; AU-6: Audit Review
Зміцнення автентифікації	Вимкнення HTTP Basic, впровадження MFA	IA-2: Identification and Authentication; AC-2: Account Management

Для підвищення стійкості таких пристроїв до кіберзагроз та уніфікації заходів безпеки відповідно до міжнародних стандартів, нижче подано таблицю з ключовими діями відповідно до NIST SP 800-53.

Запропоновані заходи дозволяють не лише нівелювати конкретні технічні вразливості, але й формують стійку систему інформаційної безпеки на рівні IoT-пристроїв, маршрутизаторів та хостів Smart City / Smart Home.

3.4 Оцінка результатів і роль стандартів безпеки

Результати практичного дослідження підтвердили високий рівень реальної загрози, пов’язаної з публічно доступними IoT-пристроями в Україні. У межах сформованої стратегії пошуку було виявлено численні пристрої з критичними вразливостями: від IP-камер до маршрутизаторів і панелей керування. Кожен із протестованих кейсів демонструє типовий сценарій порушення конфіденційності, цілісності та доступності в екосистемах Smart City / Smart Home.

Наявність відкритих портів, використання застарілих протоколів, відсутність оновлень, ненадійна автентифікація є наслідком недотримання навіть базових практик інформаційної безпеки.

Як показало дослідження, така ситуація не є поодинокою, а має системний характер, що лише підсилює важливість запровадження стандартизованих механізмів управління ризиками.

У цьому контексті фреймворк NIST SP 800-53 відіграв центральну роль. Його застосування дозволило:

- Структурувати виявлені загрози за категоріями контролів, що дало змогу уникнути фрагментарного реагування й забезпечити комплексний підхід до захисту.
- Ідентифікувати недоліки у конфігураціях пристроїв як з точки зору технічної реалізації (відсутність шифрування, відкриті сервіси), так і з позиції організаційної політики (відсутність аудиту, неактуальні прошивки).

- Побудувати карту відповідності дій конкретним вимогам, рекомендованим у стандартах безпеки (зокрема в напрямках контролю доступу, автентифікації, шифрування, журналювання, обмеження функціоналу).

Крім того, впровадження таблиць відповідності дозволило узагальнити рекомендації, зробити їх адаптованими для подальшої практичної реалізації: як для фахівців з безпеки, так і для адміністративного персоналу, відповідального за експлуатацію IoT-систем.

Слід окремо відзначити, що NIST SP 800-53 є не лише нормативною базою, але й практичним інструментом для оцінки стану безпеки в середовищі, де за замовчуванням присутня підвищена складність, динаміка змін і високий ступінь підключення пристроїв.

Саме його модульна структура дозволяє масштабувати політики захисту. Таким чином, обрана стратегія дослідження та використання фреймворку NIST SP 800-53: підтвердили наявність критичних вразливостей у публічно доступних пристроях, дозволили класифікувати та обґрунтувати ризики, сформували цілісну методику рекомендацій з практичним потенціалом для застосування та продемонстрували реальну ефективність міжнародних стандартів у контексті локальних кіберзагроз.

Загалом, запропонований підхід може бути адаптований як основа для впровадження політик кібергігієни на рівні регіональних цифрових інфраструктур.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Забезпечення безпеки життєдіяльності у розумних містах

У сучасних умовах стрімкого розвитку міст і впровадження інноваційних технологій питання безпеки життєдіяльності набуває нового змісту. Розумні міста (smart cities) — це складні соціотехнічні системи, що поєднують класичні інфраструктурні рішення з інформаційно-комунікаційними технологіями, цифровими сервісами й автоматизованими системами управління. Їх головна мета — підвищення якості життя мешканців, ефективності міського господарства, екологічної стійкості й, безумовно, безпеки. [25]

Забезпечення безпеки життєдіяльності у розумному місті передбачає інтеграцію різних підсистем: цифрового моніторингу, автоматизованого оповіщення про надзвичайні ситуації, систем відеоспостереження, аналізу даних про трафік, екологічного стану, рівень шуму, забруднення повітря, стану інженерних мереж. Усі ці дані збираються за допомогою сенсорів та передаються у єдиний центр управління, де в режимі реального часу обробляються і аналізуються. Завдяки цьому міські служби можуть миттєво реагувати на надзвичайні події, аварії, пожежі, техногенні катастрофи, а також запобігати їм на основі прогнозування ризиків.[22]

Інтеграція систем відеоаналітики, автоматичного розпізнавання номерів, облич, а також інтелектуальних сигналізацій дозволяє підвищити рівень громадської безпеки, зменшити час реагування поліції, швидкої допомоги, рятувальних служб. Важливим чинником є й інформаційна безпека — захист критичних даних міста від несанкціонованого доступу, кібератак, втрати чи викривлення інформації.[22]

Особливу увагу в розумних містах приділяють адаптації інфраструктури до потреб людей з обмеженими можливостями, впровадженню безбар’єрного середовища, організації безпечного руху транспорту і пішоходів, оптимізації маршрутів екстрених служб. Завдяки впровадженню інноваційних технологій

міста стають не лише комфортнішими, а й безпечнішими для всіх учасників міського життя.[23]

Водночас, розвиток розумних міст висуває нові вимоги до підготовки фахівців з безпеки життєдіяльності та охорони праці. Вони мають володіти знаннями не лише у сфері класичних нормативів, але й в питаннях кібербезпеки, аналізу великих даних, організації комплексних систем моніторингу й реагування на загрози. Безперервне навчання, підвищення кваліфікації та адаптація до нових технологічних інструментів стають невід'ємною частиною професійної діяльності таких фахівців.[24]

Отже, безпека життєдіяльності у розумних містах — це результат системної роботи із впровадження сучасних технологій, організації ефективної взаємодії між службами, постійного моніторингу ризиків та розвитку культури безпеки серед населення.

4.2 Вплив кольору на покращення умов праці та підвищення продуктивності роботи

Оформлення виробничого середовища, зокрема колірне рішення інтер'єрів, має суттєвий вплив на фізіологічний стан працівників, їхню працездатність, емоційний фон та продуктивність праці. Наукові дослідження у сфері ергономіки і психології праці доводять, що правильний підбір кольорів і освітлення у робочих приміщеннях здатен не лише покращити самопочуття співробітників, а й знизити рівень стресу, втоми, сприяти креативності та командній взаємодії [23].

Колір впливає на людину багатогранно: через фізіологічні та психічні процеси, емоційні стани, динаміку працездатності. Наприклад, теплі кольори (жовтий, оранжевий, червоний) стимулюють діяльність нервової системи, підвищують увагу і активність, сприяють короткотривалому підвищенню продуктивності. Холодні кольори (синій, блакитний, зелений) навпаки, заспокоюють, знижують напругу, полегшують втому очей і сприяють зосередженню при виконанні монотонної роботи. Яскраві, насичені відтінки

можуть підвищувати настрій і стимулювати роботу аналізаторів, тоді як темні, малонасичені — викликати пригніченість, знижувати мотивацію [26].

Практичне застосування кольору у виробничих приміщеннях має свої особливості. Наприклад, для робіт з високим фізичним чи нервовим навантаженням доцільно використовувати світлі відтінки холодних кольорів (блакитний, зелений), які сприяють зниженню стомлюваності. Якщо ж діяльність передбачає креативний підхід, мозкові штурми, розв'язання складних завдань, у приміщеннях рекомендують застосовувати теплі відтінки жовтого чи оранжевого, які стимулюють мозкову активність і творчість. Для зон відпочинку та релаксації доцільно використовувати нейтральні або пастельні кольори, що допомагають швидко відновлювати сили [23].

Крім кольору стін, важливу роль відіграє і колір освітлення. Світлодіодні системи дозволяють регулювати температуру світла: холодне світло підвищує концентрацію, тепле — створює атмосферу затишку. Робочі місця з оптимальним поєднанням природного й штучного освітлення, кольорової гами інтер'єру та ергономічного розташування меблів сприяють зниженню кількості помилок, підвищенню продуктивності й зменшенню рівня професійного вигорання [26].

Відповідно до стандартів з охорони праці, вибір кольорів для виробничих приміщень має бути обґрунтований не лише естетичними, а й санітарно-гігієнічними вимогами. Кольори використовують також для інформації та сигналізації: червоний — для позначення небезпеки, жовтий — для попередження, зелений — для безпечних зон, синій — для інформації. Раціональне поєднання кольорів, світла, озеленення та музики створює сприятливе середовище для ефективної роботи і підтримки психоемоційного балансу співробітників [26].

Таким чином, грамотне використання кольору в організації праці є одним із простих і дієвих засобів підвищення продуктивності, профілактики втоми і збереження психічного здоров'я персоналу.

ВИСНОВКИ

У роботі було проведено комплексне дослідження стандартів захисту даних у цифровій інфраструктурі розумного міста (Smart City) та здійснено аналіз їх практичного впровадження в умовах сучасних кіберзагроз. Отримані результати підтверджують важливість системного підходу до управління інформаційною безпекою в міських інформаційно-комунікаційних системах.

У першому розділі досліджено архітектуру Smart City, її компоненти та основні вектори інформаційних загроз. Проаналізовано роль Інтернету речей (IoT), мереж LPWAN, а також критичні точки у взаємодії міських служб і сервісів. Розглянуто приклади впровадження стандартів у містах Барселона, Торонто та Таллінн, що підтвердили ефективність формалізованого підходу до захисту даних у міському масштабі. Обґрунтовано потребу у впровадженні чітких стандартів безпеки, враховуючи розподіленість і відкритість інфраструктури розумного міста.

Другий розділ присвячено аналізу міжнародних стандартів, таких як ISO/IEC 27001, ISO/IEC 27701, NIST SP 800-53 та європейського регламенту GDPR. Визначено ключові вимоги до побудови систем управління інформаційною безпекою (ISMS) та управління персональними даними (PIMS).

У третьому розділі проведено аналіз вразливостей завдяки сервісу Shodan для виявлення відкритих портів і вразливих IoT-пристроїв в межах міської інфраструктури. Здійснено пошук за ключовими протоколами (HTTP, FTP, Telnet), отримано результати щодо ступеня відкритості систем у публічному доступі. На основі зібраних даних сформульовано рекомендації щодо підвищення безпеки, зокрема впровадження багаторівневого контролю доступу, шифрування трафіку, сегментації мережі та постійного моніторингу IoT-систем.

Результати дослідження свідчать про актуальність і практичну цінність застосування міжнародних стандартів у розвитку кіберзахисту розумних міст. Запропоновані заходи можуть бути використані як базова модель безпеки для українських Smart City-проєктів.

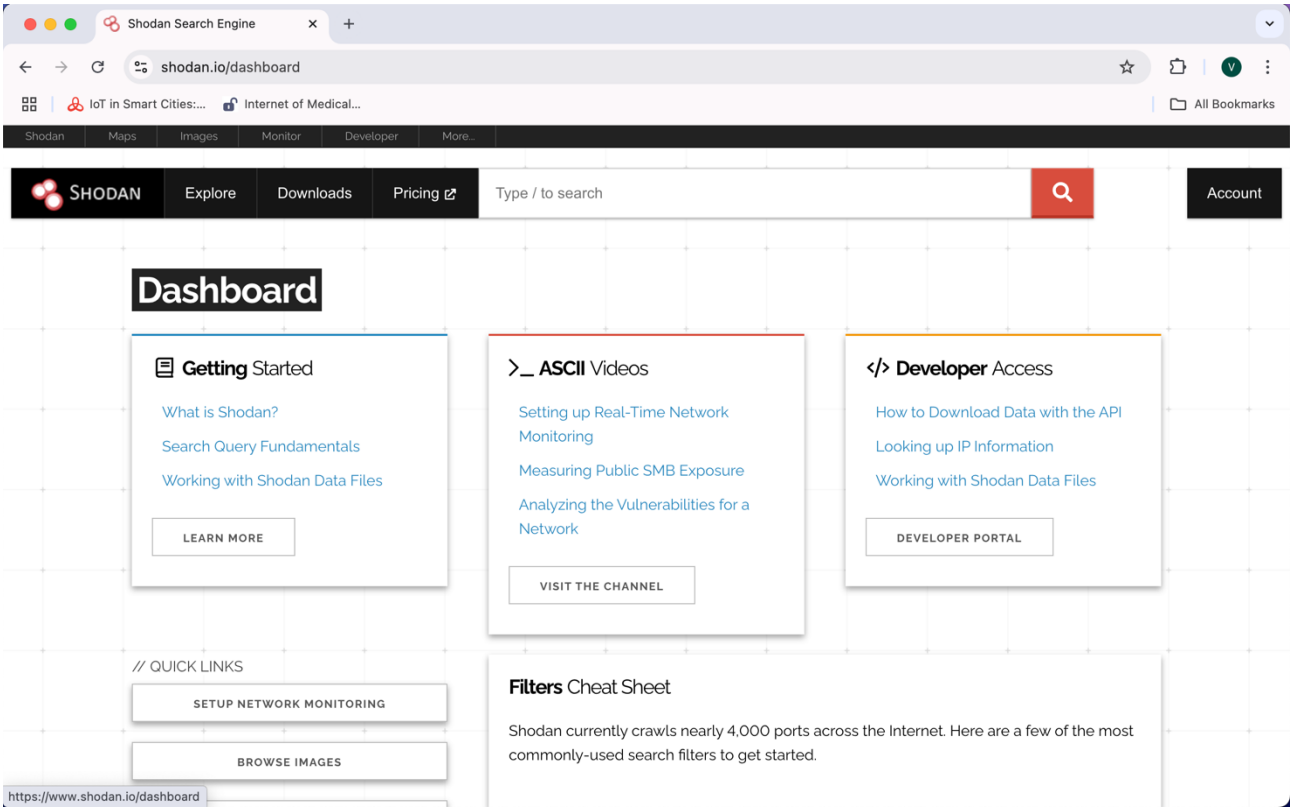
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., ... & Portugali, Y. (2012). Smart cities of the future. *The European Physical Journal Special Topics, 214*(1), 481–518. https://deps.ua/ua/knowegable-base/reference-information/67697.html
2. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things Journal, 1*(1), 22–32. https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-ukr.pdf
3. Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., ... & Scholl, H. J. (2012). Understanding smart cities: An integrative framework. *45th Hawaii International Conference on System Sciences*, 2289–2297. https://ndc-ipr.org/media/posts/presentations/0117U007020.pdf
4. Shpak, O., Fedor'ka, P., & Prygara, M. (2023). Smart cities and Internet of Things: Impact of IT developments on city development and quality of life improvement. *Innovative Technologies and Scientific Solutions for Industries*, (3), 114–123. https://journals.uran.ua/itssi/article/download/290907/284520
5. Bazan, I., & Koval, A. (2023). Detecting cyberattacks in a smart city based on machine learning. *Ternopil National Technical University*. https://elartu.tntu.edu.ua/bitstream/lib/44275/2/IMSTT_2023_Bazan_I-Detecting_cyberattacks_in_a_smart_16.pdf
6. Кривець, Д. (2024). Дослідження шляхів та розробка рекомендацій щодо забезпечення безпеки інформаційного середовища Smart City [Кваліфікаційна робота]. https://duikt.edu.ua/repozitorii/ikb/2024/bak/%D0%9A%D1%80%D0%B8%D0%B2%D0%B5%D1%86%D1%8C_%D0%91%D0%A1%D0%94-43.pdf
7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. https://www.iso.org/standard/82875.html

8. ISO/IEC 27701:2019. Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines. https://www.iso.org/standard/71670.html
9. NIST Special Publication 800-53 Rev. 5. (2020). Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
10. ENISA. (2019). Data Protection Engineering in Smart Cities. https://www.enisa.europa.eu/publications/data-protection-engineering-in-smart-cities
11. Barcelona City Council. (2021). Barcelona Smart City Strategy. https://ajuntament.barcelona.cat/digital/en/smart-city
12. Waterfront Toronto. (2020). Quayside: Sidewalk Toronto Project. https://waterfrontoronto.ca/nbe/portal/wt/home
13. City of Tallinn. (2022). Tallinn Smart City Initiatives. https://www.tallinn.ee/en/smartcity
14. ENISA. (2022). Smart Cities: Security and Resilience for Urban Infrastructures. https://www.enisa.europa.eu/publications/smart-cities-security-and-resilience-for-urban-infrastructures
15. IEC 62443 series. Industrial communication networks – Network and system security. https://webstore.iec.ch/publication/24534
16. ISO/TR 37150:2014. Smart community infrastructures – Review of existing activities relevant to metrics. https://www.iso.org/standard/61768.html
17. Hostragons. (2025). Кібербезпека в розумних містах та екосистемах Інтернету речей.
18. Babakov, R. M., Biloborodova, T. O., Brezhniev, E. V., Bojko, A. O., Bousher, V. V., Bykovyy, P. Y., ... & Waleed, A. A. (2019). Internet of Things for Industry and Human Application. Vol. 3.
19. Sachenko, A. O., Kochan, V. V., Bykovyy, P. Y., Zahorodnia, D. I., Osolinskyy, O. R., Skarga-Bandurova, I. S., ... & Fesenko, H. V. Internet of Things for intelligent transport systems.

20. Mishko, O., Matiuk, D., & Derkach, M. (2024). Security of remote iot system management by integrating firewall configuration into tunneled traffic. Вісник Тернопільського національного технічного університету, 115(3), 122-129.
21. Stanko, A., Wieczorek, W., Mykytyshyn, A., Holotenko, O., & Lechachenko, T. (2024). Realtime air quality management: Integrating IoT and Fog computing for effective urban monitoring. CITI, 2024, 2nd.
22. T. Lechachenko, R. Kozak, Y. Skorenkyy, O. Kramar, O. Karelina. Cybersecurity Aspects of Smart Manufacturing Transition to Industry 5.0 Model. CEUR Workshop Proceedings, 2023, 3628, pp. 325–329
23. Y. Skorenkyy, R. Zolotyy, S. Fedak, O. Kramar, R. Kozak. Digital Twin Implementation in Transition of Smart Manufacturing to Industry 5.0 Practices. CEUR Workshop Proceedings, 2023, 3468, pp. 12–23
24. Palamar, A., Karpinski, M. P., Palamar, M., Osukhivska, H., & Mytnyk, M. (2022, November). Remote Air Pollution Monitoring System Based on Internet of Things. In ITTAP (pp. 194-204).
25. Бурий В. П. Огляд технічних стандартів для розумних міст : кваліфікаційна робота освітнього рівня „Бакалавр“ „122 — комп’ютерні науки“ / В. П. Бурий. — Тернопіль : ТНТУ, 2021. — 43 с. http://elartu.tntu.edu.ua/handle/lib/35783
26. Андрейчук Н.І. Охорона праці. – Львів: Видавництво Львівської політехніки, 2021. https://vlp.com.ua/node/8338
27. Зав’ялова А. Д. Дослідження розумних міст як складних інформаційно-технологічних систем : кваліфікаційна робота освітнього рівня „Магістр“ „122 – комп’ютерні науки“ / А. Д. Зав’ялова. – Тернопіль : ТНТУ, 2023. – 67 с. http://elartu.tntu.edu.ua/handle/lib/43395
28. Безпека життєдіяльності та охорона праці / В.В. Сокуренко, О.М. Бандурка та ін. – Харків: ХНУВС, 2021. https://www.tkfk.te.ua/wp-content/uploads/2024/02/%D0%A1%D0%B0%D0%BA%D1%83%D1%80%D0%B5%D0%BD%D0%BA%D0%BE-%D0%91%D0%96%D0%94.pdf
29. Гогіташвілі Г.Г., Лапін В.М. Основи охорони праці. – Київ: Знання, 2018. https://library.udpu.edu.ua/library_files/409594.pdf

Додаток А. Середовище Shodan



Розділ «Vulnerabilities»