НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«МЕТОДИ ЗАХИСТУ РОЗУМНИХ МІСТ ВІД КІБЕРАТАК»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Редькін Андрій Андрійович

Керівник: д.т.н., професор
Казакова Надія Феліксівна

Рецензент: д.т.н., професор
Соколов Артем Вікторович

Одеса – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____» _____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувача Редькіна Андрія Андрійовича

1. Тема роботи: «Методи захисту розумних міст від кібератак»
Керівник роботи: д.т.н, доцент Казакова Надія Феліксівна
затверджені наказом НУ ОЮА від «18» березня 2025 року № 548-6
2. Строк подання здобувачем роботи «19» травня 2025 року
3. Дата видачі завдання «16» вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1.	Отримання та узгодження завдання на кваліфікаційну роботу	Вересень-жовтень 2024	
2.	Збір та аналіз інформації, огляд літературних джерел	Листопад 2024	
3.	Підготовка теоретичної частини роботи (Розділ 1)	Грудень 2024	
4.	Написання розділу 2 (аналіз стану захисту в Україні та м. Одеса)	Січень-лютий 2025	
5.	Формування розділу 3 (авторський підхід, алгоритм реагування, чеклист, симуляція)	Лютий 2025	
6.	Оформлення кваліфікаційної роботи та додатків	Березень 2025	
7.	Захист роботи	11.06.25	

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Методи захисту розумних міст від кібератак» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека. Робота містить 3 рисунки, 5 таблиць, 31 літературне джерело за переліком посилань. Робота виконана на 58 сторінках загального тексту та 49 сторінках основного тексту.

Кваліфікаційна робота присвячена вивченню проблем кібербезпеки в умовах впровадження технологій «розумного міста» (Smart City). Основною метою є аналіз існуючих кіберзагроз, які виникають у цифровій міській інфраструктурі, а також розробка методичного підходу до оцінки готовності та реагування на кіберінциденти в муніципальному середовищі.

У межах роботи проаналізовано архітектуру Smart City, класифіковано основні типи атак на IoT-пристрої, системи відеоспостереження, енергомережі та цифрові сервіси. Проведено порівняльний аналіз стану кіберзахисту в провідних містах України, зокрема приділено увагу місту Одеса. Встановлено зв’язок між динамікою інцидентів та обсягом фінансування заходів ІБ.

Практична частина роботи включає авторський чеклист для оцінки готовності, блок-схему алгоритму реагування, симуляцію інциденту, таблиці ризиків, а також візуалізацію архітектури цифрової інфраструктури. Запропоновані рішення можуть бути застосовані у міських органах самоврядування як частина стратегії безпеки та цифрової трансформації.

СМАРТ-МІСТО, КІБЕРБЕЗПЕКА, ІОТ, МУНІЦИПАЛЬНІ СИСТЕМИ, КІБЕРІНЦИДЕНТ, ЗАХИСТ ІНФРАСТРУКТУРИ, SMART CITY, ІНФОРМАЦІЙНА БЕЗПЕКА, РЕАГУВАННЯ НА ЗАГРОЗИ, ЧЕКЛИСТ, КРИТИЧНА ІНФРАСТРУКТУРА.

ABSTRACT

Qualification work on the topic "Methods of protecting smart cities from cyberattacks" for obtaining the first (bachelor's) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity. The work contains 3 figures, 5 tables, and 31 literary sources according to the list of references. The total volume of the document is 58 pages, including 49 pages of main content.

The thesis is dedicated to the study of cybersecurity issues in the context of implementing Smart City technologies. The main objective is to analyze existing cyber threats arising within digital urban infrastructure and to develop a methodological approach for assessing preparedness and responding to cyber incidents in the municipal environment.

The research examines the architecture of Smart Cities and classifies the main types of attacks on IoT devices, video surveillance systems, power grids, and municipal digital services. A comparative analysis of the cybersecurity status in major Ukrainian cities is provided, with special attention given to the city of Odesa. The study establishes a correlation between the dynamics of cyber incidents and the level of funding allocated to cybersecurity initiatives.

The practical part of the work includes an original checklist for readiness assessment, a response algorithm flowchart, a simulated incident scenario, risk evaluation tables, and a visualization of smart infrastructure architecture. The proposed solutions may be applied by municipal authorities as part of their cybersecurity and digital transformation strategies.

SMART CITY, CYBERSECURITY, IOT, MUNICIPAL SYSTEMS, CYBER INCIDENT, INFRASTRUCTURE PROTECTION, SMART CITY, INFORMATION SECURITY, THREAT RESPONSE, CHECKLIST, CRITICAL INFRASTRUCTURE

ЗМІСТ

ВСТУП

Сучасні міста в усьому світі стикаються з дедалі складнішими викликами: зростанням чисельності населення, збільшенням навантаження на інфраструктуру, потребою в сталому управлінні енергоресурсами, безпеці, екологічності та зручності для мешканців. У відповідь на ці виклики з’явилася концепція розумного міста (Smart City), яка передбачає використання цифрових технологій для оптимізації міського управління та покращення якості життя громадян.

Суть Smart City полягає у зборі, обробці та аналізі великих обсягів даних у режимі реального часу, які надходять від мережі сенсорів, пристроїв Інтернету речей (IoT), камер спостереження, транспортних систем, лічильників, екологічних датчиків тощо. На основі цих даних приймаються рішення – автоматизовано або з участю людини – щодо розподілу ресурсів, сигналізації, управління транспортом, енергопостачанням, охороною здоров’я, громадською безпекою та іншими аспектами функціонування міста.

Значна частина таких рішень реалізується через інтеграцію систем штучного інтелекту, хмарних обчислень, геоінформаційних платформ та мобільних застосунків. Усе це створює високотехнологічне середовище, яке, з одного боку, відкриває нові горизонти в розвитку урбаністики, а з іншого – робить міста вразливими до кіберзагроз.

Кожен цифровий компонент розумного міста може стати об’єктом кібератаки: починаючи з IoT-сенсора, що вимірює рівень забруднення повітря, і закінчуючи центральною базою даних, яка управляє усіма міськими службами. Злами, викрадення даних, маніпуляції з трафіком або навіть фізичне відключення системи – усе це може стати реальністю. Особливу небезпеку становлять скоординовані атаки на критичну інфраструктуру, зокрема на енергетичні системи, водопостачання чи служби екстреного реагування.

Актуальність теми дослідження обумовлена не лише глобальними трендами цифровізації, а й реальними загрозами, з якими вже зіткнулися багато міст по всьому світу. Так, у США, Великій Британії, Ірані, Ізраїлі, Німеччині та Україні

фіксувалися серйозні кібератаки на елементи міської інфраструктури. Зокрема, в Україні відома атака на енергосистеми у 2015 році, внаслідок якої понад 200 тисяч осіб залишилися без світла, а також серії фішингових кампаній та DDoS-атак у воєнний час.

У цьому контексті місто Одеса, як один із найбільших урбаністичних центрів півдня України, не є винятком. У місті поступово впроваджуються елементи смарт-інфраструктури – системи відеоспостереження, розумне освітлення, цифрові сервіси муніципального управління. Проте, як і в багатьох інших містах, кібербезпека таких рішень залишається другорядною, недостатньо розвиненою або фрагментарною. Тому виникає потреба не лише в аналізі наявного стану захисту, а й у розробці адаптованих методик реагування, попередження та усунення кіберзагроз для міської інфраструктури.

Метою цієї роботи є аналіз найбільш поширених кіберзагроз для компонентів розумного міста та розробка ефективних методів і рекомендацій щодо їхнього захисту, з фокусом на практичне застосування в умовах українських міст, зокрема в місті Одеса.

Основні завдання:

– Розкрити поняття та архітектуру розумного міста, зосередивши увагу на інформаційних і технологічних складових.

– Проаналізувати типові кіберзагрози, що виникають у процесі функціонування смарт-інфраструктури.

– Розглянути сучасні технічні, організаційні та нормативні методи захисту міських систем.

– Дослідити поточний стан впровадження Smart-технологій в Україні з прикладами з Одеси.

– Розробити авторський підхід – методику або алгоритм забезпечення кібербезпеки міських систем.

– Оцінити ефективність запропонованого підходу та можливість його реалізації в умовах українських реалій.

Об’єктом дослідження є цифрова інфраструктура розумного міста як складна система, що поєднує технології, сервіси, пристрої та управлінські процеси.

Предметом виступають методи кіберзахисту в умовах функціонування смарт-міст, а також підходи до аналізу загроз і реагування на них.

Методи дослідження:

У роботі застосовано такі методи наукового дослідження:

1) Теоретичний аналіз – для систематизації інформації про структуру Smart City та існуючі загрози;

2) Порівняльний аналіз – для зіставлення різних методів захисту та визначення їхніх переваг і недоліків;

3) Моделювання – для побудови авторського алгоритму реагування на кіберінциденти;

4) Описовий метод – для аналізу практики впровадження Smart City в українських містах.

Структура роботи:

Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків.

У першому розділі розглянуто теоретичні основи побудови розумного міста, типові кіберзагрози та методи захисту. У другому розділі досліджено стан впровадження Smart-технологій в Україні та в місті Одеса, проаналізовано існуючі проблеми й уразливості. Третій розділ присвячено авторській пропозиції – практичній методиці виявлення та реагування на загрози, зокрема з використанням простого програмного інструмента, алгоритмічної схеми дій і чеклиста для служб безпеки міста.

1 ТЕОРЕТИЧНІ ОСНОВИ КІБЕРЗАХИСТУ РОЗУМНИХ МІСТ

1.1 Поняття та архітектура розумного міста

У XXI столітті більшість мегаполісів і середніх міст стикаються з нагальною потребою підвищення ефективності управління міськими процесами, забезпечення стійкості до зовнішніх загроз, а також покращення якості життя населення. У відповідь на ці виклики виникла концепція «розумного міста» (smart city), яка передбачає інтеграцію сучасних інформаційно-комунікаційних технологій у всі сфери міського життя з метою підвищення прозорості, безпеки та комфорту.

Поняття «розумне місто»:

Під терміном розумне місто розуміється урбаністична модель, яка використовує цифрові технології (Інтернет речей, хмарні обчислення, великі дані, штучний інтелект) для збору, аналізу й обробки інформації в реальному часі. Отримані дані дозволяють оперативно приймати рішення щодо транспорту, енергетики, екології, безпеки, охорони здоров’я, освіти, комунальних послуг тощо.

Важливо підкреслити, що смарт-місто – це не лише набір технологій, а й стратегія розвитку, орієнтована на сталий розвиток, цифрову інклюзію та активну участь громадян у житті громади.

Ключові компоненти архітектури розумного міста

Архітектура розумного міста формується на базі комплексної взаємодії різних технічних, інформаційних та організаційних елементів. До основних складових можна віднести такі компоненти:

1. IoT-пристрої та сенсорна інфраструктура

IoT (Internet of Things – Інтернет речей) є серцем розумного міста. Це мережа взаємопов’язаних пристроїв, здатних передавати дані без участі людини. До прикладу:

- датчики якості повітря;
- камери відеонагляду;
- «розумні» лічильники електроенергії, води та газу;
- трекери транспорту;

– вуличні сенсори шуму або температури.

Ці пристрої працюють як очі й вуха міста, забезпечуючи постійний потік даних для подальшої обробки.

2. Комунікаційні мережі

Накопичена інформація повинна швидко передаватися на обробку, що потребує стійких та масштабованих мереж зв’язку. Використовуються різні технології:

– мобільний зв’язок (4G/5G);

– мережі Wi-Fi у громадських місцях;

– LoRaWAN для енергоощадних пристроїв;

– волоконно-оптичні кабелі для магістральної передачі.

Важливими вимогами є надійність, мінімальна затримка та кіберзахищеність мереж.

3. Центри обробки даних та хмарні технології

Дані, отримані з тисяч пристроїв, передаються у дата-центри або обробляються в хмарних платформах. Ці системи виконують:

– фільтрацію й агрегацію інформації;

– аналітику та побудову моделей поведінки;

– автоматичне прийняття рішень (наприклад, зміну світлофору залежно від інтенсивності руху).

Хмарні технології забезпечують масштабованість та централізацію керування даними, що дозволяє містам зменшувати витрати на локальну інфраструктуру.

4. Інтелектуальні системи керування

Остаточним елементом архітектури є застосунки та панелі моніторингу, через які уповноважені служби здійснюють контроль над інфраструктурою. Наприклад:

– системи керування дорожнім рухом;

– платформи диспетчеризації громадського транспорту;

– сервіси відстеження витоків або аварій у мережах ЖКГ;

– ситуаційні центри безпеки із застосуванням AI-аналітики.

Загалом архітектура Smart City – це динамічна, інтегрована екосистема, в якій відбувається постійна взаємодія: «збір даних – аналіз – прийняття рішення – автоматична реакція».

Практичні приклади впровадження у світі

У ряді міст світу вже реалізовано успішні приклади застосування розумних технологій:

Сінгапур: створено єдину платформу Virtual Singapore, яка моделює всі інфраструктурні процеси в цифровому вигляді.

Барселона: використання сенсорів для регулювання освітлення та іригації вулиць залежно від присутності людей.

Сеул: використання системи Smart Seoul для відстеження транспорту, моніторингу екологічного стану та надання цифрових послуг населенню.

Торонто: впровадження «розумного району» з енергоефективними будівлями, автоматизованим сміттєзбиранням та відкритими API.

Поточний стан в Україні

В Україні також спостерігається поступовий рух у напрямку смарт-технологій. Найбільш активні міста:

Київ: система відеоспостереження Безпечне місто, інтеграція е-квитків, електронні сервіси.

Львів: розумне освітлення вулиць, система моніторингу водопостачання.

Дніпро: інтелектуальні зупинки, GPS-моніторинг транспорту.

Одеса: встановлення лічильників, модернізація транспорту, відеонагляд, окремі сервіси електронного врядування.

Проте впровадження має фрагментарний характер, а кібербезпека цих систем часто залишається на низькому рівні, що створює потенційні ризики – цей аспект буде розглянуто у наступному підпункті.

У сучасних умовах цифрової трансформації міського управління архітектура смарт-міста передбачає функціонування великої кількості взаємопов’язаних

інформаційно-комунікаційних компонентів. Ключовим елементом є централізована платформа, яка обробляє вхідні дані від сенсорних систем та інших джерел, аналізує їх у реальному часі й формує рішення, що реалізуються через різноманітні сервіси.

Для ілюстрації загальної логіки взаємодії між елементами цифрової інфраструктури смарт-міста на рис. 1 представлено узагальнену схему архітектури. У схемі умовно виділено три рівні:

а) Рівень сенсорних підсистем – джерела даних (розумні лічильники, системи транспорту, SCADA-модулі, камери тощо);

б) Центральний рівень – аналітична та керуюча платформа (Smart City Core Platform);

в) Рівень сервісів та взаємодії з громадянами – інтерфейси, через які реалізується результат (CRM, мобільні додатки, інформаційні портали).

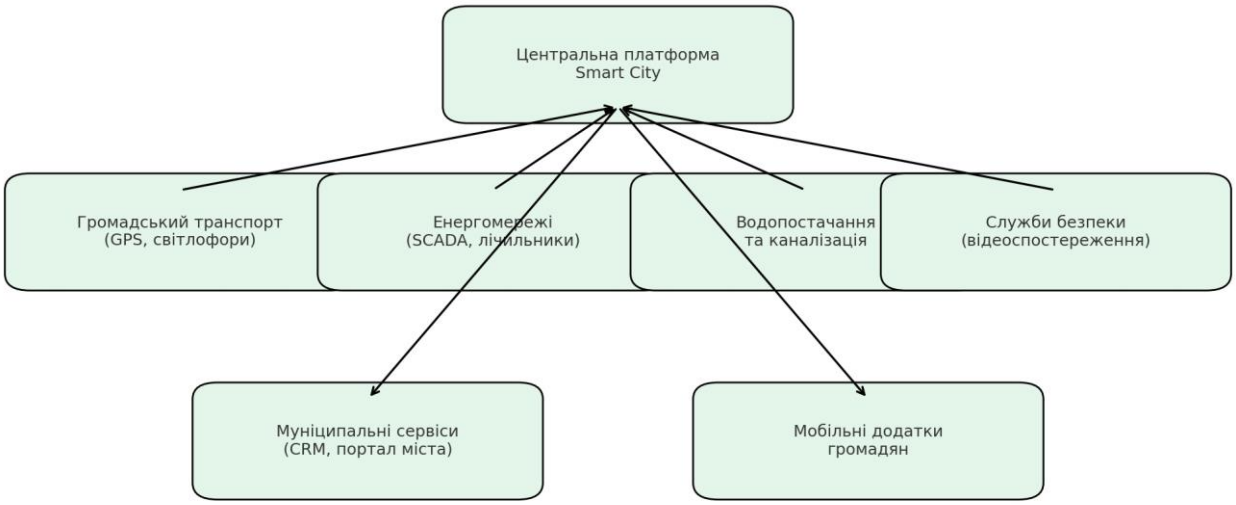

Рисунок 1.1 – Схема архітектури розумного міста (Smart City)

1.2 Основні кіберзагрози для інфраструктури розумного міста

Розумні міста базуються на масштабній цифровій інфраструктурі, що передбачає взаємодію між тисячами пристроїв, сервісів і мереж. Така складна система створює широке поле для потенційних кіберзагроз, адже практично кожен

її компонент може стати ціллю для атаки. Враховуючи критичну роль IT у функціонуванні Smart City, захист від кіберзагроз стає не лише технічним, а й національним питанням безпеки.

1. Вразливості IoT-пристроїв

Більшість IoT-сенсорів мають обмежені ресурси – слабкий процесор, обмежену пам’ять та енергоживлення. Через це на них часто не встановлюють повноцінні системи захисту. Наслідки:

– Відсутність шифрування даних під час передачі;

– Використання стандартних паролів («admin», «123456»);

– Неможливість оновлення прошивки, що відкриває шлях до постійного використання відомих вразливостей.

Приклад: у 2016 році ботнет Mirai атакував мільйони простих IoT-пристроїв (відеокамери, маршрутизатори), створивши рекордну DDoS-атаку на DNS-сервер Dyn. Після цього частина інтернету (Netflix, Twitter, GitHub) стала тимчасово недоступною.

2. Втручання в транспортні та енергетичні системи

Розумне місто часто включає автоматизовані системи регулювання транспорту (світлофори, диспетчерські служби) та енергопостачання. Їх порушення або захоплення може мати фізичні наслідки:

– Блокування руху, викликане зміною фаз світлофорів;

– Відключення електропостачання в житлових масивах;

– Маніпуляції з тарифами, підміна показників лічильників.

Приклад в Україні: у грудні 2015 року була здійснена кібератака на енергокомпанії Західної України, унаслідок якої понад 230 тисяч людей залишилися без електрики. Атака здійснювалася через шкідливе ПЗ BlackEnergy.

3. Атаки на хмарні платформи та сервіси обробки даних

Централізована обробка інформації в хмарних дата-центрах є зручною, але вразливою. У разі компрометації доступу зловмисник може:

– отримати повний контроль над сенсорними мережами;

– знищити або змінити історичні дані міста;

– стежити за переміщеннями людей або служб;

– створити інформаційний хаос (наприклад, дезінформацію на інформаційних панелях транспорту).

Особливо небезпечні атаки типу "людина посередині" (Man-in-the-Middle) при перехопленні трафіку між пристроями та серверами без шифрування.

4. DDoS-атаки на сервіси міста

DDoS (Distributed Denial of Service) – це атака, спрямована на виведення з ладу сайту або онлайн-сервісу шляхом перевантаження запитами. У контексті розумного міста мішенню можуть стати:

Портали електронних послуг (оплата ЖКГ, запис до лікаря, оформлення документів);

Системи міського моніторингу;

Комунікаційні вузли між районами.

Приклад: у 2022 році під час активної фази війни в Україні кілька міських порталів, зокрема у Львові, Івано-Франківську та Києві, стали жертвами масованих DDoS-атак, що на кілька годин зупинило надання цифрових сервісів.

5. Соціальна інженерія та фішинг

Технологічний рівень – не єдина слабка ланка. Людський фактор залишається одним із головних джерел загроз. Міські службовці, адміністратори, навіть оператори транспорту можуть стати об’єктами:

Фішингових листів із посиланнями на шкідливе ПЗ;

Підміни технічної документації;

Імітації запитів від керівництва для отримання доступів (атаки типу BEC – Business Email Compromise).

Соціальна інженерія особливо небезпечна в умовах війни, коли активується і психологічний тиск.

Таблиця 1.1 – Порівняння основних типів кібератак на смарт-міста

Тип атаки	Ціль	Наслідки	Приклад
DDoS	Сайти міськради, онлайн-сервіси	Параліч доступу до послуг, зниження довіри	DDoS-атака на «Київ Цифровий» (2022)
Злам IoT	Камери відеоспостереження, датчики	Перехоплення відео, керування пристроями	Злам Hikvision-камер у США (2021)
Злам SCADA	Енергомережі, водопостачання	Блекаут, порушення критичної інфраструктури	Атака BlackEnergy в Україні (2015)
Фішинг	Працівники служб або мерії	Викрадення облікових даних, доступ до систем	Атака на держоргани через e-mail (2023)
Wi-Fi Sniffing	Незахищені міські Wi-Fi точки	Прослуховування трафіку, крадіжка особистих даних	Зловмисники в метро м. Харків (2021)

Окрім порівняння характеристик окремих атак, важливо оцінити частотність загроз**,** з якими найчастіше стикаються смарт-міста у глобальному контексті. Візуалізована нижче діаграма показує орієнтовний розподіл основних типів кібератак, що вражають міську інфраструктуру за статистикою останніх років.

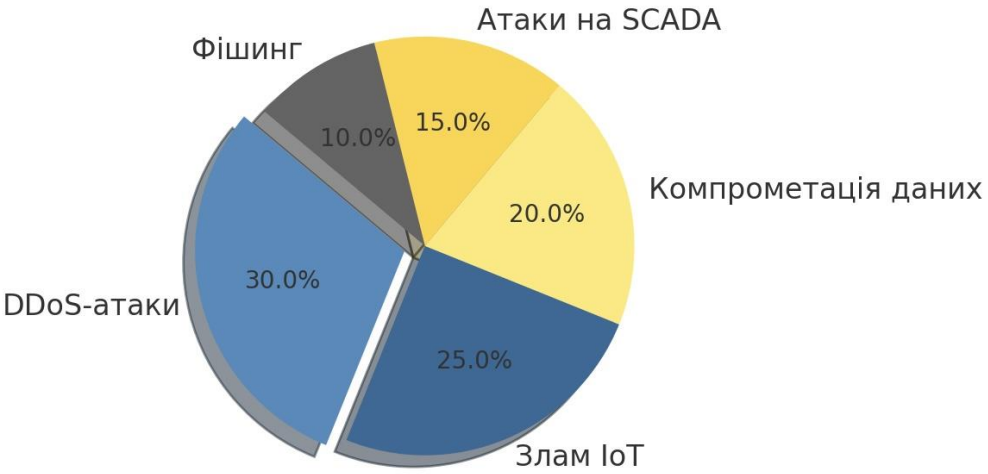

Рисунок 1.2 – Частотність основних типів кіберзагроз для інфраструктури смарт-міста

Як видно з представлених даних, найбільш поширеними загрозами залишаються атаки, пов’язані з несанкціонованим доступом та DDoS, які можуть паралізувати цілі сектори цифрового управління. Злам IoT-пристроїв також залишається критичним чинником, особливо через низький рівень шифрування та оновлення прошивок. Візуалізація підтверджує: найбільш масові атаки – це ті, що найчастіше ігноруються в міських стратегіях кіберзахисту.

1.3 Методи захисту смарт-міст

Сучасне смарт-місто є складною багаторівневою системою, вразливою до численних кіберзагроз. Тому безпека такої інфраструктури має базуватися на комплексному підході, який поєднує технічні рішення, організаційні заходи, правові норми та постійний моніторинг.

1. Технічні заходи кіберзахисту

Мережева безпека

Серед основних інструментів захисту мережі виділяють:

Брандмауери (firewall) – забезпечують фільтрацію небажаного трафіку між зонами довіри;

IDS/IPS-системи (системи виявлення та запобігання вторгнень) – аналізують трафік у реальному часі та реагують на підозрілу активність;

VPN – створення зашифрованих тунелів між пристроями, що унеможливлює перехоплення даних.

Захист IoT-пристроїв

Встановлення унікальних паролів, відмова від заводських налаштувань;

Оновлення прошивки через централізовані платформи;

Сегментація мережі, де пристрої обмежені у прямій взаємодії між собою (принцип «zero trust»).

Шифрування та автентифікація

Передача даних між компонентами інфраструктури має відбуватись із використанням шифрування TLS/SSL;

Впровадження багатофакторної автентифікації (MFA) для працівників органів управління;

Застосування цифрових сертифікатів для ідентифікації пристроїв та користувачів.

2. Використання штучного інтелекту та машинного навчання

Однією з перспективних галузей кіберзахисту є аналіз поведінкових аномалій з використанням технологій AI/ML:

Машинне навчання дозволяє виявляти підозрілу активність ще до її ескалації (наприклад, нетипову активність IoT-пристроїв уночі);

ШІ-системи можуть прогнозувати кібератаки на основі історичних патернів і змін у поведінці мережі;

Використовується в SOC (Security Operation Center) для автоматичного реагування на інциденти.

Такі рішення вже впроваджуються в розвинених смарт-містах, як-от Сінгапур, Барселона та Дубаї.

3. Організаційні та політичні механізми

- Політики безпеки

Розробка внутрішніх стандартів кіберзахисту для міських структур;

Встановлення правил обміну даними, політик щодо зберігання інформації та обмежень доступу.

– Навчання персоналу

Проведення регулярних тренінгів для службовців, IT-спеціалістів і операторів міських систем;

Імітаційні тестування на фішинг та соціальну інженерію для підвищення пильності.

– Аудит і тестування

Залучення зовнішніх експертів до проведення тестів на проникнення;

Оцінка відповідності інфраструктури міжнародним стандартам та оновлення політик відповідно до нових загроз.

4. Нормативно-правова база та стандарти

Міжнародні стандарти

ISO/IEC 27001 – управління інформаційною безпекою;

NIST Cybersecurity Framework – структурований підхід до виявлення, реагування та усунення кіберзагроз;

Zero Trust Architecture – принцип, за якого не довіряють жодному елементу системи «за замовчуванням».

Національні ініціативи

В Україні діють стандарти ДСТУ у сфері захисту інформації;

НКЦК (Національний координаційний центр кібербезпеки) забезпечує стратегічний рівень захисту об’єктів критичної інфраструктури, в т.ч. і Smart City.

Узагальнення

Кіберзахист розумного міста – це багаторівнева система, яка повинна включати:

1) Базові технічні засоби (firewall, IDS, VPN);
2) Сучасні підходи (AI/ML для виявлення загроз);
3) Організаційну дисципліну (політики, навчання);
4) Підтримку міжнародних та національних стандартів.

Усе це працює лише в умовах комплексного та постійного підходу, коли безпека розглядається не як разовий захід, а як невід’ємна частина стратегії розвитку міста.

2 АНАЛІЗ СТАНУ КІБЕРЗАХИСТУ В УКРАЇНІ ТА ОДЕСІ

2.1 Смарт-міста в Україні: загальний огляд

У XXI столітті більшість великих міст світу почали трансформуватись у так звані «розумні міста» (smart cities) – міста, де технології допомагають ефективніше керувати інфраструктурою, зменшувати витрати, підвищувати безпеку та комфорт для мешканців. Україна також робить кроки в цьому напрямку.

Станом на 2024 рік, в Україні існує понад 15 муніципалітетів, які офіційно декларують перехід до smart city-моделі. Однак рівень впровадження технологій, підхід до безпеки та наявність цілісної стратегії дуже різняться.

Приклади впровадження смарт-технологій в українських містах:

Київ. Столиця – лідер за кількістю впроваджених рішень. Тут діє проєкт «Безпечне місто», що включає:

– понад 7 000 камер відеоспостереження;

– аналітику номерних знаків;

– централізоване сховище даних (міський дата-центр);

– систему відеоаналітики з автоматичним виявленням підозрілої поведінки.

– Також Київ має електронну систему подачі заяв на дитсадки, мобільні сервіси для транспорту, відкриті міські API, систему «Kyiv Smart City ID» тощо.

– Львів.

– Місто активно інвестує у «розумний» транспорт та енергоефективність:

– GPS-трекінг комунального транспорту;

– електронні квитки та система «Леокарт»;

– платформи онлайн-звернень;

– автоматичне регулювання вуличного освітлення.

– Крім того, Львів розробив власну концепцію кіберзахисту муніципальних даних.

– Дніпро.

– Фокус зроблено на розумному обліку ресурсів:

– IoT-лічильники тепла, води та електроенергії;

– система диспетчеризації аварійних служб;

– модернізована система вуличного освітлення з дистанційним керуванням.

У місті працює муніципальна IT-команда, яка забезпечує технічну підтримку сервісів.

Харків.

Тут частково впроваджено:

– електронні сервіси для мешканців (довідки, звернення, оплата послуг);

– автоматизацію управління світлофорами;

– початкова фаза створення міського дата-центру;

– систему відеоспостереження на основі китайських рішень.

Однак, через складну ситуацію з безпекою, розвиток digital-напрямку в місті частково уповільнений.

Загальні характеристики смарт-інфраструктури в Україні:

На сьогодні більшість впроваджених рішень мають технічний характер – встановлення камер, лічильників, екранів, онлайн-сервісів. Значно рідше впроваджується аналітика даних, автоматизація прийняття рішень або штучний інтелект.

Серед типових рішень:

– системи відеонагляду;

– GPS-моніторинг транспорту;

– smart-освітлення;

– облік комунальних ресурсів;

– електронні сервіси для громадян;

– розумні паркування;

– електронні черги та документообіг.

Але рідко ці елементи утворюють єдину інтегровану систему, що ускладнює їх захист. І тут виникає ключове питання – рівень кіберзахисту всіх цих систем

Проблеми впровадження кіберзахисту в українських містах.

Незважаючи на технічний прогрес, смарт-інфраструктура в Україні має серйозні виклики в безпековому плані:

а) Відсутність стандартів.

У більшості міст не існує узгоджених політик щодо кіберзахисту. Часто безпека залежить від конкретного підрядника або відділу IT.

б) Фрагментарність систем.

Камери можуть належати одному підрозділу, мережі – іншому, а сервіси – третій фірмі. Це створює складнощі для моніторингу та реагування.

в) Недостатнє фінансування.

Часто системи встановлюються без урахування витрат на підтримку, оновлення, аудит або захист.

г) Використання застарілих або ненадійних пристроїв.

Дешеві IoT-сенсори, куплені за залишковим принципом, рідко мають захист, а ще рідше оновлюються.

д) Людський фактор.

Недостатня підготовка персоналу, небезпека фішингу, відкриті порти, незахищені Wi-Fi – усе це залишає системи вразливими.

Хоча в Україні помітний прогрес у цифровізації міст, рівень кіберзахисту відстає. Переважно впроваджуються окремі рішення без єдиної захисної стратегії. Це створює потенційні «дірки» у безпеці – особливо в умовах воєнного та гібридного тиску, де критична інфраструктура може бути ціллю кібератак.

Упродовж останнього десятиліття в Україні відбувається активне впровадження концепції «розумного міста», яке передбачає цифровізацію ключових міських функцій – від керування транспортом до надання е-сервісів населенню. Проте рівень кіберзахисту в різних містах залишається нерівномірним, залежить як від фінансових ресурсів, так і від управлінських рішень місцевих органів влади.

Щоб оцінити загальний стан цифровізації та готовності до кіберзагроз, нижче подано порівняльну таблицю п’яти українських міст, які активно реалізують елементи Smart City. Вона включає основні сервіси, наявність систем безпеки, а також короткі коментарі щодо проблем або досягнень.

Таблиця 2.1 – Оцінка стану впровадження Smart City та рівня кіберзахисту в окремих містах України

Місто	Основні цифрові сервіси	Рівень кіберзахисту	Коментар
Київ	Громадський транспорт, відеонагляд	Високий	Функціонує CERT-KY, SIEM на базі КМДА
Львів	Освітлення, е-сервіси для містян	Середній	Впроваджено базове шифрування
Дніпро	Онлайн-портали, транспорт, GPS	Середній	Впроваджується SIEM-система
Харків	Відеоспостереження, е-квиток	Низький	Бракує оновлень IoT
Одеса	Розумні лічильники, відеонагляд	Низький	Частина камер працює без шифрування, вразливі порти, відсутність VPN

Проведений аналіз показує, що хоча багато українських міст поступово інтегрують цифрові сервіси у свої інфраструктури, рівень кіберзахисту не завжди відповідає темпам цифровізації. Київ демонструє системний підхід із впровадженням централізованих систем моніторингу, тоді як інші міста часто стикаються з проблемами безпеки, зумовленими недостатнім шифруванням, слабким контролем доступу та браком кадрів. Одеса, попри розвиток IoT-рішень, наразі належить до групи міст з підвищеним ризиком, що потребує негайного вдосконалення підходів до захисту критичних цифрових систем.

2.2 Що зроблено в Одесі у напрямку смарт-інфраструктури

Одеса – одне з найбільших міст України, важливий транспортний вузол, порт та туристичний центр. Саме тому логічним виглядає курс на цифрову трансформацію міста, впровадження смарт-рішень для покращення керування, безпеки та якості життя. Проте, як і в багатьох інших українських містах, розвиток smart city-технологій в Одесі має як досягнення, так і помітні обмеження – особливо у сфері безпеки.

Ключові елементи смарт-інфраструктури в Одесі

1. Система відеоспостереження

У місті діє система відеонагляду, яка активно розвивається з 2017 року. Станом на 2024 рік встановлено понад 2 000 камер відеоспостереження, з них частина – з функцією розпізнавання номерів авто.

Ці камери охоплюють:

- центральні вулиці;
- перехрестя;
- парки;
- набережну;
- підходи до шкіл та громадських об’єктів.

Камери підключені до міського ситуаційного центру, де оператори ведуть моніторинг у реальному часі. Також здійснюється зберігання відео, хоча є питання щодо термінів зберігання та захисту даних.

2. Система керування дорожнім рухом

В Одесі впроваджено автоматизовану систему управління світлофорами. Частина світлофорів підключена до єдиної системи, яка дозволяє:

- регулювати світлофазу в залежності від трафіку;
- надавати пріоритет громадському транспорту;
- зменшувати затори.

Проте не всі вузли міста автоматизовані – багато ділянок залишаються на старих контролерах.

3. Вуличне освітлення

Впроваджується енергоефективне LED-освітлення, частково з можливістю дистанційного керування. Це дозволяє економити електроенергію та зменшити витрати міського бюджету. Деякі вулиці обладнані датчиками освітленості, які автоматично вмикають освітлення.

4. Транспорт і смарт-паркування

Існує система GPS-моніторингу муніципального транспорту. Інформація передається в мобільні додатки (наприклад, EasyWay), що дозволяє мешканцям відстежувати рух маршрутів у реальному часі.

Щодо паркування – діє електронна система оплати, проте вона охоплює не всі зони. Смарт-аналіз завантаженості паркомісць поки що не реалізовано.

5. Електронні сервіси

На порталі Одеської міської ради та через додаток «Мій Одеса» мешканці можуть:

- подати звернення;
- записатись на прийом;
- перевірити нарахування;
- залишити скаргу.

Проте ці сервіси поки не пов’язані з іншими системами міста (відеоспостереження, транспорт тощо), тобто є фрагментованими.

Проблеми кіберзахисту існуючих рішень

Попри наявність технологій, кібербезпека часто залишається на другому плані. Основні виклики:

1. Відсутність загальної стратегії захисту

Окремі елементи інфраструктури захищаються точково, але єдиної політики кіберзахисту міста немає. Наприклад, камери можуть обслуговуватись сторонніми підрядниками без належного аудиту їхніх рішень.

2. Низький рівень шифрування та контролю доступу

У ряді випадків відеопотоки з камер не мають сучасного шифрування або використовуються стандартні паролі. Це створює ризик витоку конфіденційних даних або зовнішнього втручання.

3. Відсутність аномалійного моніторингу

Системи керування світлофорами або освітленням не оснащені інструментами виявлення аномальної активності. Це означає, що зловмисник може непомітно втрутитись у роботу мережі.

4. Небезпека DDoS-атак

Міські сервери (портал ради, системи відеонагляду) можуть бути вразливими до атак на відмову в обслуговуванні, оскільки не мають масштабованої хмарної інфраструктури або захисту рівня CDN.

Чи використовується штучний інтелект в Одесі?

На сьогодні офіційної інформації про впровадження AI у міську інфраструктуру Одеси немає. Наприклад:

– відеоаналітика не використовує розпізнавання облич;
– системи керування трафіком не застосовують машинне навчання;
– відсутній аналіз поведінкових патернів у кіберпросторі.

Це залишає потенціал для подальшого розвитку – особливо з огляду на зростаючу кількість кіберзагроз

Одеса має низку досягнень у напрямку smart city, зокрема у відеоспостереженні, транспорті та електронних послугах. Проте рівень інтеграції, захисту та інноваційної аналітики поки що обмежений. Ключові проблеми – відсутність єдиної політики кіберзахисту, недостатнє шифрування, застарілі підходи до моніторингу та слабке використання сучасних технологій, таких як AI.

2.3 Основні проблеми та виклики кіберзахисту смарт-інфраструктури

Розвиток smart city – це не лише про зручність, автоматизацію та цифровізацію міста. Це ще й новий фронт у сфері кібербезпеки, де міська інфраструктура стає потенційною ціллю для злочинців, хактивістів чи навіть

ворожих держав. В умовах війни та нестабільності ситуація ще більше ускладнюється. Розглянемо ключові проблеми та виклики на прикладі українських реалій, з фокусом на Одесу.

1. Технічні вразливості

– Застаріле обладнання та програмне забезпечення

Багато сенсорів, камер, маршрутизаторів у містах, включаючи Одесу, використовують застарілу техніку, часто ще з 2010-х років. Наприклад, деякі моделі IP-камер досі не підтримують шифрування трафіку, що дозволяє перехоплювати зображення з них.

У 2022 році низка українських міст зазнала DDoS-атак на міські портали, викликаних саме через відкриті, неоновлені системи керування.

– Відсутність системи моніторингу та журналювання

Багато систем працюють “в темряві” - тобто відсутні централізовані журнали подій, системи виявлення вторгнень, або їх ніхто не аналізує. В Одесі лише окремі об’єкти підключено до базового моніторингу кіберінцидентів.

– Взаємозв’язок усіх підсистем

Системи відеонагляду, транспортні сенсори, світлофори та енергетичні об’єкти часто взаємопов’язані через загальні мережі. Атака на один з елементів, наприклад - систему керування вуличним освітленням - може призвести до ефекту “доміно” в інших сегментах.

2. Організаційні проблеми

– Розпорошеність відповідальності

У реальному житті, за різні частини інфраструктури відповідають різні відділи, департаменти, іноді - підрядники. Це створює “дірки” в захисті, коли одна система оновлюється, а інша - ні.

– Відсутність політик безпеки

У багатьох містах немає жодного офіційного документу, який би регламентував:

а) створення резервних копій,

б) зміну паролів,

в) політику доступу до систем,

г) періодичний аудит безпеки.

У деяких випадках дані з камер чи сенсорів залишаються доступними публічно через відкриті порти, навіть не знаючи про це.

- Відсутність незалежного аудиту

Найбільші смарт-системи в Україні впроваджуються без обов’язкового зовнішнього кібер-аудиту. Це означає, що навіть після запуску в експлуатацію, ніхто не перевіряє захищеність системи від актуальних загроз.

3. Людський фактор

- Низький рівень обізнаності

Класична ситуація: адміністратор, відповідальний за камери чи вуличне освітлення, не має спеціальної кіберосвіти. Люди на посаді часто не вміють:

а) виявити аномальний трафік,

б) налаштувати брандмауер,

в) проаналізувати лог-файли.

Це створює ситуації, коли навіть після кіберінциденту ніхто не помічає зламу протягом тижнів.

– Випадкові або шкідливі дії працівників

У 2023 році було зафіксовано кілька інцидентів, коли колишні працівники зберігали доступ до адмін-панелей через відсутність чіткої процедури деактивації.

Іноді навіть несвідомі дії - як, наприклад, встановлення “піратського” ПЗ на сервери - можуть відкрити шлях вірусам або бекдорам.

4. Фінансові труднощі

– Недостатнє фінансування

Кібербезпека потребує інвестицій. Проте в умовах воєнного стану й обмежених бюджетів, всі кошти спрямовуються на фізичну безпеку та гуманітарні потреби. Наприклад, проєкти з оновлення мережевого обладнання відкладаються “до кращих часів”.

– Витрати на підтримку

Окрім закупівлі систем, потрібно регулярно платити за:

а) ліцензії,

б) антивіруси,

в) технічну підтримку,

г) навчання персоналу.

У багатьох випадках ці витрати не закладаються в річний бюджет або скорочуються.

5. Психологічні та соціальні виклики

– Втрата довіри громадян

Коли стаються витоки відео з камер чи збої в міських сервісах, мешканці втрачають довіру до систем. В Одесі у 2022 році соціальні мережі обговорювали випадок, коли трансляція з міської камери випадково потрапила на сторонній сайт – і це викликало обурення.

– Дезінформація та паніка

Недостатній кіберзахист створює можливість для поширення фейкових повідомлень через міські сервіси або чат-боти. Це особливо небезпечно у воєнний час, коли паніка може призвести до хаосу.

6. Нормативно-правові прогалини

– Відсутність законодавчої бази

Національне законодавство України ще не адаптоване до потреб smart city. Немає чітких вимог щодо безпеки міських IoT-систем, протоколів обміну, зберігання даних. Це дозволяє постачальникам ігнорувати найпростіші правила безпеки.

– Відсутність стандартів інтеграції

Сьогодні практично кожне місто створює свою смарт-архітектуру “з нуля”, без уніфікованих підходів. Це ускладнює централізоване реагування на загрози або аналіз подій на рівні держави.

Станом на 2024 рік, система кіберзахисту смарт-міст в Україні – фрагментована й незавершена. Технічні недоліки, нестача коштів, відсутність стандартів та людський фактор створюють сприятливі умови для атак. Успішна

реалізація smart city можлива лише за умови, що кіберзахист стане її невід'ємною частиною з першого дня, а не "опцією на потім".

2.4 Динаміка кіберінцидентів у муніципальних структурах міст України

Зі зростанням рівня цифровізації міст України зростає й кількість кіберінцидентів, що стосуються інфраструктури е-сервісів, IoT-пристроїв, адміністративних порталів та транспортних систем. Найчастіше інциденти пов'язані з відсутністю шифрування, незахищеним віддаленим доступом або людським фактором.

Зібрані нижче дані базуються на відкритих джерелах, звітах CERT-UA, муніципальних звітах із публічних закупівель і дослідженнях IT-компаній. Вони ілюструють кількісну динаміку інцидентів у п'яти великих українських містах протягом шести років:

Дані за 2024 рік – за перше півріччя (січень-червень).

Таблиця 2.4 – Кількість кіберінцидентів у муніципальних системах українських міст (2019–2024)

Рік	Київ	Харків	Дніпро	Одеса	Львів
2019	18	12	9	14	7
2020	22	14	12	15	10
2021	31	18	15	19	13
2022	35	21	17	23	17
2023	41	26	20	28	20
2024*	24	16	11	19	12

Показники демонструють чітку тенденцію до зростання кількості інцидентів до 2023 року з частковим спадом у першій половині 2024-го, що може бути наслідком посилення політик безпеки або прихованості інцидентів. Одеса

стабільно входить до групи міст із підвищеним рівнем загроз, поступаючись лише Києву, що свідчить про гостру потребу в оновленні систем захисту.

2.5 Фінансування кібербезпеки як чинник стійкості міської інфраструктури

Ключовим чинником стійкості кіберзахисту є не лише наявність технологій чи процедур, а й фінансове забезпечення відповідних проєктів**.** Без системного бюджетування унеможливлюється реалізація навіть базових заходів – таких як оновлення ПЗ, навчання персоналу чи розгортання систем моніторингу. Оцінка динаміки фінансування в обраних містах України дозволяє побачити зв’язок між ресурсною базою та загальним рівнем безпеки інфраструктури.

Нижче наведено умовну таблицю фінансування програм інформаційної безпеки за 2022–2024 роки (у млн грн), що ґрунтується на узагальнених відкритих бюджетах IT-департаментів та програм цифрової трансформації міст:

*Примітка: дані за 2024 рік сформовано на основі публічних проєктів рішень міських рад та програмних заявок.

Таблиця 2.5 – Обсяг фінансування заходів кібербезпеки у міських системах (2022–2024)

Рік	Київ	Дніпро	Одеса	Львів
2022	22	7	5	6
2023	27	9	6	8
2024*	19	6	4	5

Фінансові інвестиції у сферу кіберзахисту залишаються на стабільно низькому рівні, особливо у регіональних центрах. Хоча Київ має найбільше фінансування, навіть воно в 2024 році демонструє спад, що можна пояснити перерозподілом коштів на інші сфери. У випадку Одеси обсяг бюджетних витрат залишається найнижчим серед аналізованих міст, що частково пояснює високий рівень інцидентів, зафіксований у таблиці 2.4. Це свідчить про необхідність

перегляду пріоритетів міського управління з акцентом на захист цифрових сервісів, особливо в умовах зростання загроз.

3 ПРАКТИЧНІ МЕТОДИ ЗАХИСТУ РОЗУМНОГО МІСТА ВІД КІБЕРАТАК

3.1 Архітектура систем кіберзахисту в розумному місті

З огляду на стрімкий розвиток цифрових технологій та широке впровадження концепції «розумного міста», питання формування цілісної, багаторівневої системи кіберзахисту стає одним із ключових елементів стратегії безпечної урбаністики. Смарт-інфраструктура передбачає масштабне застосування взаємопов’язаних цифрових систем, включаючи сенсори, пристрої Інтернету речей (IoT), засоби автоматизованого управління транспортом, інтелектуальні мережі енергозабезпечення, а також сервіси електронного врядування. У такому контексті архітектура кіберзахисту виконує функцію опорного каркасу, на якому базується безпечне функціонування цифрової екосистеми міста.

Архітектура кіберзахисту – це сукупність методів, інструментів, політик і технологічних рішень, інтегрованих у єдину систему для забезпечення захисту інформаційних активів, мережевих інфраструктур та критично важливих сервісів. Вона охоплює не лише технічний рівень, а й організаційний, процедурний і управлінський аспекти. Ключовою її характеристикою є системність, тобто здатність забезпечити взаємодію всіх компонентів захисту у єдиній логіці реагування, моніторингу та профілактики загроз.

Однією з основ концептуальної побудови архітектури кіберзахисту є модель глибокоешелонованої оборони (defense-in-depth). Вона базується на принципі багаторівневого захисту, де кожен рівень системи забезпечується окремими, незалежними механізмами безпеки. Такий підхід дозволяє підвищити стійкість до атак за рахунок дублювання та перекриття потенційно вразливих місць. У практичному розрізі це означає одночасне застосування фаєрволів, систем виявлення вторгнень, шифрування, контролю доступу, сегментації мереж, багатофакторної аутентифікації та інших засобів.

Загалом архітектура кіберзахисту розумного міста умовно може бути структурована за такими рівнями:

а) Фізичний рівень – включає захист обладнання, центрів обробки даних, мережевих вузлів, контролерів. Засоби фізичної безпеки передбачають обмеження фізичного доступу, відеоспостереження, сейфове зберігання, сигналізацію та інші інженерні заходи.

б) Мережевий рівень – забезпечує захист при передачі даних між пристроями та системами. Тут використовуються міжмережеві екрани (фаєрволи), системи виявлення та запобігання вторгненням (IDS/IPS), протоколи шифрування (IPSec, TLS), віртуальні приватні мережі (VPN), а також засоби сегментації мереж (VLAN, DMZ).

в) Системний рівень – пов’язаний із забезпеченням безпеки операційних систем, прикладного програмного забезпечення, служб управління та баз даних. Впроваджуються системи обліку подій, механізми контролю оновлень, налаштування політик доступу, системи виявлення шкідливого ПЗ тощо.

г) Прикладний рівень – передбачає захист вебсервісів, мобільних застосунків, платформ е-урядування та інших інтерфейсів взаємодії з користувачем. Тут реалізуються політики автентифікації, захист API, контроль вхідних запитів, перевірка цілісності даних.

д) Організаційно-адміністративний рівень – охоплює нормативне регулювання, політики інформаційної безпеки, навчання персоналу, управління ризиками, аудит інформаційної безпеки, реагування на інциденти.

Особливу увагу слід приділити принципу мінімальних привілеїв (Least Privilege), який полягає в тому, що користувач або пристрій отримує лише ті права доступу, які необхідні для виконання його функцій. Впровадження такого принципу у розумній міській інфраструктурі дозволяє мінімізувати потенційні наслідки компрометації облікових записів.

Окреме місце в сучасній архітектурі кіберзахисту займає підхід Zero Trust Architecture (ZTA), що базується на відсутності апріорної довіри до будь-якого елемента системи – як внутрішнього, так і зовнішнього. Це означає, що кожен запит до ресурсу повинен бути аутентифікований, авторизований і зафіксований незалежно від того, звідки він походить. Для реалізації цього підходу в міському

масштабі доцільно впроваджувати системи постійної перевірки ідентичності (Continuous Authentication), засоби контекстного доступу (наприклад, доступ дозволяється лише з певної геолокації або пристрою), а також автоматизовані системи управління політиками доступу.

У контексті реального міського середовища, зокрема Одеси, критично важливим є дотримання принципу розділення зон безпеки. Зокрема, IoT-пристрої (сенсори, камери спостереження, лічильники), які мають обмежені ресурси захисту, повинні бути ізольовані від внутрішніх систем електронного документообігу або баз персональних даних. Інакше існує ризик, що через компрометацію умовного сміттєвого сенсора зловмисник зможе вийти на адміністративну частину інфраструктури.

Ще одним важливим елементом є централізований моніторинг і логування. Усі компоненти системи мають бути підключені до єдиної платформи, яка агрегує події безпеки, проводить їх кореляцію та дозволяє оперативно виявляти інциденти. Для цього доцільно застосовувати SIEM-рішення (Security Information and Event Management), які здатні обробляти великі обсяги даних у реальному часі.

Не менш значущим є захист каналів зв’язку між компонентами розумного міста. У випадках, коли передача даних відбувається через відкриті мережі або бездротові з’єднання, слід застосовувати додаткові шари шифрування, контроль доступу на основі MAC-адрес або цифрових сертифікатів. Особливо це стосується систем відеоспостереження, які часто є вразливими через невикористання сучасних протоколів шифрування.

Отже, побудова архітектури кіберзахисту для розумного міста – це не просто впровадження окремих технічних рішень, а формування інтегрованої, гнучкої та масштабованої системи, здатної забезпечити стійкість до широкого спектра загроз. У випадку Одеси як великого урбаністичного центру, доцільно розглядати архітектуру кіберзахисту як інфраструктурний елемент на рівні з дорогами, електромережами чи водопостачанням – настільки критичною вона стає для сучасного міського життя.

3.2 Технічні рішення забезпечення кіберзахисту смарт-інфраструктури: IDS/IPS, SIEM, криптографія, Zero Trust

У сучасних умовах цифрової трансформації міського середовища значення технічних засобів кібербезпеки зростає пропорційно до рівня автоматизації та мережевої взаємодії між компонентами інфраструктури. Технічні рішення в системах захисту розумного міста мають бути не лише адаптивними до змін середовища, а й здатними до проактивного виявлення, аналізу й нейтралізації потенційних загроз. Серед ключових технологічних складових ефективної системи кібербезпеки можна виділити системи виявлення та запобігання вторгненням (IDS/IPS), системи управління інформацією та подіями безпеки (SIEM), криптографічні засоби захисту даних та концепцію нульової довіри (Zero Trust Architecture, ZTA).

1) Системи виявлення та запобігання вторгненням (IDS/IPS)

Системи IDS (Intrusion Detection Systems) та IPS (Intrusion Prevention Systems) є фундаментальними елементами для забезпечення мережевої безпеки. IDS функціонують за принципом пасивного моніторингу мережевого трафіку з метою виявлення ознак аномальної або шкідливої активності. Натомість IPS реалізує активні дії щодо нейтралізації виявленої загрози в режимі реального часу, наприклад, блокування підозрілих пакетів чи ізоляція компрометованого вузла.

У контексті міської смарт-інфраструктури впровадження IDS/IPS дозволяє контролювати взаємодію між численними пристроями Інтернету речей (IoT), міськими сервісами (наприклад, платформи е-врядування, системи моніторингу транспорту), а також захищати периметри від зовнішніх зловмисників. Типовими реалізаціями є Snort, Suricata, Zeek – відкриті системи, які можуть бути адаптовані для потреб муніципалітету з мінімальними витратами.

Доцільно використовувати гібридний підхід, який поєднує сигнатурний (на основі відомих шаблонів атак) та поведінковий (аналіз аномалій у поведінці користувачів або пристроїв) методи. Це дозволяє виявляти як відомі загрози, так і нові типи атак, які не мають визначеної сигнатури.

2) Системи управління інформацією та подіями безпеки (SIEM)

SIEM (Security Information and Event Management) – це категорія систем, що забезпечують централізоване збирання, зберігання, кореляцію, аналіз та візуалізацію подій безпеки з різних джерел: серверів, мережевих пристроїв, прикладного програмного забезпечення, баз даних, хмарних сервісів тощо. Завдяки цьому SIEM дозволяє оперативно реагувати на інциденти, формувати звітність для аудиту, а також будувати історичні профілі поведінки користувачів або компонентів інфраструктури.

У масштабов міста, де кількість об’єктів обробки даних обчислюється тисячами, а рівень децентралізації високий, роль SIEM важко переоцінити. Вона є фактичним «центром ситуаційної обізнаності», який дозволяє адміністраторам бачити загальну картину кіберзагроз, виявляти складні атаки типу APT (Advanced Persistent Threat) та визначати вузькі місця у поточній архітектурі безпеки.

З-поміж доступних рішень слід згадати такі продукти, як Splunk, IBM QRadar, ELK Stack (ElasticSearch, Logstash, Kibana), OSSIM (Open Source SIEM). Їх впровадження потребує попередньої стандартизації логів, вибору релевантних джерел даних та налаштування політик кореляції, що є критично важливим для уникнення помилкових спрацювань.

3) Криптографічні методи захисту

Криптографія становить основу конфіденційності, цілісності та автентичності інформації у цифрових системах. У смарт-інфраструктурі міста криптографічні засоби застосовуються в численних сценаріях – від захисту трафіку IoT-пристроїв до забезпечення електронного документообігу та електронної ідентифікації громадян.

Основними напрямами криптографічного захисту є:

- Шифрування даних при передачі та зберіганні – застосування протоколів TLS 1.3, HTTPS, IPsec, а також end-to-end шифрування в критично важливих системах (наприклад, у медичних або енергетичних сервісах).
- Цифровий підпис і PKI (інфраструктура відкритих ключів) – для забезпечення цілісності документів і транзакцій, особливо в сервісах е-урядування.

– Аутентифікація на основі сертифікатів – як альтернатива паролям, особливо в системах машинної взаємодії без участі людини.

При впровадженні криптографії важливо враховувати обмеження на обчислювальні ресурси IoT-пристроїв, які часто не можуть підтримувати складні алгоритми шифрування. У таких випадках доцільним є використання полегшених криптографічних протоколів (наприклад, ECC – еліптичні криві) та апаратного прискорення.

4) Концепція Zero Trust Architecture (ZTA)

Модель нульової довіри (Zero Trust) відходить від традиційної парадигми, де внутрішня мережа вважається безпечною, а зовнішня – небезпечною. Натомість Zero Trust базується на тезі «нікому не довіряй, завжди перевіряй», що означає необхідність перевірки кожної дії, незалежно від її походження. Ця модель є особливо релевантною для розумного міста, де інфраструктура розподілена, а взаємодія між компонентами складна і динамічна.

Основні принципи ZTA включають:

– Постійна автентифікація та авторизація кожного доступу до ресурсу.

– Мікросегментація мережі для ізоляції сервісів і мінімізації площі атаки.

– Контроль доступу на основі контексту – наприклад, місцезнаходження, типу пристрою, рівня ризику.

– Управління ідентичностями та пристроями через централізовані системи (IAM, MDM).

Впровадження Zero Trust вимагає значних організаційних змін, зокрема у підходах до побудови архітектури мережі, але водночас надає найвищий рівень контролю за інформаційними потоками та доступом до критичних ресурсів.

Успішна реалізація системи кіберзахисту розумного міста неможлива без комплексного впровадження технічних рішень, здатних не лише реагувати на вже відомі загрози, але й виявляти нові, раніше невідомі атаки. Системи IDS/IPS забезпечують первинне виявлення вторгнень, SIEM – централізований аналіз інцидентів, криптографія – захист переданої та збереженої інформації, а концепція

Zero Trust – фундаментальний зсув у моделі довіри, що відповідає сучасному урбаністичному середовищу.

В умовах міста Одеса та інших українських урбанізованих центрів з обмеженим фінансуванням впровадження подібних рішень можливе поетапно – з використанням відкритого ПЗ, адаптації під локальні потреби та створенням муніципальних центрів обробки інцидентів (SOC). Впровадження описаних технологій дозволяє підвищити стійкість критичної інфраструктури, захистити персональні дані громадян і забезпечити стабільне функціонування міських сервісів навіть в умовах кібершантажу або атак державного рівня.

3.3 Адміністративні заходи у системі кіберзахисту розумного міста: політики, навчання та аудит

Адміністративні заходи є не менш важливою складовою комплексної системи кібербезпеки, ніж технічні рішення. Вони формують організаційний каркас, який забезпечує ефективну реалізацію заходів захисту, сприяють формуванню культури безпеки серед персоналу та регламентують процедури реагування на інциденти. Впровадження відповідних політик, навчання працівників і регулярний аудит дозволяють мінімізувати людський фактор та підвищити загальний рівень готовності до кіберзагроз у контексті розумної інфраструктури міста.

1) Розробка та впровадження політик безпеки

Політики інформаційної безпеки – це формалізовані документи, які встановлюють правила, стандарти і вимоги щодо захисту інформаційних ресурсів організації. У контексті розумного міста, де взаємодіє велика кількість учасників – від адміністративного персоналу до технічних фахівців та сторонніх підрядників – чітке регулювання є критично важливим.

Основні напрямки політик включають:

- Управління доступом – визначення ролей, рівнів привілеїв і процедур авторизації користувачів.

– Політика використання паролів – встановлення мінімальних вимог до складності, регулярної зміни, заборона повторного використання.

– Робота з інцидентами безпеки – алгоритми повідомлення, розслідування, реагування та документування.

– Обробка персональних даних - відповідність законодавству, зокрема GDPR або локальним нормативам.

– Використання зовнішніх пристроїв і програмного забезпечення - правила встановлення, оновлення та моніторингу.

Важливим є забезпечення узгодженості політик з міжнародними стандартами, такими як ISO/IEC 27001, що підвищує рівень довіри з боку громадськості та партнерів.

2) Навчання та підвищення кіберкультури персоналу

Людський фактор традиційно вважається найбільш вразливим елементом у системах кібербезпеки. Навіть найкраще технічне рішення не зможе ефективно працювати, якщо користувачі нехтують елементарними правилами безпеки. Тому систематичне навчання співробітників - один з ключових адміністративних заходів.

Рекомендації щодо організації навчання:

а) Періодичність тренінгів - мінімум двічі на рік з оновленням матеріалів згідно з поточними загрозами.

б) Форми навчання - лекції, практичні семінари, онлайн-курси, симуляції фішингових атак.

в) Контроль засвоєння - тести, сертифікація, моніторинг поведінки в інформаційних системах.

г) Інформаційні кампанії - розсилки, пам’ятки, постери з базовими правилами кібергігієни.

Особливу увагу варто приділити не тільки IT-фахівцям, але й адміністративному персоналу, операторам обладнання, службам безпеки, оскільки саме вони часто є першою лінією захисту від соціальних інженерів і фішингових атак.

3) Регулярний аудит та оцінка ефективності заходів безпеки

Аудит інформаційної безпеки – це систематична, документована перевірка відповідності реального стану системи захисту встановленим політикам, стандартам та нормативним вимогам. Він дозволяє виявити слабкі місця, ризики та невідповідності, а також оцінити ефективність впроваджених заходів.

Типи аудиту:

- Внутрішній аудит - проводиться силами організації для контролю виконання власних політик.
- Зовнішній аудит - залучення незалежних експертів, що дає об’єктивну оцінку та рекомендації.
- Технічний аудит - включає перевірку мережевої безпеки, тестування на проникнення (pentesting), оцінку захищеності програмного забезпечення.
- Аудит процесів - оцінка дотримання процедур, ведення документації, реагування на інциденти.

Регулярність аудиту має бути визначена політиками безпеки, але оптимально проводити його не рідше одного разу на рік, а також після значних змін у системі або після інцидентів безпеки.

Результати аудиту повинні лягати в основу коригувальних дій, оновлення політик та навчальних програм. Важливою складовою є також автоматизоване ведення журналів подій і змін, що дозволяє оперативно виявляти порушення та відстежувати історію інцидентів.

Адміністративні заходи у системі кібербезпеки розумного міста створюють фундамент для ефективного використання технічних рішень, сприяють формуванню усвідомленої позиції серед усіх учасників міської екосистеми та забезпечують контроль за дотриманням стандартів і процедур. Розробка чітких політик, систематичне навчання персоналу та регулярний аудит не лише знижують ризики, пов’язані з людським фактором, а й забезпечують сталість роботи міських сервісів навіть в умовах постійно зростаючих кіберзагроз.

Успішна реалізація цих заходів у місті Одеса сприятиме підвищенню рівня довіри громадян до цифрових сервісів, зміцненню іміджу міста як сучасного та

безпечного урбаністичного центру, а також створенню надійної основи для подальшої цифрової трансформації.

3.4 Рекомендації щодо впровадження систем кіберзахисту для українських міст

Враховуючи стрімкий розвиток цифрових технологій і активне впровадження концепції «розумних міст» в Україні, питання кібербезпеки набувають особливої актуальності. Розумна інфраструктура передбачає високу ступінь автоматизації, інтеграції різних інформаційних систем та доступність міських сервісів через інтернет, що підвищує загальний рівень вразливості до кіберзагроз. Тому формування комплексного підходу до кіберзахисту є необхідною передумовою успішного цифрового розвитку міст.

У цьому підрозділі розглянуто ключові рекомендації для українських міст, які прагнуть забезпечити ефективний та сталий кіберзахист розумної інфраструктури.

Формування цілісної стратегії кібербезпеки на рівні міської адміністрації

Перше, що необхідно для ефективного впровадження кіберзахисту – це розробка й ухвалення стратегічного документа, який би інтегрував питання інформаційної безпеки у загальну концепцію розвитку міста. Така стратегія повинна включати:

- Оцінку поточного стану кібербезпеки міської інфраструктури;
- Визначення пріоритетних напрямків захисту;
- Визначення відповідальних структур та посадових осіб;
- Планування ресурсів, включаючи бюджет та кадровий потенціал;

Механізми взаємодії з державними органами, підприємствами, громадськими організаціями та експертним середовищем.

Важливо, щоб стратегія була гнучкою та передбачала регулярний перегляд з урахуванням нових загроз і технологічних змін.

Впровадження стандартизованих технологічних рішень з урахуванням українських реалій

Українські міста мають унікальні особливості, які впливають на вибір технологій для кіберзахисту. Це стосується як інфраструктурної бази, так і рівня технічної підготовки персоналу, а також фінансових ресурсів.

Основні рекомендації:

– Використання відкритих стандартів і платформ, що забезпечують сумісність різних компонентів розумного міста;

– Поступове оновлення застарілих систем із акцентом на безпеку (наприклад, заміна старих контролерів, підтримка сучасних протоколів шифрування);

– Впровадження рішень на основі принципу Zero Trust – відсутність довіри за замовчуванням, постійна перевірка прав доступу;

– Акцент на автоматизації моніторингу та реагування на інциденти (впровадження SIEM, IDS/IPS систем);

– Врахування можливості масштабування системи в майбутньому.

Українські розробники та IT-компанії можуть пропонувати локальні рішення, адаптовані під специфіку державного законодавства і мови, що створює додаткову цінність.

Розбудова кадрового потенціалу та підвищення кваліфікації фахівців

Одним із найбільших викликів для українських міст є нестача кваліфікованих фахівців з кібербезпеки. Тому особливу увагу варто приділяти кадровій політиці:

– Створення програм навчання та сертифікації для співробітників міських IT-служб;

– Співпраця з університетами і навчальними центрами для підготовки молодих фахівців;

– Мотивація персоналу через конкурентні умови праці, можливості кар'єрного росту та участі у профільних конференціях і семінарах;

– Підтримка культури обміну знаннями та досвідом, організація внутрішніх тренінгів та воркшопів.

Це дозволить не тільки утримати ключових фахівців, а й створити умови для безперервного підвищення рівня безпеки.

Встановлення ефективної взаємодії між учасниками кібербезпеки міста

Безпека розумного міста – це результат спільної роботи багатьох учасників: міської адміністрації, IT-підрозділів, провайдерів, правоохоронних органів та громадськості. Важливо побудувати системний механізм комунікації і обміну інформацією:

Організація спільних координаційних рад та робочих груп;

Впровадження системи оперативного обміну інформацією про кіберінциденти (CERT/CSIRT);

Підписання меморандумів про співпрацю з державними органами, зокрема кіберполіцією та СБУ;

Активне залучення громадськості через відкриті портали безпеки та інформаційні кампанії.

Такий підхід дозволить швидше виявляти загрози, координувати реагування та підвищувати загальний рівень кібербезпеки.

Забезпечення фінансування і правової підтримки

Фінансування кіберзахисту є однією з ключових складових успішної реалізації заходів. Необхідно передбачати у міських бюджетах достатні ресурси на придбання обладнання, ліцензійного програмного забезпечення, оплату праці фахівців, а також навчання персоналу.

Правова база має бути адаптована під реалії України:

Впровадження локальних нормативних актів, що регулюють кібербезпеку на муніципальному рівні;

Врахування вимог законодавства щодо захисту персональних даних;

Забезпечення механізмів відповідальності за порушення правил кібербезпеки;

Підтримка державних ініціатив та програм з кібербезпеки.

Це дозволить створити стабільне правове середовище для розвитку безпечної цифрової інфраструктури.

Етапність впровадження і постійний моніторинг результатів

Враховуючи обмежені ресурси, українським містам доцільно впроваджувати заходи кіберзахисту поетапно, починаючи з найбільш критичних елементів інфраструктури:

Спочатку слід забезпечити базовий захист мережевого обладнання та систем керування;

Далі розширювати комплекс заходів, впроваджуючи додаткові рівні контролю і моніторингу;

Регулярно оцінювати ефективність заходів за допомогою аудиту і тестування на проникнення;

Гнучко коригувати стратегію відповідно до нових викликів.

Постійний моніторинг та аналітика дозволять вчасно реагувати на інциденти та попереджати можливі загрози.

Реалізація комплексного підходу до кіберзахисту в українських містах є невідкладним завданням, що потребує узгоджених дій на багатьох рівнях – стратегічному, технологічному, організаційному та правовому. Впровадження викладених рекомендацій дозволить створити надійну і гнучку систему захисту розумної інфраструктури, що забезпечить безперервність міських сервісів, підвищить безпеку мешканців та сприятиме цифровому розвитку України загалом.

Особливо актуальним це є для міст із великим потенціалом цифровізації, таких як Одеса, Київ, Львів, Харків, де впровадження таких систем може стати прикладом для інших регіонів. Кібербезпека – це не одноразовий проект, а безперервний процес, що вимагає постійної уваги, інвестицій і розвитку.

3.5 Методичний підхід до оцінки готовності міської інфраструктури до кіберзагроз

У контексті підвищення стійкості смарт-міст до кіберзагроз важливо не лише впроваджувати захисні механізми, а й систематично оцінювати ступінь їх ефективності та готовності до реагування**.** Це передбачає використання інструментів не лише технічного аудиту, а й організаційно-практичного аналізу**,** заснованого на структурованому підході. Одним із таких інструментів є чеклист оцінки готовності**,** який можна застосовувати на рівні комунальних структур, відділів ІТ-підтримки та управлінських органів.

Запропонована методика базується на поєднанні трьох основних напрямів:

– Оцінка наявності базової кіберінфраструктури

– Виявлення прогалин у процедурному забезпеченні

– Аналіз підготовленості персоналу до реагування на інциденти

– Цілі застосування чеклиста:

– Стандартизація перевірки кіберзахисту в різних міських службах (транспорт, відеоспостереження, зв’язок)

– Визначення пріоритетних зон ризику

– Виведення стану безпеки на рівень об'єктивного контролю та вдосконалення

На відміну від класичного технічного аудиту, який вимагає фахових знань і часу, чеклист може бути впроваджений як інструмент регулярної внутрішньої перевірки, у тому числі – несертифікованим персоналом за участі консультанта. Це розширює можливості моніторингу навіть у невеликих муніципалітетах з обмеженими ресурсами.

Заповнення даного чеклиста може виконуватися періодично (наприклад, раз на квартал) і слугувати основою для внутрішніх аудитів або підготовки до зовнішніх перевірок. На підставі результатів формується перелік коригуючих заходів**,** кожен з яких повинен мати відповідального виконавця та дедлайн. Таким чином, методика набуває циклічного характеру: перевірка – усунення – перевірка.

Таблиця 3.1 – Чеклист оцінки кіберготовності міської інфраструктури (Smart City)

№	Критерій	Так / Ні / Частково	Коментар / Примітка
1	Впроваджено політику оновлення IoT-пристроїв		
2	Усі пристрої захищено унікальними паролями		
3	Встановлено багатофакторну автентифікацію для адміністративного доступу		
4	Обмежено прямий доступ до критичних вузлів з публічного інтернету		
5	Налагоджено централізований збір логів (SIEM або аналог)		
6	Проводиться щонайменше один тест на проникнення на рік		
7	Визначено відповідального(-их) за інформаційну безпеку в організації		
8	Наявна інструкція з реагування на кіберінциденти		
9	Персонал проходить регулярне навчання з кібергігієни та розпізнавання соціальної інженерії		
10	Ведеться облік і контроль підключених IoT-пристроїв у мережі		
11	Впроваджено регулярне резервне копіювання даних		
12	Здійснюється сегментація мережі між критичними та публічними ресурсами		

Порівняння з міжнародною практикою

Структура даного чеклиста адаптована під принципи стандартів ISO/IEC

27001**,** а також підходу NIST Cybersecurity Framework**,** зокрема таких функцій як *Protect*, *Detect* і *Respond*. Це робить її застосовною не лише в Україні, але й на рівні інтеграції з міжнародними рекомендаціями з кіберзахисту.

Розроблена методика перевірки кіберготовності є універсальним інструментом для швидкої та системної оцінки поточного стану цифрової безпеки смарт-міста. Її застосування дозволяє не лише виявити критичні прогалини, а й формалізувати процеси безпеки як частину управлінської культури муніципалітету. У поєднанні з алгоритмом реагування та моделюванням інцидентів, цей підхід забезпечує цілісний контур кіберзахисту в умовах сучасного цифрового середовища.

3.6 Алгоритм реагування на кіберінциденти в інфраструктурі Smart City

Оцінка поточного рівня захищеності розумного міста, яку можна здійснити за допомогою чеклиста, є лише першим кроком у побудові стратегії кіберзахисту. Не менш важливо – мати чіткий та стандартизований алгоритм дій у разі виявлення кіберінциденту**,** що забезпечить швидку локалізацію загрози, зменшення шкоди та мінімізацію простоїв критичних сервісів міста.

Сучасна смарт-інфраструктура включає в себе IoT-пристрої, SCADA-системи, комунікаційні вузли та безліч сервісів, що функціонують у реальному часі. Навіть короткочасний збій чи проникнення в одну з частин системи може мати ланцюговий ефект для всієї міської екосистеми. Тому реагування повинне бути негайним, структурованим та повторюваним**.**

У цій частині роботи запропоновано базовий алгоритм реагування на кіберінциденти**,** що складається з семи послідовних етапів. Він може адаптуватися під структуру IT-служб конкретного міста, а також інтегруватися у політики безпеки міських департаментів.

Етапи алгоритму реагування:

1) Виявлення інциденту:

Аномалії в роботі системи можуть бути зафіксовані вручну (технічним персоналом) або автоматично (системами моніторингу – IDS, SIEM). Важливо забезпечити постійне логування та зберігання даних про всі події.

2) Класифікація загрози:

Визначається характер інциденту (DDoS, SQL-ін'єкція, злам IoT-пристрою тощо), обсяг потенційної шкоди, критичність компоненту, який постраждав. Інциденту присвоюється пріоритет.

3) Ізоляція ураженого сегменту:

Якщо є підозра на активну загрозу – уражену частину мережі ізолюють. Це може бути тимчасове вимкнення пристрою, блокування порту або відключення від центрального вузла.

4) Оповіщення відповідальних осіб:

Одразу після класифікації та ізоляції повідомляються відповідальні фахівці: адміністратори, керівники IT-підрозділу, іноді – служби CERT-UA.

5) Аналіз причин і масштабів:

Виконується глибокий аналіз журналів, логів, трафіку. Визначається джерело, тривалість, вразливості, якими скористався зловмисник.

6) Усунення наслідків і відновлення:

Після усунення загрози відновлюється працездатність систем. Важливо не лише перезапустити сервіси, а й усунути першопричини (наприклад, оновити прошивку, змінити паролі, закрити порти).

7) Документування інциденту:

Складається звіт про інцидент, вносяться зміни до політик кіберзахисту, проводиться короткий брифінг з персоналом. Усі заходи фіксуються для внутрішнього обліку та подальшого вдосконалення процедури реагування.

3.7 Приклад застосування методики реагування на кіберінцидент в умовах смарт-інфраструктури Одеси

Наявність формалізованої методики реагування на інциденти є лише частиною ефективного захисту. Не менш важливо – вміти оперативно застосувати її на практиці**,** адаптувавши до конкретних умов інфраструктури, яка постраждала. Нижче розглядається умовна, але технічно обґрунтована симуляція**,** яка ілюструє типовий сценарій кібератаки на компоненти цифрового середовища смарт-міста.

Умова ситуації

Увечері, в години пік, відбувається раптове порушення роботи міської транспортної системи в Одесі. Смарт-світлофори на кількох перехрестях відмовляються працювати за встановленими сценаріями, спостерігається неконтрольована зміна режимів, а в логах реєструється незвичний потік вхідних запитів із зовнішніх IP-адрес. У той же час веб-панель керування для оперативного моніторингу виявляється недоступною.

Можливі наслідки:

- Паралізація трафіку на критичних розв'язках
- Неможливість ручного втручання в роботу світлофорів
- Поширення аномалії на сусідні райони через взаємозв'язок систем

Застосування методики реагування

1) Виявлення:

Інцидент виявлено автоматично через систему моніторингу логів та збоїв. Від IT-відділу надходить повідомлення про нестабільну поведінку інтерфейсу керування.

2) Класифікація:

Ідентифіковано підозрілу DDoS-атаку на API смарт-світлофорів. Вразливими виявилися порти, що залишались відкритими для публічного доступу без VPN.

3) Ізоляція:

Тимчасово відключено шлюз маршрутизатора, через який проходив трафік. Ізольовано комунікацію смарт-світлофорів із хмарним контролером.

4) Оповіщення:

Інцидент задокументовано й передано у CERT-UA, локальні структури ДСНС та управління «Центр 077».

5) Аналіз:

Встановлено, що частина пристроїв працювала зі стандартною конфігурацією, а паролі до адмін-панелі не змінювались понад рік.

6) Усунення:

Проведено перезапуск систем, оновлено прошивки, реалізовано VPN-тунелі для віддаленого доступу до обладнання.

7) Документування:

Оформлено звіт. За підсумками випадку рекомендовано затвердити регулярну ротацію паролів, сегментацію мережі та впровадження додаткової системи виявлення аномалій на рівні каналу.

Для кращого розуміння логіки дій при інциденті, пов’язаному з цифровою інфраструктурою міста, нижче подано схему, що візуалізує послідовність реагування, описану в цьому підрозділі. Схема умовно ілюструє сценарій DDoS-атаки на систему смарт-світлофорів, застосовану до кейсу міста Одеса.

Рисунок 3.1 – Схема реагування на кіберінцидент у системі смарт-інфраструктури міста Одеса

Таким чином, навіть умовна симуляція кіберінциденту демонструє важливість не лише технологічного захисту, а й організаційної готовності служб міста. Запровадження формалізованого алгоритму реагування, регулярний аудит конфігурацій та протоколів доступу, а також навчання персоналу можуть суттєво зменшити потенційні ризики та втрати внаслідок кіберзагроз. Симульований сценарій доводить, що ефективність захисту залежить не лише від інструментів, а й від структури процесів прийняття рішень**.**

ВИСНОВКИ

У процесі виконання дипломної роботи на тему «Методи захисту розумних міст від кібератак» було проведено комплексне дослідження теоретичних і практичних аспектів кібербезпеки в умовах цифровізації міської інфраструктури. З урахуванням стрімкого впровадження технологій Smart City у багатьох містах світу, включно з Україною, питання кіберзахисту стало критично важливим і багаторівневим викликом як для фахівців у галузі інформаційної безпеки, так і для муніципального управління.

У першому розділі було розглянуто сутність концепції «розумного міста», описано його архітектуру, ключові технологічні складові (IoT, сенсорні мережі, дата-центри, хмарні платформи) та принципи функціонування. Проаналізовано типові кіберзагрози для смарт-інфраструктури: несанкціонований доступ до пристроїв, DDoS-атаки, компрометація хмарних сервісів, уразливості IoT-платформ, соціальна інженерія тощо. Окрему увагу приділено методам протидії загрозам, серед яких – використання міжмережевих екранів, систем виявлення атак, шифрування, мережевої сегментації та міжнародних стандартів кіберзахисту (ISO, NIST, Zero Trust).

У другому розділі виконано аналітичний огляд впровадження Smart City в Україні. Розглянуто приклади з Києва, Львова, Дніпра, Харкова, а також зроблено акцент на ситуації в місті Одеса. Установлено, що хоча цифрові технології активно впроваджуються, рівень їх захисту часто залишається недостатнім. Серед основних проблем виявлено: фрагментарність впровадження, відсутність цілісної стратегії кібербезпеки, низький рівень оновлення пристроїв, брак кадрової підготовки, нормативно-правові прогалини, обмежене фінансування заходів інформаційної безпеки на місцевому рівні.

У третьому розділі було представлено систематизований підхід до формування базових рекомендацій щодо побудови системи кіберзахисту смарт-інфраструктури. Запропоновано алгоритм реагування на інциденти безпеки, структуру дій для міських служб, а також рекомендації щодо проведення базової

оцінки поточного рівня захисту на рівні муніципалітету. Враховано технічні й організаційні аспекти захисту, адаптовані до умов функціонування українських міст.

Загалом, у роботі:

– обґрунтовано актуальність і складність захисту цифрової міської інфраструктури;

– проаналізовано типові кіберзагрози для Smart City;

– вивчено стан впровадження та захисту смарт-технологій в Україні;

– виокремлено основні проблеми кіберзахисту на прикладі міста Одеса;

– розроблено узагальнені рекомендації з організації базових механізмів безпеки.

Таким чином, поставлена мета дипломної роботи була досягнута, а завдання – виконані. Робота має як аналітичну, так і практичну цінність, і може бути використана як основа для подальших досліджень або розробки внутрішніх політик безпеки на рівні органів місцевого самоврядування в умовах цифрової трансформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII Дата оновлення 20.04.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. Указ Президента України № 447/2021 «Про Стратегію кібербезпеки України» від 26.08.2021 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 28.03.2025).
3. ISO/IEC 27001:2013. Information security management systems – Requirements [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/54534.html (дата звернення: 09.04.2025).
4. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity [Електронний ресурс]. – Режим доступу: https://www.nist.gov/cyberframework (дата звернення: 01.03.2025).
5. OWASP IoT Top Ten 2022 [Електронний ресурс]. – Режим доступу: https://owasp.org/www-project-internet-of-things/ (дата звернення: 19.01.2025).
6. Струк А. О. Кібербезпека: методи захисту інформаційних систем: навч. посіб. – Київ: НаУКМА, 2020. – 142 с.
7. Грищенко А. М. Інформаційна безпека в IT-системах: навч. посіб. – Харків: ХНУРЕ, 2021. – 160 с.
8. Cisco Systems. Smart City Security Guidelines: White Paper [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities.html (дата звернення: 05.04.2025).
9. IBM X-Force Threat Intelligence Report: Smart Cities under Attack. IBM Corporation, 2022 [Електронний ресурс]. – Режим доступу: https://www.ibm.com/reports/threat-intelligence (дата звернення: 17.01.2025).
10. Microsoft. Securing Smart Cities: Best Practices [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/security/smart-cities-security (дата звернення: 12.02.2025).

11. European Union Agency for Cybersecurity (ENISA). Good Practices for Smart Cities [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/good-practices-for-smart-cities (дата звернення: 29.03.2025).
12. Gartner. Top Cybersecurity Trends in Smart Infrastructure. Research Report, 2023 [Електронний ресурс]. – Режим доступу: https://www.gartner.com/en/documents/40000-top-cybersecurity-trends (дата звернення: 20.01.2025).
13. Хакери намагалися отруїти воду у США // Українська правда [Електронний ресурс]. – Режим доступу: https://www.pravda.com.ua/news/2021/02/9/7284044/ (дата звернення: 23.01.2025).
14. Державна служба спеціального зв'язку та захисту інформації України. Рекомендації для органів місцевого самоврядування щодо захисту інформаційної інфраструктури [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua/news/rekomendatsii-dlya-organiv-miscevogo-samovryaduvannya (дата звернення: 08.03.2025).
15. Smith R. Internet of Things Security. – New York: Springer, 2020. – 198 p.
16. Cyberthreats in Smart Cities: Global Overview / Kaspersky Lab [Електронний ресурс]. – Режим доступу: https://www.kaspersky.com/blog/smart-city-cybersecurity/ (дата звернення: 03.03.2025).
17. IBM. Smart City Cybersecurity Threats [Електронний ресурс]. – Режим доступу: https://www.ibm.com/topics/smart-city-security (дата звернення: 26.01.2025).
18. Cisco Annual Cybersecurity Report 2023: Global Threat Landscape [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/security/annual-cybersecurity-report.html (дата звернення: 16.04.2025).
19. ENISA. Smart Cities Threat Landscape [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/threat-landscape-smart-cities (дата звернення: 19.02.2025).

20. NIST. IoT Device Cybersecurity Guidance [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-213/final (дата звернення: 11.01.2025).
21. OWASP. Top IoT Security Threats [Електронний ресурс]. – Режим доступу: https://owasp.org/www-project-top-ten/2017/A10_2017-Insufficient_Logging%26Monitoring.html (дата звернення: 25.03.2025).
22. Microsoft Defender for IoT. Smart Infrastructure Overview [Електронний ресурс]. – Режим доступу: https://azure.microsoft.com/en-us/products/defender-for-iot (дата звернення: 14.04.2025).
23. Cisco Smart+Connected Digital Platform [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities/overview.html (дата звернення: 04.01.2025).
24. Gartner. Smart City Security Challenges Report [Електронний ресурс]. – Режим доступу: https://www.gartner.com/en/insights/smart-cities (дата звернення: 27.03.2025).
25. Інститут модернізації змісту освіти. Захист критичної інфраструктури: навчальні матеріали [Електронний ресурс]. – Режим доступу: https://imzo.gov.ua/wp-content/uploads/2023/07/InfrastructureSecurityGuide.pdf (дата звернення: 09.03.2025).
26. McKinsey & Company. Smart Cities: Digital Solutions for a More Livable Future [Електронний ресурс]. – Режим доступу: https://www.mckinsey.com/business-functions/smart-cities (дата звернення: 02.04.2025).
27. Amazon AWS IoT Security Whitepaper [Електронний ресурс]. – Режим доступу: https://docs.aws.amazon.com/whitepapers/latest/iot-security-best-practices (дата звернення: 28.02.2025).
28. ISO/IEC 30141:2018. Internet of Things (IoT) – Reference architecture [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/65695.html (дата звернення: 06.03.2025).

29. OECD. Smart Cities and Cybersecurity Policy Paper [Електронний ресурс]. – Режим доступу: https://www.oecd.org/digital/smart-cities-cybersecurity (дата звернення: 10.01.2025).
30. Google Cloud. Smart City Cybersecurity Guidelines [Електронний ресурс]. – Режим доступу: https://cloud.google.com/solutions/smart-cities/security (дата звернення: 21.02.2025).
31. Центр кіберзахисту ДССЗЗІ. Рекомендації з кібергігієни для органів влади [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua/guidelines (дата звернення: 07.02.2025).