

ПРОБЛЕМАТИКА ПОБУДОВИ КОНЦЕПЦІЇ «РОЗУМНОГО МІСТА»

Іван Опірський, Олег Тютіков

Використання штучного інтелекту дозволяє максимально автоматизувати усі процеси, які керують системами розумного міста. Використання такої системи виключає можливість несанкціонованого доступу до даних системи розумного міста через найуразливішу точку - людський фактор. Для побудови систем розумного міста, захисту даних та збереження конфіденційності необхідно розробити засоби захисту від витоку інформації. Існує ряд проблем та загроз, зокрема одні із них, це - кібератаки, атаки, які спроможні заблокувати рух машин перемиканням світлофору, перехопити сигнал приватних та публічних камер, комутаційних мереж таких як Wi-Fi, 4G/5G, RFID, GSM та інші, перекрити доступ подачі води, газу та електроенергії жилим будинкам. Проте, системи розумного міста дозволяють підвищити рівень логістики шляхом встановлення датчиків на дорогах, безпеки, встановлюючи камери відеонагляду в громадському транспорті, захист кожної покупки або обміну, економії ресурсів води, газу, електроенергії та захищеності у місті. Також це стосується і загального «розумного» розвитку людини, яка буде володіти електронними навичками. У цій статті розкрито проблематику створення такої системи розумного міста, представлено основні загрози з точки зору побудови систем «розумного міста». Наведено переваги та недоліки таких систем. Наведено основні концепції з побудови нових систем «розумного міста», зокрема місце штучного інтелекту у них.

Ключові слова: «розумне місто», smart city, штучний інтелект, кібератака, IoT, безпека, конфіденційність.

Вступ. Метою створення розумного міста є покращення та спрощення управління містом, благоустрій міського середовища, забезпечення безпеки та підвищення якості життя жителів міста.

Розумне місто – це структура, що складається переважно з інформаційних та комунікаційних технологій (ІКТ) для розробки, розгортання та просування практики сталого розвитку для вирішення завдань урбанізації. Значна частина цієї ІКТ-базису по суті є інтелектуальною мережею підключених об'єктів і машин, які передають дані за допомогою бездротової технології та хмари. Хмарні програми IoT отримують, аналізують та керують даними в режимі реального часу, щоб допомогти муніципалітетам, підприємствам та громадянам приймати кращі рішення, які покращують якість життя.

Громадяни взаємодіють із розумними екосистемами міста різними способами за допомогою смартфонів та мобільних пристроїв, а також підключених автомобілів та будинків. Парування пристроїв та даних із фізичною інфраструктурою та послугами міста може зменшити витрати та покращити стійкість.

Переваги впровадження розумного міста.

Громади можуть покращити розподіл енергії, упорядкувати збирання сміття, зменшити затори транспортних потоків і навіть покращити якість повітря за допомогою IoT. Наприклад:

– Підключені світлофори отримують дані від датчиків та автомобілів, регулюючи світлову частоту та час реагування на рух у режимі реального часу, тим самим зменшуючи затори на дорогах.

– Підключені автомобілі можуть «спілкуватися» з лічильниками паркування та док-станціями для зарядки електромобілів та направляти водіїв до найближчого доступного місця.

– Розумні сміттєві баки автоматично надсилають дані компанії з управління відходами та розкладають графіки за необхідністю порівняно із заздалегідь запланованим графіком.

– Смартфон громадян стає їх водійським посвідченням та посвідченням особистих даних із цифровими обліковими даними, що прискорює та спрощує доступ до послуг міста та місцевої влади.

– Разом ці розумні міські технології оптимізують інфраструктуру, мобільність, суспільні послуги та комунальні послуги [1].

Такі системи успішно існують та розвиваються в таких містах як Нью-Йорк, Лондон, Париж, Токіо, Торонто, Гонконг.

Наприклад уже другий рік поспіль, Нью-Йорк очолив список лідерів, як одне з найбільш розвинених розумних міст в світі. Маючи населення, яке перевищує 8,5 мільйонів, Нью-Йорк вживає 1 мільярд галонів води щодня. В рамках свого інтелектуального плану міста, Департамент міста по

охороні навколишнього середовища розгортає великомасштабну систему автоматизованого зчитування лічильників, щоб отримати кращий знімок споживання води, в той час надаючи клієнтам корисний інструмент для перевірки їх використання води щодня. Місто також звернулося до «розумних» смітників, що працюють на сонячній батареї Bigbelly, які відстежують рівень сміття та забезпечують регулярне збирання відходів [2].

Основні складові розумного міста. Розумні міста мають справу з величезною кількістю даних у реальному часі та пов'язаних з ними технологій, що є керованими даними технологіями які діють, генерують, обробляють, запускають та виробляють дані. Розумні міста мають багато ресурсів для виробництва різних типів даних. Ці системи широко поширені в розумних містах, і отримані ними дані називаються великими даними. Інші системи перетворюють малі і звичайні дані в інфраструктурні набори даних, які використовуються декількома способами. Є системи, які роблять заблоковані дані доступними для публічних відкритих даних [3].

Ще однією системою, є системи, пов'язані з машинним навчанням, які розробляють та аналізують дані. Усі ці міські дані використовуються для управління розумними міськими технологіями, тому важливо захистити їх величезну кількість. Крім того, необхідно підтримувати конфіденційність заблокованих даних і особистих даних та переконатися в тому, що до них не вдалося навмисно чи випадково звернутися або отримати доступ до них. Конфіденційність забезпечується захищаючи п'ять питань, пов'язаних з конфіденційністю:

- захист ідентичності, що вказує на захист персоналу та їх особи;
- захист простору та права кожного; захищаючи місця, які вказують на запобігання просторового відстеження;
- захист зв'язку, який вказує на те, що не підслуховується жодного виду розмов;
- захист транзакцій, який захищає кожен покупок, обмін та запит.

Тому, можна виділити ось такі основні складові розумного міста:

- Розумний уряд: приватні, публічні і цивільні організації, інфраструктури, уряд, комунальні послуги.
- Розумна економіка: електронний бізнес, комерція, виробництво.
- Розумні люди: люди з електронними навичками.

– Розумна мобільність: транспорт, логістика, трафік.

– Розумний спосіб життя: розумне споживання, стабільна поведінка.

– Розумне управління енергією: вода та відходи, чисте навколишнє середовище, контрольоване забруднення.

Проблематика безпеки та конфіденційності. Безпека та конфіденційність - завжди гарячі теми для обговорення. Для розумного міста питання безпеки та конфіденційності ще більше важливіше, ніж для будь-яких технологічних явищ, оскільки кількість розумних міст швидко збільшується. Таким чином, дослідники повинні приділяти більше уваги, щоб питання безпеки та конфіденційності у розумних містах мали для цього збагатити літературу більшістю досліджень у цьому плані [4]. Для нашої роботи ми розглянули дослідження загроз розумного міста, які обговорюють проблеми безпеки та конфіденційності та пов'язані з цим проблеми. У дослідженні представлено розумне місто, як найсучасніший збір інформаційно-комунікаційних технологій, де обговорюються сучасні міські проблеми та сучасні міські технології. Крім цього уточнено поточні ризики та невизначеності у розумних містах шляхом визначення шести сценаріїв міст, які заявляються розумними. Це також говорить про нове бачення Cloud of Things (CoT), що є інтеграцією між Інтернетом речей (IoT) та наукою хмарних обчислень; і в ньому обговорюється, як послуги розумних міст можна надавати на основі Cloud of Things.

Дослідницька компанія Juniper Research і Intel дослідили проблеми безпеки та конфіденційності, запропонували модель, яка є основним елементом розумних міст (сервери, люди та речі) та взаємодією між ними, активно обговорюються питання положення про порушення безпеки та конфіденційності, і вони стверджують, що ці норми не відповідають важливості та критичності питань безпеки та конфіденційності.

Відомо, що розумні міста надають користувачам величезні переваги, але при цьому користувачі турбуються про свої конфіденційні дані, які передаються через незахищені канали. Таким чином, необхідно забезпечити канали зв'язку і забезпечити безпечний носій для переміщення даних спеціально по бездротовим мережам.

Загрози для розумного міста.

Міська інфраструктура, така як електропостачання, розподіл води, вулиці, будівлі та інші [5] стикаються з кількома загрозами безпеки у своїх

конкретних кіберфізичних компонентах та системах зображено схематично (рис. 1):

– камери: у містах повно приватних і публічних камер, які захищені варіативно, використовуючи шифрування даних та захист імені користувача і пароля. Досягнення приватних або публічних камер та доступ до них порушує конфіденційність приватних осіб та слідкують за проблемами уряду;

– комунікаційні мережі: кіберфізичні об'єкти з'єднані разом уздовж розумного міста за допомогою декількох комунікаційних технологій, такі як Wi-Fi, 4G, RFID, GSM та інші. Кожен з яких має специфіку проблеми безпеки, які слід сприймати під час використання комунікаційних технологій;

– системи управління будівлями: дизайнери та розробники таких систем зазвичай зосереджуються на наданому сервісі нехтуючи питаннями кібербезпеки. Таким чином, в таких системах відсутня опція сповіщення користувачів про порушення безпеки та реагування на них, в результаті чого створюються системи управління будівлями, які є незахищеними та слабо захищеними;

– системи управління транспортом: такі системи стикаються з найбільш критичними зламами, оскільки вони спричиняють катастрофи з

системами повітряного руху або системами управління поїздами. Більше того, вони викликають величезні затори, які можуть тривати годинами при зломі систем керування світлофорами та їх послідовностями, дорожніми знаками та знаками обмеження швидкості.

Основні концепції майбутніх розробок концепцій «розумного міста». Міська влада не повинна бути єдиним інвестором та оператором усіх типів послуг та інфраструктури. Державне фінансування може бути використане лише для тих суспільних благ, які повинні бути надані урядом. Схему фінансового розподілу представлено графічно (рис. 2). Крім того, більше половини початкових інвестицій, які потребує державний сектор, призведе до позитивного фінансового прибутку, що відкриває двері до партнерських відносин.

Також хочемо виділити алгоритми штучного інтелекту (AI), які стають невід'ємною частиною ініціативи Smart City, спрямованих на автоматизацію та вдосконалення широкого кола муніципальних заходів та операцій. Ці програми сильно відрізняються залежно від конкретного випадку, але більшість із них, як правило, поділяють цілі покращення умов життя, підвищення міст більш конкурентоспроможними та екологічно стійкими [6].

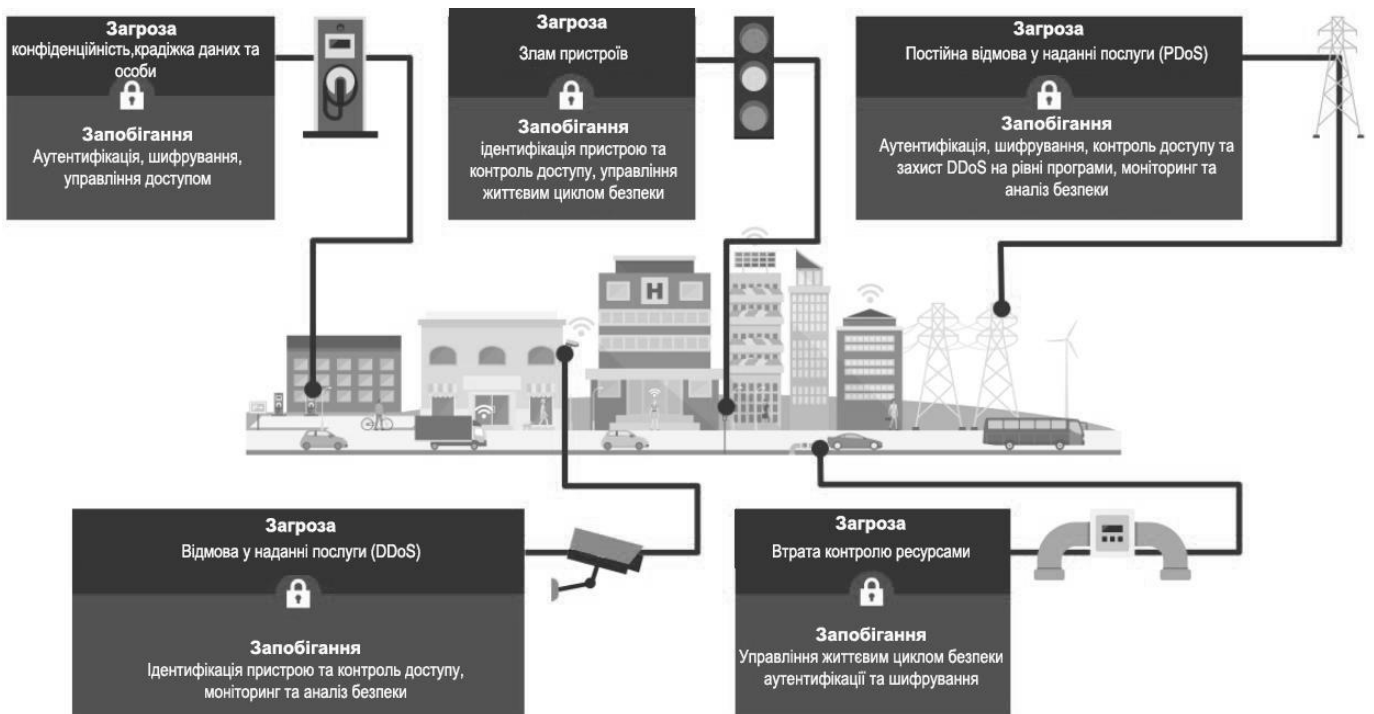
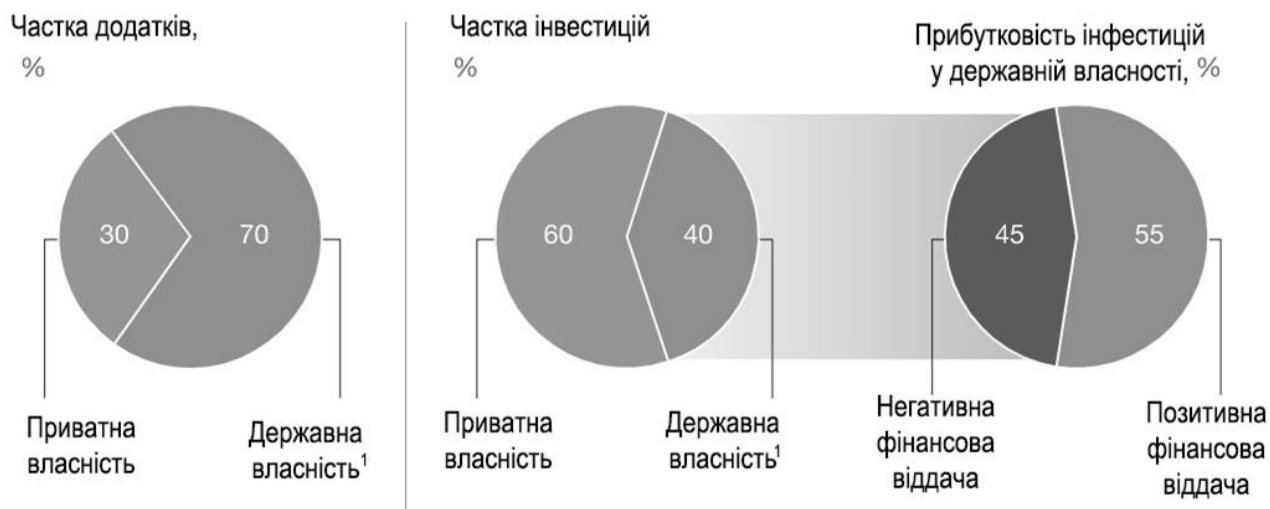


Рис. 1 Схема загроз для розумного міста

Державний сектор був би природним власником більшості додатків розумного міста, але більшість інвестицій може бути отримана від приватних суб'єктів



¹ Енергетика, вода, комунальні послуги, оператори громадського транспорту та лікарні

Рис. 2 Схема фінансового розподілу

Певною мірою планувальники працюють над покращенням цих показників до тих пір, поки існують міста. Тепер вони просто застосовують новітні технології до цих проблем. Наприклад, будівельники створювали та розширювали вулиці, щоб зменшити затори або будували парки для поліпшення життєдіяльності у містах протягом десятків років. І одним з найдавніших прикладів використання комп'ютерних технологій в управлінні містами був Лос-Анджелес, починаючи з 1960-х, коли інженери використовували бази даних та аерофотозйомку для відстеження демографічних тенденцій та оцінки якості житла.

Але сучасна ініціатива розумного міста - це не просто "містобудування плюс цифрова технологія", або навіть "містобудування плюс Інтернет". Сучасний поштовх до розумних міст розпочався у 2005 році, коли Фонд Клінтон заручився допомогою Cisco для покращення сталого розвитку міст. Використовуючи грант від фонду, Cisco запустив Програму зв'язаного містобудування спільно з Сан-Франциско, Амстердамом та Сеулом. Їх реалізація концепції була зосереджена на вдосконаленні широкопasmової інфраструктури та обміні даними, зокрема, щоб допомогти містам зменшити рівень CO₂.

Наступний великий учасник цього сектора був у 2008 році, коли ІВМ запустила свою групу Smarter Planet для дослідження використання датчиків, мереж та аналітики для досягнення економічного зростання, ефективності, сталого розвитку та суспільного прогресу.

По мірі підтримки таких технологій, як Інтернет речей, енергоефективне світлодіодне освітлення та хмарні обчислення, ми побачили широке поширення недорогих датчиків, загальноміського Wi-Fi та економічно вигідного освітлення, які зробили великий внесок у міські програми. Зростання хмарних обчислень також дозволило містам масштабувати аналітику та значно спростило придбання цих складних систем.

Зараз ми спостерігаємо останні великі сили для ініціатив Smart City у формі штучного інтелекту. AI дає комп'ютерам можливість бачити, чути, рухатися та міркувати. Наприклад, системи комп'ютерного зору, що працюють на AI, можуть дозволяти комп'ютерам одночасно ідентифікувати мільйони елементів міського життя, таких як люди, машини, громадські працівники, сміття, аварії, пожежі, катастрофи тощо. Система могла допускати не лише автономний моніторинг, але й прийняття рішень на основі того, як поводить себе кожен з цих елементів, як поведінка змінюється протягом дня або з часом, і як елементи реагують на міські системи. Простіше кажучи, AI зрозуміє, як використовувати міста та як ними функціонувати, і може допомогти планувальникам зрозуміти, як місто реагує на різні зміни та ініціативи.

Поточні програми розумного міста, що використовують AI, включають вдосконалення управління дорожнім рухом та паркуванням. Майбутні програми можуть включати безпечну інтеграцію автономних транспортних засобів. Але є певна темна сторона щодо потенціалу AI у містобудуванні

– і така перспектива використовувати моніторинг AI жителів для контролю поведінки через страх покарання.

Впровадження Китаєм своєї системи соціального кредитування - саме таке починання. Використовуючи технологію розпізнавання обличчя для ідентифікації окремих громадян, їх система зможе визначити поведінку, таку як не оплата квитків на поїзд чи автобус, нерозумність, грубіянство або спричинення суєти. Порушення правил призведе до того, що бали віднімаються від оцінки соціального кредиту громадянина. Спочатку кожен урядовий департамент та міське агентство матимуть власну систему соціального кредитування - орган з паркування надасть кредитні бали за порушення паркування, тоді як транзитна система встановить пункти для порушення правил громадського транспорту. Але мета Китаю - приєднати ці системи до Універсальної системи соціального кредитування - там, де порушення в одній сфері може призвести до втрати можливості в суспільстві в іншій галузі. Якщо ви не сортуєте сміття правильно або не сплачуєте податки вчасно, ви можете втратити роботу або освітні можливості, права на поїздки або час відпустки. Наслідки лякають.

Хоча вже багато написано на цю тему, і можна з упевненістю сказати, що між авторитарним Китаєм і демократичним Заходом велика різниця, але будь-яке обговорення впровадження штучного інтелекту міськими урядами - незалежно від того, наскільки благородним у своїх цілях - повинно включати усвідомлення цих потенційних недоліків. Це створює проблеми, лише в тому випадку, якщо воно може послужити відверненню людей від неймовірних можливостей покращити не тільки ефективність, якість життя та стійкість за допомогою технології AI, але і свободи людини та права людини. Зараз декілька програм у США зосереджені на моніторингу поліції за допомогою систем AI, щоб гарантувати, що взаємодія між поліцією та громадянами є законною, а також захищені права поліції та громадянина.

Насправді найбільшим сучасним випадком використання в програмах розумних міст в усьому світі є системи візуального спостереження, а інші два - це громадський транспорт та розумне зовнішнє освітлення. Ці три області разом становлять майже 25% загальних витрат на розумні міста.

Нещодавно International Data Corporation (IDC) опублікував своє останнє керівництво витратами на розумні міста та підрахував, що у 2018 році понад 81 мільярд доларів буде витрачено на ініціативи Smart City та очікує, що це зросте до 158 мільярдів доларів до 2022 року.

Зараз у містах проживає понад 50% світового населення, і прогнозується, що він зросте до двох третин до 2050 року. З точки зору викидів вуглецю, тоді як міста займають лише 2% світової суші, вони несуть відповідальність за понад 70% викидів CO₂ в усьому світі. Потрібні інноваційні технологічні рішення для того, щоб урбанізація могла продовжуватись здійснюватися безпечним, ефективним та здоровим для нас та для планети шляхом. Посадження AI, датчиків, хмарних обчислень, що працюють рука об руку, з чіткими законами про конфіденційність та жорстким визначенням прав людини, дасть нам справді розумні міста, які можуть слугувати основою для зростання та процвітання людини.

ЛІТЕРАТУРА

- [1]. M. Batty, "Geocomputation. Environment and Planning B", *Urban Analytics and City Science*, 44(4):pp. 595-597, 2017.
- [2]. *New York City*. [Електронний доступ]. Режим доступу: <https://www.gigabitmapagazine.com/big-data/top-10-smart-cities-world>.
- [3]. *Основні складові розумного міста*. [Електронний доступ]. Режим доступу: <https://www.smartcitiesworld.net/special-reports/pain-points-politics-and-the-future-of-transport>.
- [4]. *Проблематика безпеки та конфіденційності*. [Електронний доступ]. Режим доступу: <https://media.iese.edu/research/pdfs/ST-0471-E.pdf>.
- [5]. *Загрози для розумного міста*. [Електронний доступ]. Режим доступу: <https://www.rambus.com/iot/smart-cities/>.
- [6]. *Штучний інтелект в розумних містах*. [Електронний доступ]. Режим доступу: <https://medium.com/neuromation-blog/ai-in-smart-cities-dfe2fa7d2829>.
- [7]. O. Milov, A. Voitko, I. Husarova, O. Domaskin, Y. Ivanchenko, I. Ivanchenko, O. Korol, H. Kots, I. Oprisky, O. Frazze-Frazenko, "Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems", *Eastern-european journal of enterprise technologies. Information and controlling system*, Vol 2, No. 9(98), pp. 56-66, 2019. DOI: <https://doi.org/10.15587/1729-4061.2019.164730>.

ПРОБЛЕМАТИКА ПОСТРОЕНИЯ КОНЦЕПЦИИ «УМНОГО ГОРОДА»

Использование искусственного интеллекта позволяет максимально автоматизировать все процессы, которые управляют системами умного города. Использование такой системы исключает возможность несанкционированного доступа к данным системы умного города через уязвимую точку - человеческий фактор. Для построения систем умного города, защиты данных и конфиденциальности необходимо разработать средства защиты от утечки информации. Существует ряд проблем и угроз, в том числе одни из них, это - кибератаки, атаки, которые способны заблокировать движение машин переключением светофора, перехватить сигнал частных и публичных камер, коммутационных сетей таких как Wi-Fi, 4G / 5G, RFID, GSM и другие, перекрыть доступ подачи воды, газа и электроэнергии жилым домам. Однако, системы умного города позволяют повысить уровень логистики путем установки датчиков на дорогах, безопасности, устанавливая камеры видеонаблюдения в общественном транспорте, защиту каждой покупки или обмена, экономии ресурсов воды, газа, электроэнергии и защищенности в городе. Также это касается и общего «умного» развития человека, который будет обладать электронными навыками. В этой статье раскрыты проблематику создания такой системы умного города, представлены основные угрозы с точки зрения построения систем «умного города». Приведены преимущества и недостатки таких систем. Приведены основные концепции по построению новых систем «умного города», в частности место искусственного интеллекта в них.

Ключевые слова: «умный город», smart city, искусственный интеллект, кибератака, IoT, безопасность, конфиденциальность.

PROBLEM OF CONSTRUCTION OF THE CONCEPT OF "SMART CITY"

The use of artificial intelligence allows you to automate as much as possible all the processes that control the systems of a smart city. Using such a system eliminates the possibility of unauthorized access to the data of the smart city system through a vulnerable point - the human factor. To build smart city systems, data protection and privacy, it is necessary to develop means of protection against information leakage. There are a number of problems and threats, including one of them - cyber attacks, attacks that can block the movement of cars by switching traffic lights, intercept the signal of private and public cameras, switching networks such as Wi-Fi, 4G / 5G, RFID, GSM and others, block access to the supply of water, gas and electricity to residential buildings. However, smart city systems can improve the level of logistics by installing

sensors on the roads, security, installing CCTV cameras in public transport, protecting every purchase or exchange, saving water, gas, electricity and security in the city. This also applies to the general "smart" development of a person who will possess electronic skills. This article reveals the problems and features of creating a system of "smart city". Analysis of the "smart city" systems made it possible to identify the main threats from the point of view of building "smart city" systems - threats to confidentiality, data theft, evil devices, the constant denial of access, the denial of service, the loss of control over resources. An analysis of the threats presented allowed us to introduce methods by which we can secure the systems of the "smart city". The article also describes the advantages and disadvantages of such systems. The analysis of financial distribution from the side of the state and private organizations for the construction of smart city systems was carried out. The basic concepts for building new systems of the "smart city", in particular, the place of artificial intelligence in them are given. The analysis carried out in the article showed that modern society needs innovative technological solutions so that urbanization can continue in a safe, efficient and healthy way for us and the planet. The combination of AI, sensors, cloud computing, working hand in hand, with clear privacy laws and a strict definition of human rights, will give us truly smart cities that can serve as the basis for human growth and prosperity.

Keywords: smart city, artificial intelligence, AI, cyberattack, IoT, security, confidentiality.

Опірський Іван Романович, д.т.н., доц., професор кафедри захисту інформації Національного університету «Львівська політехніка».

E-mail: ivan.r.opirskyi@lpnu.ua.

Orcid ID: 0000-0002-8461-8996.

Опирский Иван Романович, д.т.н., доц., профессор кафедры защиты информации Национального университета «Львовская политехника».

Opirsky Ivan, Doctor of Technical Sciences, Associate Professor, Professor of the Department of Information Protection of the National University "Lviv Polytechnic".

Тютіков Олег Юрійович, студент кафедри захисту інформації Національного університету «Львівська політехніка».

E-mail: tutikov.oleg@gmail.com.

Orcid ID: 0000-0002-6112-6278.

Тютиков Олег Юрьевич, студент кафедры защиты информации Национального университета «Львовская политехника».

Tiutikov Oleh, Student, Department of Information Security, National University "Lviv Polytechnic".