УДК 004.8.65.05.681.5 DOI: 10.31673/2786-8362.2023.010303

Зінченко О.В., д.т.н., **Катков Ю.І.,** д.т.н.,
Березовська Ю.В., PhD, **Вишнівський О.В.**,
Щербаков Є.М.

КРИТИЧНІ АСПЕКТИ ПІД ЧАС ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ГАЛУЗІ БЕЗПІЛОТНИХ ТРАНСПОРТНИХ ЗАСОБІВ

Zinchenko O.V., Katkov Y.I, Berezovska Yu.V., Vyshnivskyi O.V., Shcherbakov E.M. Critical aspects when implementing artificial intelligence in the industry of unmanned vehicles. The article is devoted to critical aspects during the implementation of artificial intelligence in the field of unmanned vehicles. The task is to determine the critical aspects that will have a negative impact based on the analysis of the introduction of artificial intelligence to solve the set of tasks of managing an unmanned vehicle in the external environment. To solve this problem in the article: an analysis of the methods of full autonomy of vehicles is performed and the classification of control systems of unmanned vehicles in the external environment is considered; a description of the levels of autonomy/automation of the Automated driving system, which allow distinguishing autonomous vehicles based on the SAE J3016 standard; performed analysis of tasks of each level regarding the possibility of applying artificial intelligence; explore the possibilities of driverless vehicle control systems using a variety of automotive computer networks, in which vehicles and roadside devices are communication nodes providing each other with information such as safety warnings and traffic information.

Based on the analysis, the following conclusions are drawn: firstly, to manage a fully autonomous system of an unmanned vehicle, it is necessary to use artificial intelligence, which will be able to process information from navigation aids, sensors and means of communication between unmanned vehicles in the external environment in a timely manner; secondly, it will require a complex multi-level artificial intelligence system with a single interface to make the right decisions at the right time to achieve the intended result requires; thirdly, the use of artificial intelligence in the field of unmanned vehicles today faces the problem of the need to have large computing power on this autonomous vehicle, which leads to the appearance of critical aspects, namely: the problem of power supply and cooling of many processors in the computing system.

Keywords: intelligent systems, vulnerability of autonomous driving, autonomous vehicle.

Зінченко О.В., Катков Ю.І., Березовська Ю.В., Вишнівський О.В., Щербаков Є.М. Критичні аспекти під час впровадження штучного інтелекту в галузі безпілотних транспортних засобів. Стаття присвячена критичним аспектам під час впровадження штучного інтелекту в галузі безпілотних транспортних засобів. Ставиться завдання: на основі аналізу впровадження штучного інтелекту для вирішення множини завдань управління безпілотним транспортним засобом у зовнішньому середовищі визначити критичні аспекти, які будуть мати негативний вплив. Для вирішення цього завдання в статті: виконано аналіз способів повної автономії транспортних засобів та розглянута класифікація систем управління безпілотними транспортними засобами в зовнішньому середовищі; зроблено опис рівнів автономії/автоматизації Automated driving system, що дозволяють розрізняти автономні транспортні засоби на основі стандарту SAE J3016; виконаний аналіз завдань кожного рівня відносно можливості застосування штучного інтелекту; розглянуто можливості систем управління безпілотними транспортними засобами за допомогою різноманітних автомобільних комп'ютерних мереж, в яких транспортні засоби та придорожні пристрої є вузлами зв'язку, що надають один одному інформацію, таку як попередження про безпеку та інформацію про дорожній рух. На основі виконаного аналізу робляться висновки: по-перше, для управління повністю автономною системою безпілотного транспортного засобу необхідно використання штучного інтелекту, який буде здатен своєчасно обробляти інформацію від засобів навігації, датчиків та засобів спілкування між безпілотними транспортними засобами в зовнішньому середовищі; по-друге, знадобиться складна багаторівнева система штучного інтелекту з одним інтерфейсом для прийняття правильних рішень у потрібний час щоб досягнути призначеного результату; по-третє, використання штучного інтелекту в галузі безпілотних транспортних засобів сьогодні стикається з проблемою необхідності мати великі обчислювальні потужності на цьому автономному засобі, а це призводить до появи критичних аспектів, а саме: проблеми енергопостачання та охолодження багатьох процесорів в обчислювальний системі.

Ключові слова: інтелектуальні системи, уразливість автономного водіння, автономний транспортний засіб.

Вступ

Сьогодні стало очевидним, що новим етапом розвитку інформаційних та інтелектуальних технологій буде їх застосування повсюдно у безпілотних транспортних засобах (повітряних, наземних, надводних та підводних). Дорожньо-транспортні пригоди стали однією з найбільших у світі проблем суспільної охорони здоров'я та запобігання травматизму. Тому одним із найбільш важливих мотивуючих факторів для зниження аварійності, травм та смертей водіїв, пасажирів та пішоходів сьогодні є створення сучасних систем безпеки руху [1–4]. Новим напрямом розвитку систем безпеки руху є створення безпілотних транспортних засобів (автомобілів), які мають автопілот із застосуванням технологій штучного інтелекту.

Метою впровадження технологій штучного інтелекту в автопілоті є використання переваг від такого впровадження, а саме: підвищують безпеку та зручність водіння; створюють умови для екологічних переваг; надають кращий доступ для людей з обмеженими можливостями; створюють нові робочі місця [5–7].

Сьогодні впровадження штучного інтелекту в галузі безпілотних транспортних засобів вирішується за рахунок використання централізованої обробки всієї інформації виключно у вигляді «хмарних обчислень» у стаціонарних центрах обробки даних (ЦОД). Тобто, при «хмарних обчисленнях» усі дані від датчиків, сенсорів та відеокамер, які необхідні для роботи автопілоту, завантажуються по каналах телекомунікації в ЦОД для обробки, а потім периферійні комп'ютери очікують на відповідь від ЦОД для виконання команди. Звідси під час централізованої обробки даних на основі «хмарних обчислень» виникає затримка реакції в процесі управління транспортним засобом на вплив зовнішнього середовища. Мова йде про час затримки, коли транспортний засіб продовжує рухатися. Для того щоб не було аварійних ситуацій час затримки повинен бути значно меншим допустимого часу реакції на конкретну дорожньо-транспортну ситуацію. Наприклад, автономний транспортний засіб, що рухається, за допомогою датчиків встановив наявність загрози. Для безпечної навігації необхідно негайно зупинитися. Відомо, що для прийняття рішення на гальмування і сам процес гальмування потрібен час (час реакції). Природно, якщо загроза виявлена і потрібне гальмування, то чим раніше буде гальмування, тим краще. Отже, якщо затримка реакції буде співмірна з часом, що необхідний на гальмування, відбудеться зіткнення (аварія або катастрофа). Виникає завдання зменшення часу затримки реакції.

Для вирішення цього завдання існують різноманітні способи, а саме: зменшення швидкості руху; передбачення розвитку дорожньо-транспортної ситуації; підвищення пропускної спроможності каналів телекомунікації, збільшення продуктивності засобів обчислювання. Такі способи постійно вдосконалюються, але вони стають досить не ефективними через досягнення фізичних не можливостей або функціонального обмеження безпілотних транспортних засобів. Звідси випливає очевидний висновок, що такий підхід має вразливі (критичне) місця: централізовану обробку даних для використання технологій хмарних обчислень; засоби телекомунікації для передачі даних в каналах зв'язку. Тому застосування штучного інтелекту через організацію «хмарних обчислень» не є перспективним із наступних причин: внаслідок сумарного часу затримки обробки даних та їх передачі у каналах зв'язку з допустимим часом реакції на конкретну дорожню ситуацію; робота в конкурентному середовищі (обмежений ресурс частот і кодів) з обмеженою пропускною здатністю та ненадійними комунікаціями.

Для усунення вказаних вразливих (критичних) місць сьогодні вивчається нова парадигма використання штучного інтелекту в галузі безпілотних транспортних засобів – *створення обчислювальної потужності в автономному транспортному засобі для його управління за допомогою штучного інтелекту* [8].

Дійсно, у разі застосування засобів обчислення безпосередньо в автономному транспортному засобі в будь-якій дорожньо-транспортній ситуації рішення про гальмування може бути прийняте значно скоріше. Але це вимагає мати великі обчислювальні потужності на цьому автономному засобі. Необхідність наявності великої обчислювальної потужності пов'язані з тим, що для виконання складних алгоритмів управління безпечного руху

необхідний аналіз великих обсягів даних від сенсорів, датчиків і камер, а також необхідно накопичення і систематизація даних у системах баз даних для використання під час прийняття рішення на рух.

Таким чином, нова парадигма використання штучного інтелекту в галузі безпілотних транспортних засобів вимагає застосування автономного обчислювального засобу з великою потужністю. Але збільшення обчислювальної потужності на автономному транспортному засобі вимагає необхідність дослідження можливості появи нових вразливих (критичних) місць. Це є актуальною та своєчасною задачею для дослідження.

Постановка завдання

Тому, в роботі вирішується **наукове завдання** визначення шляхів застосування штучного інтелекту в галузі безпілотних транспортних засобів на основі нової парадигми розміщення великих обчислювальних потужностей на автономних транспортних засобах. Необхідно визначити, в якому вигляді його треба застосовувати для вирішення множини завдань управління безпілотним транспортним засобом у зовнішньому середовищі та вказати загальний перелік критичних місць, де застосування штучного інтелекту буде мати вразливості.

Аналіз останніх наукових досліджень

Можна припустити, що ідея створення автономного транспортного засобу була запропонована Леонардо да Вінчі близько 1500 року. Його самокерований візок використовував пружинний механізм рульового управління, який може бути налаштований заздалегідь, щоб рухатися по заданому шляху. На практиці дослідні самокеровані автомобілі з'явилися у 1920-х роках у вигляді радіокерованих транспортних засобів, що дозволяло вирішувати технічні завдання дистанційного керування автомобілем. Першим завданням щодо автономії транспортного засобу є завдання автомобільного круїз-контролю, який підтримує задану швидкість під час руху. Круїзний контроль Тієтера був запропонований у 1945 році, він не використовувався для комерційних цілей до 1958 року. З іншого боку, перші функції безпеки в транспортних засобах розпочали впроваджуватися в 1950-х роках з ременя безпеки, анти блокувальної системи гальм. Основним результатом цього часу було створення першого самокерованого транспортного засобу в 1961 році для руху по місячній поверхні Stanford Cart (Стенфордський візок), коли аспірант Джеймс Адамс запропонував спосіб керування рухом, незважаючи на 2.5-секундну затримку передачі даних з віддаленого пристрою керування, що був на Землі. У 1960-х роках зароджується напрям розвитку створення автономного транспортного засобу на основі концепції автоматизації допомоги водієві. Ця концепція визначала перелік завдань, які необхідно автоматизувати щоб підвищувати безпеку та зручність водіння на автомагістралях. Результатом впровадження цієї концепції є створення електронної системи контролю стану автомобіля. У 1977 році японська компанія Tsukuba Mechanicaleering впровадила концепцію безпілотних транспортних засобів, який використовував камери для виявлення вуличних маркувань під час руху зі швидкістю майже 20 миль на годину. На основі цього у 1980-х роках концепція автоматизації допомоги водієві трансформується в концепцію контролю безпеки руху на автомагістралях, наприклад, на початку 1980-х фірма Mercedes-Benz представила перший автомобіль із «динамічним зором» – системою візуалізації на основі відеокамер, яка зосереджується лише на важливих об'єктах. Завдяки цьому автомобіль зміг рухатися зі швидкістю до 60 миль.

Застосування штучного інтелекту для реалізації функції безпеки навігації по дорогах починається з 2000-х років у наслідок розвитку обчислювальної техніки, коли були введені розширені функції безпеки, що включають: виявлення сліпих зон; електронний контроль стабільності руху; попередження про лобове зіткнення; попередження про вихід зі смуги руху. Також, до системи автоматичного візуального керування було додано розширені функції безпеки руху у складних транспортних умовах для безпеки водіїв, пасажирів та пішоходів. Були розпочаті практичні дослідження, наприклад, з 2004 по 2013 рік Агентство перспективних дослідницьких проектів оборони США (DARPA) в Арлінгтоні, спонсорувало ряд завдань для академічних, промислових та приватних винахідників для розвитку

автономного автомобіля, який міг би незалежно рухатися в різних середовищах. Для іспиту треба було рухатися по маршруту в 150 миль по пустелі та по 60-мильному міському маршруту. Хоча жоден із учасників не пройшов тест у пустелі, чотирьом автомобілям вдалося подолати міський маршрут за межі шестирічного часу цього тесту.

Наступним кроком впровадження обчислювальної техніки до системи автоматичного візуального керування є впровадження технологій автономного руху на основі технологій радарів. Технологія радарів забезпечувала попередження водія про несподівану небезпеку на автомагістралях під час руху. З тих пір безпілотні трамваї, таксі та особисті машини були введені з різним ступенем успіху. Але збільшення кількості транспортних засобів на автомагістралях, підвищення швидкості руху та застосування автомобілів у всіх процесах нашого життя – викликало необхідність зміни парадигми концепції безпеки руху. Тому у 2010-х роках була сформована нова концепція безпеки руху, в якій запропоновані розширені функції допомоги водієві, а саме: контроль за рухом автомобілів у складних транспортних умовах на основі автопілоту; впровадження розширених функцій автопілоту та можливість повного автономного керування автомобілем. Так, були запропоновані розширені функції допомоги водієві, багато з яких є стандартними для сучасних автомобілів, а саме: автоматичне аварійне гальмування; допомога з центрування смуги руху; пішохідне та заднє автоматичне аварійне гальмування; оповіщення про перехресний рух позаду; відеоспостереження заднього виду. Починаючи з 2016 року запропоновані нові автоматизовані функції безпеки та допомоги водієві, а саме: адаптивний круїз-контроль; допомога утримання смуги руху; самостійне паркування; допомога у пробках [4]. Сьогодні автовиробники, такі як Ford, General Motors, Tesla та інші модернізують існуючі та впроваджують нові технології безпілотних автомобілів з метою забезпечення безпеки та зручності водіння [4–8].

Впровадження нових технологій породжує нові уразливі місця, які необхідно постійно шукати. Тому, застосування штучного інтелекту в галузі безпілотних транспортних засобів на основі нової парадигми розміщення великих обчислювальних потужностей на автономних транспортних засобах вимагає пошуку цих критичних місць, де застосування штучного інтелекту буде мати вразливості.

Метою роботи є підвищення ефективності використання управління безпілотним транспортним засобом у зовнішньому середовищі та наявності вразливостей.

Виклад основного матеріалу дослідження.

Стандартом Society of Automotive Engineers (SAE J3016) визначені наступні рівнів автономії/автоматизації автомобільних систем (Advanced driver systems – ADS), що дозволяють розрізняти автономні транспортні засоби [9]:

1. *Рівень SAE ADS 0:* рівень без автоматизації. Людина керує автомобілем без сторонньої допомоги;

2. *Рівень SAE ADS 1:* рівень часткової автоматизації. Водій залишається відповідальним за водіння та всі інші функції, пов’язані з рухом. Але йому допомагає вдосконалена система допомоги водієві (Advanced driver assistance systems – ADAS), яка застосовує технології запобігання зіткненням (наприклад, попередження про вихід зі смуги руху та програми для сліпих зон), для гальмування та прискорення або керування рухом та допоміжні засоби для водія, такі як нічне бачення, оповіщення водія та адаптивний круїз-контроль;

3. *Рівень SAE ADS 2:* рівень початкової автономії та високої автоматизації. Створюється часткова автоматизація водіння: автономні функції водіння можуть бути корисні в ситуації, забезпечуючи як активне рульове управління, так і підтримку гальмування або прискорення у конкретних завданнях динамічного водіння. Очікується, що водій залишатиметься уважним, контролюватиме ситуацію та несе відповідальність за всі інші динамічні функції;

4. *Рівень SAE ADS 3:* рівень умовної автономії. Застосовується автоматизована система водіння, яка може виконувати всі завдання водіння динамічного водіння замість водія в певних умовах навколишнього середовища та дорожніх умовах. Водій повинен завжди залишатися

готовим втручатися і здатним повернути собі керування на запит ADAS і повинен виконувати всі завдання в неоптимальних умовах;

5. *Рівень SAE ADS 4:* рівень високого ступеня автономії. Система ADS виконує всі завдання динамічного водіння в певних умовах навколишнього середовища та дорожніх умов. Наявність або увага людини-водія не потрібні;

6. *Рівень SAE ADS 5:* рівень повної автономії транспортного засобі. Система ADS повністю керує транспортним засобом у будь-яких умовах, тобто може автономно виконувати всі динамічні завдання водіння у всіх комбінаціях дорожньої поверхні та умов навколишнього середовища. При цьому людям чи пасажирам не потрібно звертати увагу або брати участь у керуванні автомобілем.

Також відомо, що для управління автономним транспортним засобом потрібні такі системи:

– внутрішня навігаційна супутникова система для визначення розташування в дорожній ситуації та маршруту руху, яка пов'язана з Global Navigation Satellite System (GNSS);

– візуально-сенсорна система, що розпізнає складні дорожні умови у дальній та ближніх зонах, яка здійснює обмін інформацією за допомогою комунікаційних систем;

– високопродуктивна вбудована обчислювальна система (high-performance embedded computing – HPEC), яка має доступ до необхідних даних із сенсорів (датчиків, приймачів, камер) двох попередніх систем та перетворює її за допомогою алгоритмів штучного інтелекту на дію управління безпілотним автономним транспортним засобам.

Зосередження цих систем безпосередньо в автономному транспортному засобі дозволяє потенційно подолати проблему сумарного часу затримки та реакції, забезпечити глибоке машинне навчання. Але необхідно розглянути потенційні загрози для кожної з перерахованих систем.

1. Загрози для геолокації автономного транспортного засобу, які застосовуються для визначення розташування в дорожній ситуації та маршруті руху. Відомо, що автономними транспортними засобами можуть бути використані для знаходження свого місцезнаходження:

– глобальні навігаційні супутникові системи позиціонування (GNSS);

– тріангуляція топологічного простору за допомогою стільникового зв'язку.

GNSS – це геолокація методом позиціонування за допомогою сигналів GPS супутнику. GNSS дозволяє створювати навігаційні сервіси позиціонування будь-яких мобільних пристроїв, наприклад, Google Maps.

Принцип побудови GNSS наступний: систему створює сукупність радіоелектронних засобів, що дозволяє визначати положення та швидкість руху об'єкта на поверхні Землі або в атмосфері відносно положення супутників. Положення об'єкта обчислюється завдяки використанню розміщеного на ньому GPS-приймача, який приймає та обробляє сигнали супутників космічного сегменту GPS-системи глобального позиціонування. Для визначення точних параметрів орбіт супутників та керування GPS-системою вона в своєму складі має наземні центри управління. GNSS дозволяють спеціалізованим радіоприймачам визначати своє тривимірне космічне положення, а також час, з точністю 2–20 метрів або десятки наносекунд. GNSS найкраще працює в ідеальних умовах, коли є надійне з'єднання з будь-яким пристроєм, який показує місцезнаходження. Сьогодні існують такі системи: система глобального позиціювання (GPS – Global Positioning System) або система NAVSTAR США, яка працює з 1995 року; ГЛОНАСС – працює з 2011 року; Galileo – Європейське Товариство, функціонує з 2019 року. Також тестуються для впровадження національні навігаційні системи: Beidou – запланований проект у Китаї; Індійська регіональна навігаційна супутникова система.

Процес позиціонування наступний: пристрої отримують сигнали як мінімум від 3-4 супутників, а в ідеалі від 7-8, щоб надавати найбільш точні дані про місцезнаходження. Цим сигналам від багатьох супутників доводиться долати величезні відстані через атмосферу, щоб досягти спеціальних пристроїв, і якість такого сигналу відіграє велику роль. В ідеальному

випадку краще всього знаходитися на відкритому повітрі, якщо необхідно отримати найкращий сигнал. Крім того, як міські, так і природні каньйони (великі будинки в містах, дерева, гори, хребти тощо) можуть впливати на будь-який сигнал GPS. Тобто, якщо супутник не знаходиться прямо над головою, точне відстеження стає набагато складнішим, а точність сигналу GPS знижується. Тому, раптово виникає погане відстеженням геолокації (зміна точності відстеження місцезнаходження). Особливістю GNSS є використання мікрохвильових сигналів від супутників, які надійно можуть прийматися лише на відкритому повітрі та покривають більшу частину поверхні Землі, а також навколоземний простір.

Уразливість системи GPS має багато чинників, що можуть блокувати пряму видимість супутників GPS або показувати неправильну геолокацію (впливають на точність місцезнаходження): погода (хмарність та сильні пориви вітру, а також зливи); середовище для проходження сигналу від супутнику до приймача (стіни, дахи автомобілів, будівлі, дерева, одяг та людське тіло); місце знаходження приймача (тунелі, естакади, находження в гірській місцевості); перешкоди сигналам GPS, які можуть бути викликані несправністю чи неправильним налаштуванням передавачів; перешкоди від ненавмисно переданих сигналів інших систем в тому ж частотному діапазоні, що і сигнали GPS; перешкоди роботи засобів зв'язку, які можуть бути заблоковані внаслідок включення телефонних дзвінків, приймання текстових повідомлень в мережі Wi-Fi.

Особливо небезпечними є навмисні перешкоди GPS (глушення або спуфінг GPS), коли пристрої глушіння (блокатори мобільних сигналів), які випромінюють сигнали на частоті GPS для створення перешкод. GPS так легко заглушити тому що оскільки приймачі GPS приймають слабкі радіохвилі з супутників, їх можна легко заглушити або спотворити, використовуючи сильніші радіочастотні сигнали, які імітують сигнали, отримані від супутника за допомогою глушника GPS. Супутники GPS передають свої сигнали із певним ступенем точності, але те, що ви отримуєте на рівні землі, залежить від наступних факторів: супутникова геометрія; блокування сигналу; атмосферні умови; конструктивні особливості/якість приймача.

Таким чином, уразливість GPS пов'язана зі слабким сигналом у приймача. Уразливість проявляється в положенні на карті, яке при слабкому сигналі у приймача може бути неправильним. Для створення уразливості GPS існують три поширені джерела помилок сигналу GPS: атмосферні перешкоди; помилки обчислення та округлення; помилки даних ефемеріду (орбітальний шлях).

Тріангуляція топологічного простору за допомогою стільникового зв'язку. Використання мобільних пристроїв з підтримкою базових станцій мережі, наприклад, LTE/4G – це тріангуляція відносно розташування базової станції, що дозволяє відслідковувати позиціонування з відносно гарною точністю. Під час подорожі ви переміщаєтеся з однієї стільникової зони до іншої. Базові станції відстежують потужність сигналу вашого телефону, і в міру того, як ви наближаєтеся до краю одного осередку, потужність сигналу зменшується. У той же час базова станція, до якої ви наближаєтеся, помічає посилення сигналу. Коли ви переміщаєтеся від однієї соти до наступної соти, вишки передають ваш сигнал від однієї до іншої, а відстань між приймачами по суті визначає ваше положення.

Процес тріангуляції наступний: для точного визначення місцезнаходження потрібно мати сигнал мінімум від трьох базових станцій. Навіть за великої кількості вишок у великих містах чи густонаселених районах виникають складнощі для отримання сигналу, також впливає складна топографія місцевості, наприклад, високі будівлі можуть переривати сигнал, створювати перешкоди. У віддалених місцях вишки можуть бути навпаки так далеко одна від одної, що не можуть забезпечувати стабільні сигнали, а це призводить до неточного позиціонування. Оскільки перешкоди, такі як дерева та будівлі, туман чи дощ та багато інших можуть вплинути на якість тріангуляції, то вважається, що цей метод менш точний, ніж вимірювання GPS по сигналах супутнику. Тобто тріангуляція за допомогою стільникового зв'язку не може забезпечити таку ж якість, що робиться під час геолокації методом позиціонування за допомогою сигналів GPS супутнику.

На основі аналізу умов роботи цих методів визначення місцезнаходження можна визначити умови появи уразливості та загроз для геолокації автономних транспортних засобів під час визначення розташування в дорожній ситуації та маршруту руху:

– *холодні пуски* – коли GPS увімкнене або якщо GPS надто довго неактивний у фоновому режимі, GPS необхідно завантажити дані з супутників, які описують положення та синхронізацію всіх супутників у системі. Виправлення може тривати до п'яти або більше хвилин і може призвести до неправильного відстеження GPS;

– *недостатньо супутників* – багатьом пристроям GPS в ідеалі необхідно отримувати сигнали щонайменше від 7 або 8 супутників, щоб обчислювати місцезнаходження з точністю до 10 метрів. При меншій кількості супутників зростає невизначеність та неточність. Маючи менше 4 супутників, багато приймачів GPS не можуть точно оцінити місцезнаходження і повідомляють про втрату сигналу GPS в точках маршруту;

– *погане обладнання* – якщо ваш пристрій застарів або не має хороших можливостей прийому GPS, він буде важко приймати сигнали супутників або вишок стільникового зв'язку;

– б*агатопроменеві сигнали* – коли сигнали від супутників GPS або вишок стільникового зв'язку відбиваються від будівель, приймач GPS може збиватися з пантелику додатковим часом, який знадобився сигналу для його досягнення. У цих випадках можна спостерігати раптові помилки у місцезнаходженні. У цих обставинах мало що можна зробити, щоб зменшити вплив помилок багатопроменевості. GPS просто менш точний у таких ситуаціях;

– *GPS дрейф* – трек GPS відхиляється від дороги. Ви можете помітити, що маршрут зазвичай повторює форму дороги, але з набагато меншою точністю;

– *раптова втрата сигналу GPS* – якщо сигнал втрачено, а через якийсь час відновлено, точки до і після втрати сигналу будуть оброблятися так само, як будь-які інші дві точки (хоча між ними пройшло більше часу) і зєднувати їх прямою лінією;

– *відскок GPS* – тремтливий GPS-трек може призвести до того, що ваша активність покаже більшу відстань, ніж ви фактично проїхали, оскільки кожен «зиг» і «загин» вашого GPS-трека повинен враховуватися прямою лінією, що їх з'єднує;

– *радіоперешкоди або глушіння* – технічне обслуговування/маневри супутників створюють тимчасові перерви в покритті. У деяких випадках апаратне забезпечення GPS пристрою працює нормально, але програмне забезпечення несправне, наприклад, користувачів можуть ввести в оману програмні служби GPS, у тому числі: неправильно намальовані карти, неправильно помічені підприємства та інші визначні пам'ятки, неправильно оцінені адреси вулиць, відсутність доріг, будівель, населених пунктів тощо;

– *низький рівень заряду батареї на пристроях GPS* – низький заряд акумулятора може вплинути на правильну роботу GPS на будь-якому пристрої.

Таким чином, без належного GPS-приймача будь-які пристрої для позиціювання не можуть надати достовірну інформацію про місцезнаходження. Для підвищення точності позиціювання застосовується спеціальне програмне забезпечення, яке використовує цю інформацію для визначення місця розташування на основі вимірювання параметрів за допомогою обох способів. Це вимагає мати великі обчислювальні потужності на автономному транспортному засобі.

2. Загрози для візуально-сенсорної системи автономного транспортного засобу, що розпізнає складні дорожні умови у дальній та ближніх зонах, яка здійснює обмін інформацією за допомогою комунікаційних систем.

Для постановки завдань щодо розробки інтелектуальних систем автономного водіння необхідно визначити основні групи загроз, які необхідно нейтралізувати в першу чергу, а саме:

1 група. Загрози контролю за станом транспортного засобу – це загрози для систем контролю за станом транспортного засобу, які відображають керування внутрішніми системами автомобіля. Сучасний автомобіль – це дуже складна машина, що складається із сотень складових частин, які працюють разом у ідеальній гармонії. Значна частина конструкції автономного транспортного засобу пов'язана із повсякденними проблемами, такими як: система контролю функціонування двигуна, паливна система, система запалювання,

електрична система, вихлопна система, система приводу трансмісії, системи підвіски та рульового керування, система гальмування, система контролю за каркасом і корпусом.

2 група. Загрози позиціонуванню транспортного засобу – це загрози позиціонуванню та навігації, які визначають, де ви знаходитесь, куди ви хочете потрапити і як ви туди дістанетеся були розглянуті вище. Для цього потрібні надійні інструменти та методи геолокації, а також алгоритми обчислювання розташування транспортних засобів із різним ступенем точності, узгодженості та доступності.

3 група. Загрози застосування для датчиків від різних перешкод – це велика група загроз для водіння та безпеки руху, які визначають керування транспортним засобом, забезпечення правильної поведінки транспортного засобу за будь-яких обставин та дотримання правил дорожнього руху. Автономний автомобіль повинен уміти бачити та інтерпретувати, що знаходиться попереду, коли він рухається вперед (і, звичайно, з усіх боків та позаду). Інакше кажучи, йому потрібен огляд 360°. Очевидним вибором є набір відеокамер, які визначають, де знаходиться смуга руху, та виявляють об'єкти чи маркери на дорозі. Однак на датчики, сенсори та відеокамери під час руху можуть впливати дорожні умови: бруд, вода, температура.

4 група. Загрози сенсорної системи комп'ютерного зору та розпізнавання образів дорожніх та погодних умов – комп'ютерний зір або комп'ютерне бачення та розпізнавання образів дорожніх та погодних умов – це технології, які можуть проводити виявляння, відстеження та визначення об'єктів на основі відеоданих, які можуть бути представлені у вигляді багатьох форм. Прикладами таких систем можуть бути: системи керування процесами (промислові роботи, автономні транспортні засоби); системи відеоспостереження; системи організації інформації (наприклад, для індексації баз даних зображень); системи моделювання об'єктів або навколишнього середовища (аналіз медичних зображень, топографічне моделювання); системи взаємодії (наприклад, пристрої введення для систем людино-машинної взаємодії).

5 група. Загрози обміну інформацією з іншими транспортними засобами руху – для впровадження штучного інтелекту в галузі безпілотних транспортних засобів необхідно отримання, передавання та обробки всієї інформації про зовнішнє і внутрішнє середовище автономного транспортного засобу при конкретній дорожньо-транспортній ситуації під час руху, щоб приймати вірні рішення для усунення аварійних ситуацій. Для цього сьогодні існують такі автономні системи [10–13]: автомобіль – загальна система керування до всього (Vehicle-to-everything, V2X); автомобіль – автомобіль (Vehicle-to-Vehicle, V2V); автомобіль – інфраструктура (Vehicle-to-Infrastructure, V2I); автомобіль – стільникова мережа (Vehicle-to-Net, V2N); автомобіль – пішохід (Vehicle-to-Pedestrian, V2P); автомобіль – мотоцикл (Vehicle-to-Motorcycle, V2M); автомобіль – пристрій (Vehicle-to-Device, V2D); автомобіль – енергосистема (Vehicle-to-Grid, V2G); автомобіль – хмара (V2C).

Основна мета всіх технологій зв'язку – запобігти автомобільним аваріям до того, як вони виникнуть. Кожна з цих систем призначена для передачі інформації між транспортними засобами та іншими об'єктами на дорозі в режимі реального часу. Ця інформація робить попередження водіям та автономним транспортним засобам. Зв'язок між транспортними засобами допомагає автомобілям обмінюватися даними з іншими автомобілями, що знаходяться поблизу, у тому числі загальним станом та напрямком, наприклад, станом гальмування, положенням кермового колеса, швидкістю, маршрутом та іншою інформацією, такою як зміна смуги руху. Автомобілі зможуть передавати важливу інформацію сусіднім автомобілям для підвищення загальної ефективності та безпеки дорожнього руху. Але кожна така система створює загрози для обміну інформацією з іншими транспортними засобами руху в наслідок: перешкод, через досягнення фізичних не можливостей або функціонального обмеження безпілотних транспортних засобів.

6 група. Загрози керуванню дорожньою інфраструктурою – ці загрози можуть мати вплив на керування дорожньо-транспортною інфраструктурою, що дозволяє автомобілям розуміти та підключатися до різноманітної дорожньої інфраструктури. Сюди входять світлофори, розмітка смуг руху, дорожні знаки, зони будівництва, шкільні зони та інші. Дорожні умови

можуть бути вкрай непередбачуваними і змінюватись від місця до місця. У деяких випадках зустрічаються рівні та позначені широкі магістралі, а в інших випадках дорожні умови сильно погіршені – немає розмітки, а саме: смуги не позначені, є вибоїни, гірські та тунельні дороги, де зовнішні сигнали спрямування не дуже чіткі тощо. Також погодні умови відіграють ще одну погану роль. Може бути сонячна та ясна погода або дощова та бурхлива погода. Автономні автомобілі повинні працювати за будь-яких погодних умов.

7 група. Загрози для алгоритмів навчання автономних автомобілів – процес впровадження машинного навчання не обходиться без величезного набору проблем. Автономні автомобілі мали виїхати на дорогу, де їм довелося б рухатися в різних дорожніх умовах. Їм довелося б їхати з іншими автономними автомобілями дорогою, де водночас є багато перешкод, а також людей. Скрізь, де задіяні люди, задіяно багато емоцій. Трафік може бути дуже різноманітним (хаотичним або саморегульованим). Але часто трапляються випадки, коли люди можуть порушувати правила дорожнього руху. Об'єкт може бути в несподіваних умовах. У разі щільного трафіку навіть рух на кілька сантиметрів за хвилину має значення. Не можна нескінченно чекати, поки трафік автоматично очиститься та з'являться якісь передумови для початку руху. Якщо більше таких автомобілів на дорозі чекають, поки рух буде розчищений, це може призвести до глухого кута.

8 група. Загрози захисту програмного забезпечення від втручання зловмисників – даний аспект проблеми безпеки програмних комплексів є порівняно новим і пов'язаний з можливістю впровадження в тіло програмних засобів на етапі їх розробки (або модифікації в ході авторського супроводу) так званих «програмних закладок». У зв'язку з цим актуальніше стає проблема забезпечення технологічної безпеки програмного забезпечення.

9 група. Загрози виникнення морально-правових питань – це відповідальність за нещасний випадок, що може статися за помилкою системи керування автономним автомобілем. У випадку автономних автомобілів програмне забезпечення буде основним компонентом, який керуватиме автомобілем та прийматиме всі важливі рішення. У початкових проектах автономних автомобілів рівня SAE ADS 3 та 4 людина фізично знаходилася за кермом, у нових проектах рівня SAE ADS 5 немає ні панелі приладів, ні керма. Такі випадки вже відомі, коли автономний автомобіль компанії Тесла попав в дорожньо-транспортну пригоду. У таких конструкціях, де в автомобілі немає жодних органів керування, таких як кермо, педаль гальма, педаль акселератора, виникає питання: як людина в машині повинна керувати автомобілем у разі несприятливого інциденту? Крім того, через характер автономних автомобілів пасажири в основному будуть у розслабленому стані та можуть не звертати пильної уваги на умови руху.

3. Загрози для система HPEC (високопродуктивна вбудована обчислювальна система (High-Performance Embedded Computing – HPEC). Використання HPEC у незалежних або частково незалежних обчислювальних системах, що вбудовуються, мають вирішальне значення для успіху впровадження штучного інтелекту тому що вони дають такі переваги:

– по-перше, HPEC дозволяють функціонально розширити обробку великих наборів даних ближче до датчика, тобто там, де своєчасність результатів найбільш необхідна;

– по-друге, HPEC дозволяють підвищити доступність цих систем, оскільки обчислювальна потужність може використовуватися автономно та мобільно там де це найбільш необхідно;

– по-третє, HPEC дозволяють розташовуватися локально, щоб забезпечити низьку затримку обробки даних, яка необхідна для додатків на основі штучного інтелекту.

Прикладами таких вбудованих систем можуть бути: Kite-Strike і Raven-Strike, новітні графічні процесори на базі NVIDIA Ampere і Jetson Xavier у захищених комп'ютерах малого форм-фактора SFF (Small-Form Factor) [14]. Однак у безпілотних транспортних засобах, які оснащені автономними потужними HPEC, виникає нова уразливість. Вони мають проблеми енергопостачання HPEC та охолодження багатьох процесорів HPEC.

Проблема енергопостачання HPEC полягає в тому, що в бортових (вбудованих) обчислювальних системах чітко проглядається тенденція багатопроцесорних рішень для обробки цільових завдань, що постійно ускладнюються, а це вимагає великих ресурсів

бортових джерел живлення, тобто багатоядерна революція у створенні сучасних мікропроцесорів дозволяє підвищувати їх продуктивність, але одночасно збільшує енергоспоживання. Аналіз ситуації, що склалася на сьогодні в галузі енергозберігаючих технологій, які застосовуються для побудови та управління обчислювальними системами, показав, що:

– проблема енергозберігаючого функціонування обчислювальних систем є актуальною внаслідок економічного і технічного характеру;

– підвищення вимог до продуктивності та надійності обчислювальних систем, що функціонують в умовах обмеженого енергоресурсу, у найближчому майбутньому вимагатиме принципово нових підходів до всебічної організації енергозберігаючих обчислювальних процесів.

Мова йде про те, що у стаціонарних умовах ця проблема вирішується за допомогою різноманітних систем енергопостачання обчислювальних процесів: мережі гарантованого електроживлення (стаціонарна мережа); резервні джерела електроживлення (дизель-генератори, бензогенератори); джерела безперебійного та аварійного електроживлення (акумулятори). У безпілотних транспортних засобах джерелами енергопостачання, як правило, є акумулятори або генератори, які створюють багато складнощів при експлуатації залежно від їх виду. Наприклад, кислотні акумулятори мають недоліки: сульфатація, коротке замикання в акумуляторі, інтенсивне саморозрядження акумулятора, зміна полярності акумулятора, засмічення електроліту, неправильний режим заряду/розряду та інші. Акумулятори літій-іонного типу бояться як морозів нижче –20°С, так і спеки вище +60°С, можуть вибухати і самозайматися, мають обмежену кількість циклів/заряджання, не допускається перезарядження акумулятора тощо.

Проблема охолодження множини процесорів НРЕС виникає тому, що в потужних обчислювальних системах струм, який проходить через елементи схеми, виділяє тепло. При цьому по мірі того, як обладнання стає менше і воно знаходиться в компактнішому просторі, то для відведення тепла потрібно застосовувати більш ефективні способи. При цьому чим ефективніша система охолодження, тим менші габарити всієї багатопроцесорної обчислювальної системи. У стаціонарних умовах ця проблема вирішується за допомогою різноманітних систем охолодження: вентиляторів у комп’ютерах, зовнішніх блоків, прецизійних шафових кондиціонерів, усередині рядні кондиціонери; усередині стійкові системи охолодження, чилерів, градирень, адіабатичних систем.

Для автономних транспортних засобів це стає складною технічною проблемою – мікроелектроніка продовжує розвиватися та впроваджувати інновації в галузі зменшення розмірів та тепла, що виділяється потужною електронікою. Перші кроки в цьому напрямі показали, що завжди існує безліч факторів, які впливають на розробку нового або оновленого продукту безпілотних транспортних засобів. І чим складніший продукт, тим більше факторів необхідно враховувати. Наприклад, для автономних транспортних засобів, незалежно від сфери діяльності, необхідно враховувати продуктивність, розмір, вагу та вартість вбудованої обчислювальної системи та можливості інтеграції до платформ автономних транспортних засобів. Тому, для характеристики таких систем вводиться показник форм-факторів SWaP-C (Size, Weight, Power and Cost) [14].

Форм-фактор SWaP-C – це показник, який вказує на оптимальний розмір, вагу, потужність та вартість пристрою, системи чи програми у поєднанні з можливостями штучного інтелекту. Наприклад, при розробці нового електронного пристрою для автономного транспортного засобу конструктивні рішення включають прагнення, з одного боку, зменшення показників розмірів, полегшення ваги, енергоспоживання, а, з іншого боку, підвищення потужності (продуктивності), безпеки, доступності. І все це при та/або зниженні вартості виробу. У спрощеному вигляді вважається, що чим менше форм-фактор SWaP-C, тим краще. Інакше кажучи, чим меншими будуть показники розмірів, ваги, енергоспоживання та більше продуктивності, безпеки, доступності на одиницю вартості, тим краще. З точки зору математики – це можна описати принципом ефективності за Парето. Ефективність за Парето

або «множиною парето-оптимальних альтернатив» – це такий стан системи, при якому жоден показник системи не може бути покращений без погіршення будь-якого іншого показника. Таким чином, будь-яка зміна, яка нікому не завдає збитків, а приносить користь, є покращенням. У нашому випадку, коли досягнуто оптимальності щодо Парето, то це ситуація, коли всі вигоди від поліпшення якихось показників вичерпані. Тому, сьогодні розробляються декілька напрямків щодо створення систем з оптимальним за Парето форм-фактором SWaP-C:

– технологія мережевої взаємодії відбувається з іншими вбудованими обчислювальними системами на загальній платформі автономних транспортних засобів (Swarm Intelligence – груповий, роєвий інтелект). У цьому випадку виходить розподілена система баз даних та продуктивності процесорів, що з'єднуються телекомунікаціями з високою пропускною здатністю;

– створення функціональної сумісності через модульну архітектуру відкритих систем (Modular Open Systems Architecture – MOSA), яка дозволить усунути бар'єри для розвитку в безпілотних системах, побудованих на основі штучного інтелекту. Це можливо шляхом поступового додавання, видалення або заміни окремих основних системних компонентів на відповідному рівні протягом життєвого циклу основної системної платформи, щоб надати можливості для посилення конкуренції та інновацій;

– впровадження технології машинного навчання, що дозволить значно прискорити темпи розробки та розгортання безпілотних систем.

Для досягнення малого форм-фактора використовують технологію GPGPU (General-Purpose Graphic Processing Unit), наприклад, фірма Sagetech забезпечила поліпшення форм-фактору SWaP-C завдяки вдосконаленій конструкції мікроелектроніки, яка має нові технічні рішення для розсіювання тепла щодо покращення теплових характеристик без використання радіаторів або вентиляторів.

Висновки

Таким чином, процес побудови автономного транспортного засобу під час впровадження нових технологій породжує нові уразливі місця, які необхідно постійно шукати. Тому застосування штучного інтелекту в галузі безпілотних транспортних засобів на основі нової парадигми розміщення великих обчислювальних потужностей на автономних транспортних засобах створює перераховані вище уразливості під час застосування штучного інтелекту. Ці критичні місця, коли вони виявлені, вимагають знаходження нових інженерно-технічних рішень, а це допомагає розробляти нові технології.

Список використаної літератури:

1. National Highway Traffic Safety Administration US / [електронний ресурс] – режим доступу: / https://www.nhtsa.gov/(Дата перегляду 20 червня 2023).

2. Statistical Annex, World report on road traffic injury prevention/ [електронний ресурс] – режим доступу: / https://en.wikipedia.org/wiki/Road_traffic_safety#cite_note-5/(Дата перегляду 20 червня 2023).

3. "World report on road traffic injury prevention". World Health Organisation. Retrieved 14 April 2010. / https://en.wikipedia.org/wiki/Road_traffic_safety#cite_note-5/(Дата перегляду 20 червня 2023).

4. Про схвалення Концепції Державної цільової програми підвищення рівня безпеки дорожнього руху в Україні на період до 2016 року/ [електронний ресурс] – режим доступу: /https://zakon.rada.gov.ua/laws/show/771-2012-%D0%BF#Text/(Дата перегляду20червня 2023).

5. Self-driving car (autonomous car or driverless car) / [електронний ресурс] – режим доступу: / https://www.techtarget.com/searchenterpriseai/definition/driverless-car/(Дата перегляду 20 червня 2023).

6. What is an Autonomous Car? / [електронний ресурс] – режим доступу:/ https://www.synopsys.com/automotive/what-is-autonomous-

car.html#:~:text=Ultrasonic%20sensors%20in%20the%20wheels,acceleration%2C%20braking%2C%20and%20steering//(Дата перегляду 20 червня 2023).

7. How do self-driving cars work? / [електронний ресурс] – режим доступу: / https://www.bankrate.com/insurance/car/how-do-self-driving-cars-work//(Дата перегляду 20 червня 2023).

8. Artificial intelligence and machine learning for unmanned vehicles - April 26, 2021/ [електронний ресурс] – режим доступу: / https://www.militaryaerospace.com/unmanned/article/14202040/artificial-intelligence-and-machine-learning-for-unmanned-vehicles (Дата перегляду 20 червня 2023).

9. SAE J3016 2018, Sistemy avtomatizirovannogo upravleniya dvizheniem ATS. Klassifikaciya, terminy i opredeleniya (Taxonomy and Definitions for Terms Related to OnRoad Motor Vehicle Automated Driving Systems), SAE, 2018, 35 p.

10. 7 Types of Vehicle Connectivity/ [електронний ресурс] – режим доступу: https://blog.rgbsi.com/7-types-of-vehicle-connectivity/(Дата перегляду 20 червня 2023).

11. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_201806 / [електронний ресурс] – режим доступу: / https://www.sae.org/standards/content/j3016_201806/(Дата перегляду 20 червня 2023).

12. The Drive for Vehicle-To-Everything Connectivity/ [електронний ресурс] — режим доступу: /https://www.electronicdesign.com/markets/automotive/article/21215345/mouser-the-drive-for-vehicletoeverything-connectivity/(Дата перегляду 20 червня 2023).

13. VEHICLE-TO-GRID (V2G) IS A TECHNOLOGY THAT HAS THE POWER TO TRANSFORM THE ENERGY SYSTEM. / [електронний ресурс] – режим доступу: https://www.virta.global/vehicle-to-grid-v2g/(Дата перегляду 20 червня 2023).

14. Small-form-factor embedded computing offers new SWaP-based distributed design paradigm/ [електронний ресурс] – режим доступу: https://www.militaryaerospace.com/computers/article/16714704/smallformfactor-embedded-computing-offers-new-swapbased-distributed-design-paradigm (Дата перегляду 20 червня 2023).

Автори статті

Зінченко Ольга – доктор технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Катков Юрій – доктор технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Березовська Юлія – PhD, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Вишнівський Олександр – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Щербаков Є. - студент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Authors of the article

Zinchenko Olga – Doctor of Science (technic), associate professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

Katkov Yuriy – Doctor of Science (technic), associate professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

Berezovska Yulia – PhD, associate professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

Vyshnivskyi Olexander – postgraduate student, State University of Information and Communication Technologies, Kyiv, Ukraine.

Shcherbakov E. – student, State University of Information and Communication Technologies, Kyiv, Ukraine.