УДК 004.056.5:629.3 DOI: 10.30977/BUL.2219-5548.2022.96.0.59

КІБЕРБЕЗПЕКА АВТОМОБІЛІВ: ІСТОРІЯ ЦИФРОВІЗАЦІЇ АВТОМОБІЛІВ, ПОТОЧНИЙ СТАН ПРОБЛЕМИ, ЦІЛІ СТАЛОГО РОЗВИТКУ ТА СТАНДАРТИ

Колодяжний В. М.[1], Левтеров А. І.[1], Малащук Є. В.[2]
[1]Харківський національний автомобільно-дорожній університет
[2]Фізична особа, підприємець, м. Київ

Анотація. *Розглянута сукупність методів і практик захисту від атак зловмисників для забезпечення безперебійної роботи комп'ютерів, мобільних пристроїв, електронних систем, мереж та даних транспортних засобів і транспортної інфраструктури. Наведені посилання на основні міжнародні документи, що забезпечують безпеку транспортних засобів. Указано на проблеми, що мають привести до розроблення технологій із кібербезпеки в майбутньому.*
Ключові слова: *кібербезпека автомобілів, безпека особистих даних, захист від кібератак, технології штучного інтелекту в автомобілях.*

Вступ

На сьогодні питання захисту інформації мають пріоритетне значення. Потреба у фахівцях, які мають відповідну кваліфікацію, зростає, і перед освітніми закладами виникають завдання підготовки студентів, що планують отримати спеціалізацію з технологій кібербезпеки, зокрема й кібербезпеки автомобільного транспорту, і надалі працювати в транспортній галузі.

У роботі розглядаються історія виникнення, поточний стан проблеми та можливий розвиток, що може зацікавити майбутніх студентів у процесі вибору напряму підготовки для вирішення проблем кібербезпеки в автомобільній галузі.

Аналіз публікацій

Кібербезпека (іноді її називають комп'ютерною безпекою) – це сукупність методів та практик захисту від атак зловмисних фахівців (тобто фахівців зі зламу інформації в системі – хакерів) на комп'ютери, сервери, мобільні пристрої, електронні системи, мережі та дані [1]. Методи й захисні практики комп'ютерної безпеки застосовуються в різних галузях – від бізнес-сфери до мобільних технологій, серед яких можна виокремити кібербезпеку автомобілів і транспортної інфраструктури. У кінці серпня 2021 р. [2] був надрукований міжнародний стандарт інженерії комп'ютерної безпеки дорожніх транспортних засобів *ISO/SAE 21434:2021*, що призначені допомогти виробникам завжди бути на крок попереду [3]. Мірою того як автомобілі все частіші починають підключатися до глобальної мережі, зростає ризик порушення кібербезпеки. Так, дослідження, проведені в Англії організацією Zenzic, показали, що з 2016 р. кількість зламів програмного забезпечення в автомобільній галузі в річному обчисленні зросло на 94 %, майже удвічі [4]. Незважаючи на те, що галузь, яка займається боротьбою з хакерами, розвивається, ведеться постійна боротьба за те, щоб не відстати від усе більш досконалих технологій.

Кібербезпека транспорту – це безпека особистих даних, якими користувач ділиться з транспортним засобом або агрегатором транспортних даних. Нині «розумні» системи поширені всюди: вони контролюють траси й залізниці за допомогою платформ для моніторингу, як навігатори відслідковують затори та запобігають їм, відповідають за безпеку пасажирів та водія в середині автомобілів [5]. Усі ці системи використовують контролери та датчики, які дозволяють тримати зв'язок із зовнішніми джерелами даних. На практиці виявляється, що чим більше в транспортного засобу є зв'язок із зовнішнім світом, тим уразливіший він стає зовні для кібератак і тим більше йому потрібна особлива система захисту.

Мета та постановка завдання

Мета цієї статті – розглянути історію виникнення, поточний стан проблеми та сталий розвиток міжнародного співробітництва у сфері кібербезпеки в автомобільній галузі, що може зацікавити майбутніх студентів під час вибору напряму підготовки для вирішен-

ня проблем кібербезпеки на автомобільному транспорті.

Завдання статті – ознайомити читача з основними поняттями кібербезпеки, поточним станом та сталим розвитком міжнародного співробітництва у сфері кібербезпеки в автомобільній галузі, зі стандартами ISO/SAE інженерії комп'ютерної безпеки.

Виклад основного матеріалу

Початком цифровізації автомобілів можна вважати електронне запалювання, антиблокувальну систему гальмування або електронну систему керування двигуном, які запропонували Pontiac, Chrysler та GM ще 1963, 1971, 1979 рр. [6]. У подальшому компоненти автомобілів ставали все більш електронними й, нарешті, цифровими (тут складно провести чітку межу), але справжнім початком цифрової революції в автомобільних технологіях можна вважати лютий 1986 р., коли на конгресі автомобільних інженерів (SAE) компанія Robert Bosch GmbH представила світу цифровий мережний протокол комунікації електронних компонент автомобіля (CAN – controller area network). Що цікаво, фахівці цієї теми й авторитетні інтернет-джерела засвідчують: цей мережний протокол і сьогодні є найбільш поширеним та присутній практично в кожному серійному автомобілі. Крім різновидів CAN-шин (low-speed, high-speed CAN, FD-CAN) сьогодні ще використовуються FlexRay (трансмісія), LIN (низькошвидкісна шина), оптична MOST (мультимедіа) і, нарешті, бортовий Ethernet (на сьогодні 100 Мбіт/с, у наступних генераціях до 1 Гбіт/с).

На сьогодні, з розвитком різних комутаційних протоколів, під час проєктування сучасних автомобілів використовуються так звані технології Drive by Wire (без механічних приводів), що містять електронну педаль газу, гальмову педаль (Toyota, Ford та GM застосовують її з 1998 р. у своїх гібридах і електроавтомобілях), електронні системи паркування (parking sensors parktronics), електронний перемикач передач, електронне рульове управління (першими були Infinity з моделлю Q50 2014 р.). 2000 р. Honda встановлює на серійну S2000 систему EPS (Electric Power Steering), що за визначених умов може керувати кермом замість людини. Починаючи з 2001 р., коробка передач спілкується з людиною тільки по проводах (раніше цю функцію виконував тросик). Тоді ж масово почали застосовувати електронні кнопки запуску, що дозволяли керувати двигуном усупереч бажанню водія. З 2010 р. поширюється мода на повністю графічні приладні панелі, що можуть виводити «все, що завгодно». Електроніка кузова (двері, замки, вікна тощо) з 2015 р. практично в усіх виробників зав'язана на спеціальний комп'ютер і має свою автономію прийняття рішень.

Кількість підключених автомобілів (connected car, з'єднаних із «хмарою» автовиробника) постійно зростає та стрімко наближається до 100 %. Необхідно зазначити, що в деяких країнах існують обмеження на такі автомобілі, але вони мають застарілий законодавчий характер і з часом будуть обов'язково переглянуті. Перший у сучасному сенсі підключений автомобіль з'явився 1996 р. і був результатом співробітництва GM та Motorola Automotive, що привело до появи телематичної (сфери інформатики, що охоплює напрям комунікацій) системи On-Star – системи, що спроможна була самостійно з'єднуватись з оператором служби порятунку у випадку аварії. Віддалена діагностика автомобіля була представлена 2001 р., а 2003 р. підключений автомобіль навчили відправляти виробнику звіти про стан бортових систем. Телематичні блоки data-only були запропоновані індустрією 2007 р. Улітку 2014 р. кампанія Audi першою запропонувала опцію встановлення хотспотів (точок доступу) 4G-LTE-Wi-Fi на свої авто. 2015 р. в GM серійно впроваджували хотспоти до всіх своїх машин і отримали понад мільярд телематичних звітів від клієнтів. Нині автовиробники не тільки збирають телеметрію, але починають її монетизацію: провідну роль тут відіграє BMW із конвергенцією смартфонів та автомобілів [7].

Приблизно шість років тому всерйоз взялися за кібербезпеку, почали інвестувати в проєктування та розвиток кіберзахисних рішень [8]. На сьогодні в автомобільній індустрії кібербезпека забезпечується як апаратними, так і програмними рішеннями, але потрібно пройти довгий шлях, перш ніж усі ЕБК (електронні блоки керування) в машині будуть захищені від активності кібератак.

Кібербезпека в автомобільному будівництві значно складніша, ніж на смартфонах і персональних комп'ютерах, з двох основних причин:

а) десятки ЕБК у кожній машині з'єднані множиною електронних шин і відповідають за різні функції та характеристики;

б) множина потенційних точок доступу як розташованих всередині автомобіля, так і віддалених, зокрема: OBDII, USB та SD-порти, безключовий доступ, Bluetooth і Wi-Fi, вбудований модем, датчики, інфотейнмент або застосунок для смартфонів, а також множина підключень із використанням телеметричних та інших хмарних систем, що мають доступ до систем автомобіля.

Що зазвичай відбувається під час традиційної IT-атаки на підключений автомобіль? Фірма Trend Micro Incorporated проаналізували чотири тематичні дослідження віддаленого злому автомобілів (Jeep Hack 2015, Tesla Hack 2016 та 2017 та BMW Hack 2018) та виявили закономірність, за якою слідували ці атаки (рис. 1) [9].

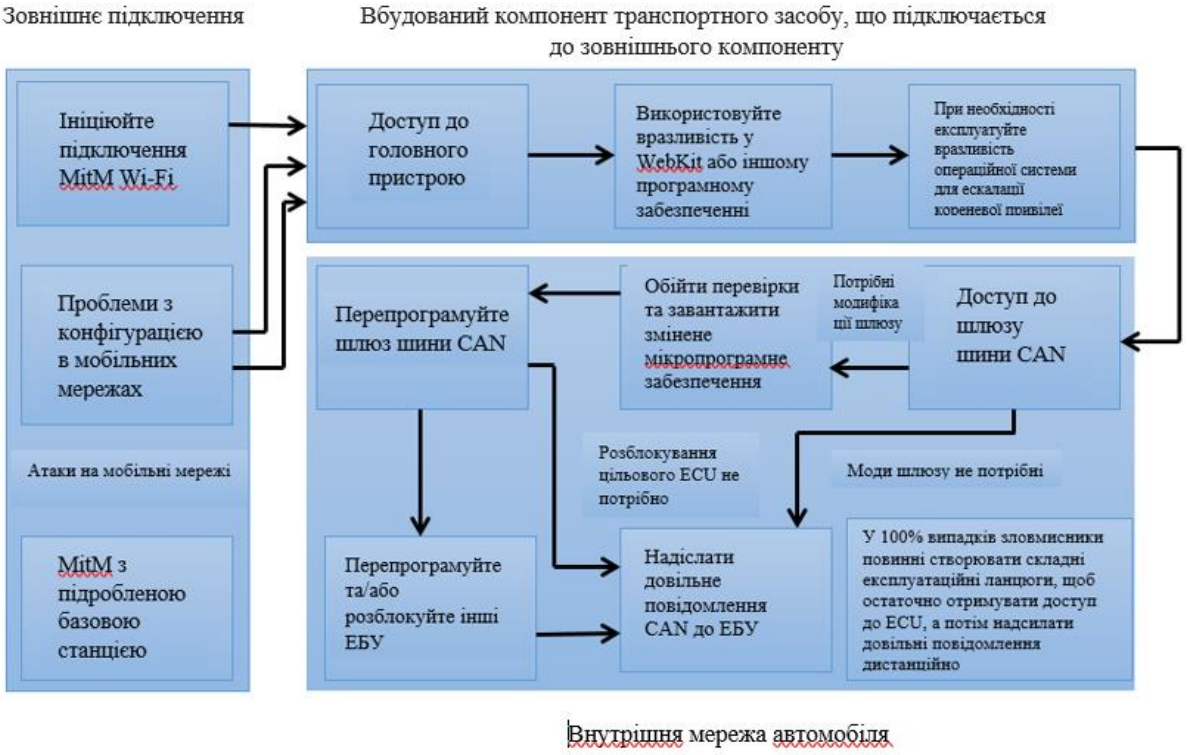

Рис. 1. Узагальнений ланцюг віддалених атак хакерів на основі тематичних досліджень віддалених атак

Нагода для оптимізму полягає в тому, що в галузі автомобільної кібербезпеки все більше робиться для оснащення автомобіля власним апаратним і програмним забезпеченням, а також для розвитку хмарових платформ, що забезпечують кібербезпеку. Формується декілька стандартів і регламентів, які регулюють кібербезпеку, що додатково сприяють розгортанню кіберзахисних рішень у всіх автомобілях, які підключаються.

Кібербезпека автомобіля: поточний стан

Компанія Upstream Security надрукувала декілька різних звітів з аналізом кібератак на автомобілі. Новітній із цих звітів, виданий на початку 2021 р. (за адресою: https://upstream.auto/2021report/) містить інформацію за період з 2010 до 2020 рр. і розглядає понад 200 кіберінцидентів з автомобілями по всьому світу. Звіт містить інформацію про глибокі мережі та даркнет (*DarkNet* – прихована мережа), де кіберзлочинці, які спеціалізуються на автомобілях, мають можливість спілкуватися, зберігаючи значну анонімність. Існують форуми, де детально обговорюють атаки на підключені транспортні засоби, доступ до конфіденційних даних, перехват управління автомобілем та способи угону машини. Навіть у «поверхневому» вебі кіберзлочинці часто знаходять інтернет-магазини, що торгують інструментами для зламу, сервісами, які відключають імобілайзери, кодграбберами, а також довідками щодо угону машини.

Таблиця 1 – Напрямок атак на автомобільному транспорті за 2010–2020 рр. від Upstream Security

Апаратні або програмні компоненти	Доля від цілого
Хмарні сервери	32,9 %
Безключовий доступ / брелок для ключів	25,3 %
Мобільний застосунок	9,9 %
Порт комп'ютерної діагностики автомобіля	32,9 %
Система інфотейнменту (мультимедійний інтерфейс)	8,4 %
ІТ-система	7 %
Датчики	4,8 %
Шлюз між блоками управління електронікою та телематикою	4,3 %
Бортова мережа	3,8 %

Із табл. 1 чітко видно, що найбільш популярні дві цілі: хмарні сервери (бо вони є воротами для 33 % усіх кібератак, оскільки хакери намагаються отримати доступ до цінних паперів, що можуть бути використані для зламу кіберзахисту автомобіля) та незахищений безключовий доступ (електронні брелоки також часто застосовуються для проникнення в машину та угону). Замикають трійку мобільні застосунки: через них здійснюється близько 10 % кібератак. Цікаво, що сумарна доля віддалених атак становить приблизно 80 %, а доля фізичних атак – близько 20 %.

У лютому 2021 р. Агентство з мережної та інформаційної безпеки Євросоюзу (ENISA) надрукувала документ «Виклики кібербезпеки, які зв'язані з упровадженням штучного інтелекту в автономному водінні». Звіт дозволяє скласти враження про виклики кібербезпеки, пов'язані з використанням ШІ-технологій (технологій штучного інтелекту) в автомобілях. Проблема описана в контексті політики, що реалізується як на європейському, так і більш широкому, міжнародному рівні.

У листопаді 2019 р. ENISA надрукувала документ «Рекомендації про забезпечення інформаційної безпеки розумних автомобілів», в якому визначені практики, що рекомендуються для забезпечення безпеки підключених автомобілів та напівавтономних транспортних засобів. А 2017 р. ENISA надрукувала документ «Кібербезпека та надійність розумних автомобілів», в якому основна увага приділена практикам, що рекомендуються для виробників автомобільних комплектуючих та для їхніх постачальників із метою захисту автомобільних систем, що встановлюються, від кібератак.

Основна вимога до стандартів та регламентів у галузі кібербезпеки – захистити автомобіль протягом усього його життєвого циклу – від проєктування до виробництва й далі до використання клієнтом.

Після дворічної підготовки та редагування ООН 24 червня 2020 р. прийняла документ WP/29 ЕЄК, який регулює питання кібербезпеки. WP.29 діє у 54 країнах, зокрема ЄС, Великої Британії, Японії та Південної Кореї. На ці 54 країни доводиться близько 35 % світового виробництва автомобілів. У багатьох інших країнах приймаються автомобілі, що відповідають нормам ООН. США не входять до складу цих 54 країн. Усі виробничники, зокрема автовиробники із США, які продають автомобілі на світових ринках, мають дотримуватися вимог кібербезпеки, що викладені в WP.29 щодо всієї їхньої продукції та процесів. Регламенти ООН є юридично забезпеченими. Якщо країна або регіон приймає регламент WP.29, то від усіх діючих у ній виробників комплектуючих вимагається доказ відповідності для проходження обов'язкової сертифікації та подальшого права працювати на ринку. У Європі проходження обов'язкової сертифікації вимагає взаємного визнання відповідно до нормам на рівні всього автомобіля. Якщо виробник отримує сертифікат на автомобіль визначеного типу в одній країні ЄС, то може продавати таку модель у всіх країнах ЄС без подальших перевірок.

У червні 2020 р. були прийняті дві нові регламентні норми ООН щодо кібербезпеки в межах документа WP.29. Дві норми, що застосовуються до транспортних засобів усіх типів, були оновлені в березні 2021 р. Упровадження цих норм у деяких країнах починається 2021 р. і 2022 р., а найбільш широке впровадження відбудеться 2023 р. і 2024 р. *У першому документі* основна увага приділяється кібербезпеці й системам управління кібербезпекою (CSMS). Останнє оновлення документа CSMS можна знайти за адресою: https://unece.org/sites/default/files/2021-03/R155e.pdf.

Під CSMS розуміється системний підхід на основі оцінки ризиків, що визначають організаційні процеси, зони відповідальності та управління для правильного тлумачення ризиків, пов'язаних із кіберзагрозами транспортним засобам та їхнім захистом від кібератак. У документі CSMS детально розглянуті загрози, пов'язані з кібербезпекою, та наведена значна кількість прикладів нападів і методів кібератаки. У додатку 5 міститься 10 аркушів з описом вразливостей, розподілених за множинними категоріями. У першій із таблиць документа CSMS, який наводиться за вищевказаною адресою, узагальнені загрози й вразливості. Існують шість типів загроз та множина типів вразливостей (29) з великою кількістю прикладів (67), що перелічені в документі CSMS. Другий документ стосується процесів оновлення програмного забезпечення та систем управління актуальними оновленнями (SUMS). Документ SUMS доступний за адресою:
https://unece.org/sites/default/files/2021-03/R156e.pdf.

У ньому наводиться система управління оновленнями програм як системний підхід, що визначає, які організаційні процеси й процедури мають відповідати вимогам за доставку програмних оновлень згідно із цим регламентним документом. Нова норма ООН про універсальні передумови до оновлень програм і систем управління оновленнями програм стосується автомобілів, робота яких залежить від оновлення програмного забезпечення. Ця норма стосується трейлерів і сільської господарчої техніки, а також пасажирського транспорту, фургонів, грузовиків і автобусів.

Цілі сталого розвитку та стандарти ISO

Цілі сталого розвитку є амбіційним планом для укріплення миру та процвітання, викоренення зубожіння та захисту планети [10]. Цілі сталого розвитку визнані скрізь як першочергові для майбутнього нашого світу. Вони містять заклик до всіх елементів суспільства, зокрема до місцевих і національних урядів, ділових кіл, промисловості та окремих осіб. Для досягнення більш ефективних показників необхідно досягнути консенсусу, ефективної взаємодії та інновацій. ISO надрукувала понад 22 000 міжнародних стандартів і пов'язаних із ними документів, що є міжнародними визнаними керівними принципами й структурою змісту, що основані на міжнародному співробітництві. Основані на консенсусі, вони є підґрунтям для інновацій, а також важливими інструментами, що допомагають урядам, промисловості й споживачам робити внесок у досягнення кожної з цілей сталого розвитку.

Стандарт ISO/SAE 21434 встановлює межі кібербезпеки для автомобільних компаній і містить єдину термінологію для спілкування та управління ризиками, що пов'язані з кібербезпекою. Незважаючи на те, що зазначене не належить безпосередньо до технологій як таких і не сприяє їхньому впровадженню, надані межі розширюють співробітництво у сфері кібербезпеки в галузі автотранспорту й таким чином приведуть до появи технологій і рішень, що краще відповідатимуть проблемам кібербезпеки сьогодні й у майбутньому. Це допоможе розглядати проблеми кібербезпеки на кожному етапі процесу розроблення та в польових умовах, створювати контрольний лист для інженерів, що передбачають сканування на наявність помилок, збільшення кількості власних засобів кіберзахисту й проведення аналізу ризиків потенційних вразливостей за кожним компонентом. Стандарт ISO/SAE 21434 вже задіяний для підтримки чинних правил.

З метою подальшого покращення взаємозв'язку між регулюванням та стандартизацією в Організації Об'єднаних Націй нещодавно почалась робота над загальнодоступною специфікацією ISO/PAS 5112, в якій містяться вказівки керівництву організацій з організаційних аудитів щодо інженерних аспектів кібербезпеки. Вона буде основана на стандарті ISO/SAE 21434 і призначена для проведення аудиту систем управління кібербезпекою, як це визначено в постанові ООН.

Майбутній стандарт призначений покращити кібербезпеку автомобілів і знизити ризики за всією довжиною ланцюга постачання – від розроблення й проєктування автомобілів до їхнього введення в експлуатацію. Багато представників галузі вже будують плани щодо забезпечення його інтеграції. Кінцевою метою є широке впровадження цього стандарту в повсякденну інженерну практику галузі поряд із підвищенням інформованості, яка досягається за рахунок включення вищезгаданого стандарту в навчальну програму підготовки інженерів.

Висновки

Унаслідок проведеного дослідження розглянута історія, поточний стан і сталий розвиток міжнародного співробітництва в сфері

кібербезпеки в автомобільній галузі, розглянута сукупність методів та практик захисту від атак зловмисників для забезпечення безперебійної роботи комп'ютерів, мобільних пристроїв, електронних систем, мереж і транспортних засобів та транспортної інфраструктури. Наведені посилання на основні міжнародні документи, що забезпечують безпеку транспортних засобів. Визначені проблеми, що мають привести до розроблення технологій із кібербезпеки в майбутньому.

Література

1. Касперский Е. Что такое кибербезопасность. URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security.
2. Кибербезопасность автомобилей. URL: https://www.iso.org/ru/news/ref2705.html.
3. Road Vehicles – Cybersecurity Engineering ISO/SAE21434. URL: https://www.sae.org/
4. standards/content/iso/sae21434/
5. В подключённом автомобиле главное – безопасность // Вестник ГЛОНАС. Межотраслевой журнал навигационных технологий. URL: http://vestnik-glonass.ru/news/avtonet/v-podklyuchyennom-avtomobile-glavnoe-bezopasnost/
6. Что такое «кибербезопасность транспорта». URL: https://trends.rbc.ru/trends/industry/614041579a79471ac5adba05.
7. Касперский Е. Кибербезопасность – новое измерение качества автомобилей. URL: https://www.kaspersky.ru/blog/cybersecurity-automotive/29026/
8. Касперский Е. Кибербезопасность – новое измерение качества автомобилей. доступа: URL: https://eugene.kaspersky.ru/2020/08/27/kiberbezopasnost-novoe-izmerenie-kachestva-avtomobilej/
9. Кибербезопасность? Да, теперь и ваша машина в зоне риска. URL: https://habr.com/ru/company/macloud/blog/564054/
10. In transit, interconnected, at risk. Cibersecurity Risks of Connected Cars. URL: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars.
11. Стандарты. Каким образом стандарты ИСО содействуют достижению цели устойчивого развития (ЦУР). URL: https://sabs.isolutions.iso.org/ru/sdgs.html.

References

1. E. Kaspersky. Chto takoe cyberbezopasnost. URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security.
2. Cyberbezopasnost avtomobiley. URL: https://www.iso.org/ru/news/ref2705.html.
3. Road Vehicles – Cybersecurity Engineering ISO/SAE21434. URL: https://www.sae.org/ standards/content/iso/sae21434/
4. V podkluchennom avtomobile glavnoe – bezopasnost // Vestnik GLONAC. Mezhotraslevoy zhurnal navigacionnikh tekhnologiy. URL: http://vestnik-glonass.ru/news/avtonet/v-podklyuchyennom-avtomobile-glavnoe-bezopasnost/
5. Chto takoe "cyberbezopasnost transporta". URL: https://trends.rbc.ru/trends/industry/614041579a79471ac5adba05.
6. Kaspersky E. Cyberbezopasnost – novoe izmerenie kachestva avtomobiley. URL: https://www.kaspersky.ru/blog/cybersecurity-automotive/29026/
7. Kaspersky E. Cyberbezopasnost – novoe izmerenie kachestva avtomobiley. URL: https://eugene.kaspersky.ru/2020/08/27/kiberbezopasnost-novoe-izmerenie-kachestva-avtomobilej/
8. Cyberbezopasnost? Da, teper i vacha machina v zone riska. URL: https://habr.com/ru/ company/macloud/blog/564054/
9. In transit, interconnected, at risk. Cibersecurity Risks of Connected Cars. URL: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars.
10. Standarti. Kakim obrazom standarti ISO sodeytvuut dostizheniu celi ustoychivogo razvitiya (CUR). URL: https://sabs.isolutions.iso.org/ru/sdgs.html.

Колодяжний Володимир Максимович, д.ф.-м.н., професор, професор кафедри інформатики і прикладної математики, Харківський національний автомобільно-дорожній університет,
61002, м. Харків, вул. Ярослава Мудрого, 25,
тел. (057)707-37-74, VladMax1949@ukr.net,
Левтеров Андрій Іванович, к.т.н., професор, завідувач кафедри інформатики і прикладної математики, Харківський національний автомобільно-дорожній університет,
61002, м. Харків, вул. Ярослава Мудрого, 25,
тел. (057)707-36-58, lai@khadi.kharkov.ua,
Малащук Євген Володимирович, фізична особа, підприємець, 04209, м. Київ, вул. Богатирська, 18А, кв. 31, тел. +380661930303, Yevgen.Malashchuk@gmail.com.

Cybersecurity in cars: history of digitalization of cars, current status of the problem, sustainable development goals and standards

Abstract. Problem. *At present, information security issues are a priority. The need for specialists with appropriate qualifications is growing, and educational institutions face the task of training students who plan to specialize in cybersecurity technologies, including cybersecurity of road transport and continue to work in the transport industry.* ***Goal.*** *The purpose of this article is to consider the history,*

current state of the problem and sustainable development of international cooperation in the field of cybersecurity in the automotive industry, which may be of interest to prospective students in choosing training to solve the problems of cybersecurity in road transport. ***Method.*** *This paper examines the history, current state of the problem and possible developments that may be interesting to future students in choosing the direction of training to address cybersecurity in the automobile industry. Cybersecurity in automotive construction is much more complex than on smartphones and personal computers, for two main reasons:*

a) dozens of EBCs in each vehicle, connected by a set of electronic bases and responsible for different functions and characteristics;

b) many potential access points, both located inside the car and remote, in particular, OBDII, USB and SD ports, without key access, Bluetooth and Wi-Fi, built-in modem, sensors, infotainment or smartphone application, and many connections using telemetry and other cloud systems that have access to car systems.

The reason for optimism is that in the field of automotive cybersecurity, more and more is being done to equip the car with its own hardware and software, as well as to develop cloud platforms that provide cybersecurity. Several standards and regulations are being developed to regulate cybersecurity, which further facilitates the deployment of cyber security solutions in all connected vehicles. ***Results.*** *As a result of the study, the history, current state of the problem and sustainable development of international cooperation in the field of cybersecurity in the automotive industry were investigated and a set of methods and practices were developed to protect against attackers to ensure the smooth operation of computers, mobile devices, electronic systems, networks and data means and transport infrastructure.* ***Practical significance.*** *References are made to the main international documents that provide the safety of vehicles. The problems that should lead to the development of cybersecurity technologies in the future are pointed out.*

Key words: *car cybersecurity, personal data security, cyber-attack protection, artificial intelligence technologies in cars.*

Kolodyazhny Vladimir, Dr.Sc., Phys.-Math., Professor, Professor, of the Department of Informatics and Applied Mathematics, Kharkiv National Automobile and Highway University, 25 Yaroslava Mudrogo, Kharkiv, 61002, Ukraine, +380577073658, e-mail: VladMax1949@urk.net,

Levterov Andriy, PhD in Technical Sciences, Professor, Head of the Department of Informatics and Applied Mathematics, Kharkiv National Automobile and Highway University, 25 Yaroslava Mudroho, Kharkiv, 61002, Ukraine, +380577073658,
e-mail: lai@khadi.kharkov.ua,

Malashchuk Evgen, Individual entrepreneur, Bogatyrska street 18A, apartment 31, Kyiv, 04209, Ukraine, +380661930303,
e-mail: Yevgen.Malashchuk@gmail.com.