УДК 004.65:621.391.7

к.т.н., доц. **Гуменний Д. О.** (КНУБА)
Кузін О. М. (N-iX Corp., Freelancer)
д.т.н., проф. **Хлапонін Ю.І.** (КНУБА)

DOI: https://doi.org/10.17721/2519-481X/2023/79-09

КРИТЕРІЇ ISO 21434 ДЛЯ ФОРМУВАННЯ СИСТЕМНИХ СПЕЦИФІКАЦІЙ У ПРОЦЕСАХ A-SPICE ДЛЯ АВТОМОБІЛІВ

Зі зростанням присутності електроніки та автономних систем у сучасних автомобілях кібербезпека стала критично важливою проблемою. Виробники автомобілів та інші зацікавлені сторони активно шукають способи забезпечення надійного захисту від кібератак. Один з підходів полягає у використанні стандарту ISO 21434, який призначений для підвищення кібербезпеки в автомобільній промисловості. Ця наукова стаття досліджує стандарт ISO 21434 та його застосування в галузі автомобільного виробництва, зокрема у розробці програмного забезпечення в рамках стандарту A-SPICE. Публікація описує методи та концепції, які використовуються для покращення кібербезпеки в автомобільній промисловості, та встановлює роль стандарту ISO 21434 в моделі A-SPICE. Висновки дослідження є цінними для компаній та фахівців, які займаються розробкою та впровадженням заходів з кібербезпеки в автомобільному секторі. Впровадження стандарту ISO 21434 може зменшити ризик кібератак та покращити якість та надійність автомобілів, зробивши автомобільну промисловість безпечнішою та надійнішою для споживачів. Стаття надає огляд основних стандартів кібербезпеки в автомобільній промисловості. ISO 26262 визначає процеси та вимоги щодо функціональної безпеки в автомобільних системах, включаючи аспекти кібербезпеки. SAE J3061 акцентує увагу на управлінні кібербезпекою в електронних системах транспортних засобів і широко використовується в галузі. ISO/SAE 21434, введений у 2020 році, замінює попередній стандарт ISO 26262 та встановлює вимоги до кібербезпеки в автомобільній промисловості. Ці стандарти тісно пов'язані, оскільки спрямовані на забезпечення безпеки та захищеності автомобільних виробів.

У висновку, включення критеріїв ISO 21434 у процес розробки програмного забезпечення для автомобілів значно впливає на якість та безпеку продуктів. Дослідження показує, що застосування критеріїв ISO 21434 дозволяє здійснювати систематичний та структурований підхід до розробки програмного забезпечення, забезпечуючи надійність, безпеку та відповідність програмних продуктів регулятивним вимогам в автомобільній промисловості. Стаття надає аналіз стандартів, методів та підходів, що використовуються в автомобільній галузі, і висвітлює вплив ISO 21434 на фреймворк A-SPICE, визначаючи його положення в рамках моделі. В цілому, ця публікація сприяє розвитку знань у сфері кібербезпеки автомобілів.

Ключові слова: Автомобільна промисловість, кібербезпека, структура A-SPICE, стандарт ISO 21434, специфікація системи.

Вступ. Кібербезпека стає актуальною в сучасних автомобілях, які містять все більше електроніки та автономних систем. У зв'язку з цим, виробники автомобілів та інші зацікавлені сторони шукають способи забезпечення надійного захисту від кібератак [1]. Один з таких способів - використання стандарту ISO 21434 [2], який спрямований на забезпечення кібербезпеки в автомобільній промисловості.

У цій статті проведено дослідження стандарту ISO 21434 та його застосування в галузі автомобільного виробництва, зокрема у виробництві програмного забезпечення за стандартом A-SPICE. Також у публікації описано методи та концепції, що використовуються для забезпечення кібербезпеки в автомобільній галузі, а також встановлено місце стандарту ISO 21434 в A-SPICE моделі.

Результати дослідження можуть бути корисними для компаній та фахівців, що займаються розробкою та впровадженням заходів кібербезпеки в автомобільній галузі. Застосування стандарту ISO 21434 дозволить зменшити ризик кібератак та підвищити якість та надійність автомобілів, що, у свою чергу, зробити автомобільну галузь більш безпечною та довіреною для споживачів [3, 4].

Огляд основних стандартів кібербезпеки автомобільної галузі

Для забезпечення безпеки та надійності автомобільних продуктів, на ринку існує декілька важливих стандартів, що регулюють питання кібербезпеки. Деякі з найбільш важливих стандартів, які пов'язані з кібербезпекою у автомобільній сфері, описані нижче:

- ISO 26262: Цей стандарт описує процеси та вимоги до функціональної безпеки в автомобільній галузі. Він встановлює вимоги до безпеки електронних систем управління в автомобілях та включає в себе вимоги до кібербезпеки [4, 6].

- ISO 26262 став основоположником у визначенні вимог до безпеки електронних систем управління автомобілями [5, 6].

- SAE J3061: Цей стандарт створений для керування кібербезпеою в автомобільній галузі. Він включає в себе рекомендації з управління ризиками та забезпечення кібербезпеки в електронних системах автомобілів. Цей стандарт є широко використовуваним у галузі та є важливим для забезпечення кібербезпеки в автомобільних продуктах [7].

- ISO/SAE 21434: Новий стандарт ISO/SAE 21434, який був запроваджений у 2020 році, встановлює вимоги до кібербезпеки в автомобільній галузі та замінює старий стандарт ISO 26262 [7, 8].

Впровадження заходів з функціональної безпеки є важливим для мінімізації ризику виникнення аварій, спричинених відмовою систем у транспортних засобах. ISO 26262 та ISO 21434 тісно пов'язані, оскільки обидва стандарти мають на меті забезпечити безпеку та захищеність автомобільних продуктів [6].

Крім того, фреймворк Automotive SPICE (Software Process Improvement and Capability Determination) є застосовуваний для оцінки та покращення процесів розробки програмного забезпечення в автомобільній галузі. A-SPICE, конкретний варіант Automotive SPICE, забезпечує фреймворк для покращення процесів розробки програмного забезпечення в організаціях автомобільної галузі. ISO 21434 надає керівництво для діяльності, пов'язаної з кібербезпекою, в рамках фреймворку A-SPICE, підкреслюючи важливість систематичного та стандартизованого підходу до кібербезпеки.

Застосування ISO 21434 для виявлення ризиків проектування та розробки систем автомобіля

Для ефективної реалізації кібербезпеки у виробах автомобільної галузі, які розробляються відповідно до A-SPICE, важливо враховувати стандарт ISO 21434 та дотримуватись його вимог. Однак, просте дотримання стандарту може бути недостатньо для забезпечення високого рівня кібербезпеки у виробах [7].

Додаткові засоби, такі як методології ризик-аналізу та управління кібербезпекою, також можуть бути використані для забезпечення високої якості кібербезпеки у виробах. Результати ризик-аналізу можуть допомогти виявити слабкі місця в системі безпеки, що дозволить розробити ефективні заходи для їх усунення. Управління кібербезпекою дозволяє забезпечити відповідність вимогам стандарту на кожному етапі розробки виробу.

Стандарт ISO 21434 може бути застосований на різних етапах V-моделі розробки програмного забезпечення, зокрема, на етапах вимог, проектування та тестування.

Так, на етапі формування вимог, визначаються вимоги до кібербезпеки та врахувати їх у специфікації до системи чи програмного продукту.

На етапі проектування, виконується розробка архітектури з урахуванням вимог стандарту по кібербезпеці.

На етапі тестування, вирішується питання виконання вимог кібербезпеки та дослідити ефективність заходів з її забезпечення.

Застосування ISO 21434 показано на рис. 1 відповідно до списку, що наведений вище.

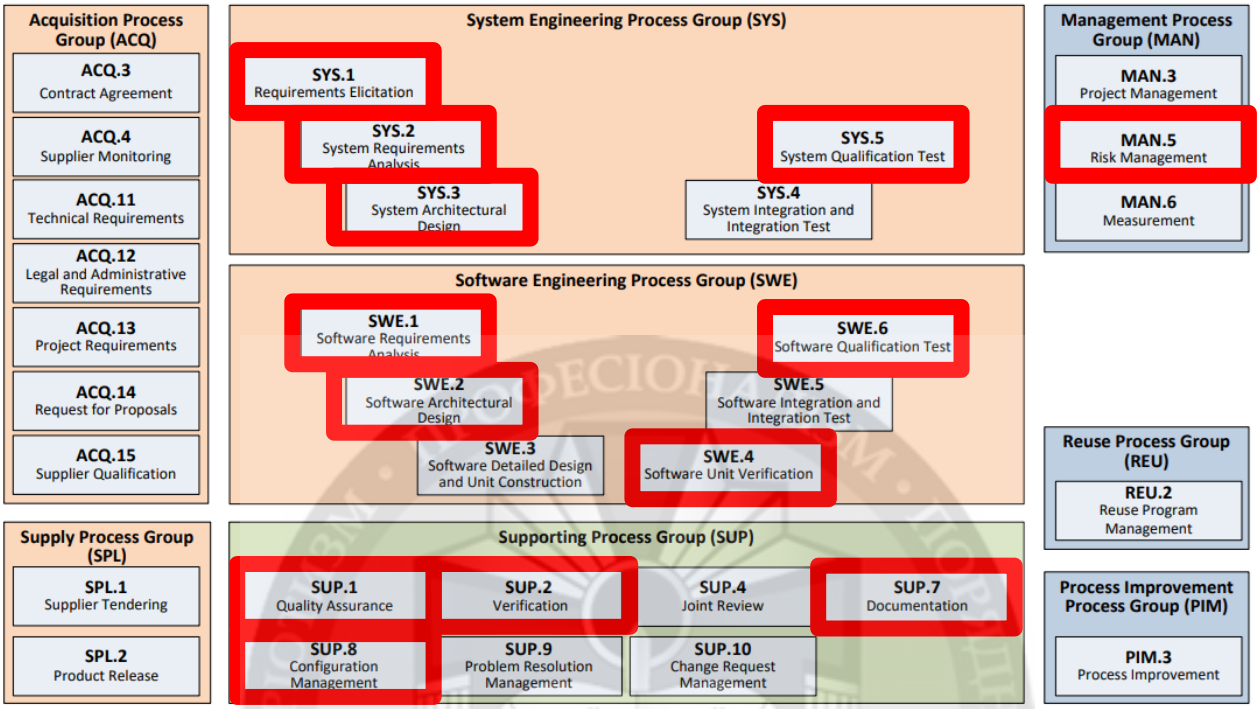

Рисунок 1 - Модифіковані процеси A-SPICE
для забезпечення відповідності до ISO 21434 (на базі Figure 2: Primary Life Cycle Processes, Organizational Life Cycle Processes, Supporting Life Cycle Processes (source: Automotive SPICE process reference model - Overview

З рис. 1 видно, що залучення ISO 21434 до A-SPICE реформує System Engineering Process Group, Software Engineering Process Group, Supporting Process Group, Management Process Group. Детальний опис реформування винесено з публікації.

Методи аналізу загроз для кібербезпеки

Очевидним є існування низки методів аналізу загроз та методів роботи з цими загрозами. Але, для роботи у автомобільній галузі можуть бути вилучені лише ті методи, що відповідають іншим ключовим вимогам, зокрема ISO 26262. До таких методів належать: Метод Ризик-аналізу, Методологія управління кібербезпекою, та Plan-Do-Check-Act" (PDCA).

Метод Ризик-аналізу

Ризик-аналіз є одним з ключових елементів управління кібербезпекою [9]. В основі цієї методології лежить процес визначення потенційних загроз безпеці та оцінки ризику, який пов'язаний з цими загрозами [9, 10].

Основні кроки методології ризик-аналізу включають визначення системи, яку необхідно захистити, виявлення потенційних загроз, визначення вразливостей системи, які можуть бути використані зловмисниками для здійснення атак, та оцінку можливого впливу таких атак на систему та її користувачів [11].

Для виявлення потенційних загроз можуть використовуватись різноманітні методи, включаючи аналіз документів, спостереження та тестування системи. Далі, визначені загрози

та вразливості системи оцінюються за допомогою різних метрик, таких як ймовірність виникнення загрози та її потенційний вплив.

Після визначення потенційних ризиків, необхідно визначити заходи, які можуть бути прийняті для зменшення цих ризиків. Ці заходи можуть включати в себе розробку технічних засобів захисту, впровадження політик безпеки, проведення навчання та підвищення свідомості користувачів, а також встановлення механізмів моніторингу та виявлення вторгнень [12]. Важливою частиною методології ризик-аналізу є постійне оновлення та перегляд заходів безпеки з метою забезпечення ефективного захисту системи [13].

Методологія управління кібербезпекою

Методологія управління кібербезпекою передбачає комплекс заходів, які забезпечують збір, обробку та аналіз інформації щодо потенційних загроз безпеці інформації та діяльності підприємства в цілому. Передбачається, що ці заходи будуть відповідати вимогам міжнародних стандартів, зокрема, ISO/IEC 27001:2013 [14].

Перший етап управління кібербезпекою полягає у визначенні цілей та завдань, які необхідно досягти для забезпечення безпеки інформації. Для цього використовуються методології SWOT-аналізу, який дозволяє визначити сильні та слабкі сторони підприємства, а також можливості та загрози [14, 15].

Другий етап передбачає визначення кібер безпекових ризиків, які можуть вплинути на безпеку інформації та діяльність підприємства в цілому. Для цього використовуються різноманітні методи ризик-аналізу, такі як аналіз відкритих джерел, оцінка ймовірності та впливу загроз, дослідження сценаріїв загроз та їх взаємозв'язків тощо [15].

Третій етап передбачає визначення стратегій та заходів щодо запобігання кібербезпеці. Для цього використовуються методи стратегічного планування, які дозволяють визначити найбільш ефективні способи захисту інформації та діяльності підприємства від кібератак та інших загроз [16].

Четвертий етап передбачає визначення системи контролю за застосуванням заходів з кібербезпеки та регулярний аудит системи [16].

Інші методи специфічні для автомобільної сфери

Для забезпечення ефективного управління кібербезпекою в автомобільній індустрії, використовуються різні методології, що допомагають організаціям забезпечити безпеку своїх продуктів та процесів.

Однією з таких методологій є "Plan-Do-Check-Act" (PDCA) [15, 16], яка є базовою моделлю управління якістю. Застосування цієї методології для управління кібербезпекою передбачає такі етапи:

Plan (планування): на цьому етапі здійснюється оцінка ризиків та визначаються заходи для запобігання та/або зменшення впливу можливих кібератак на систему. Основними завданнями на цьому етапі є: визначення обсягу та видів даних, що будуть захищатися; визначення вразливостей системи та визначення методів захисту; визначення потенційних загроз, які можуть виникнути в майбутньому;

Do (виконання): на цьому етапі здійснюється впровадження заходів, які були визначені на попередньому етапі;

Check (контроль): на цьому етапі здійснюється оцінка ефективності вжитих заходів та виявлення потенційних проблем;

Act (вдосконалення): на цьому етапі здійснюються відповідні корективи, з метою поліпшення ефективності системи кібербезпеки та запобігання виникненню нових проблем.

Іншою методологією управління кібербезпекою є "Cybersecurity Framework" (CSF), розроблена Національним інститутом стандартів і технологій США (NIST). CSF є фреймворком, який надає рекомендації щодо управління кібербезпекою. Цей фреймворк

складається з трьох основних елементів: цілей кібербезпеки, керівництва та описів рекомендованих практик.

Цілі кібербезпеки - це загальні цілі, які організації повинні визначити для досягнення оптимальної кібербезпеки. Ці цілі можуть включати забезпечення конфіденційності, цілісності та доступності даних, захист від кібератак та інші аспекти кібербезпеки.

Керівництво складається з вказівок та рекомендацій для організацій з питань управління кібербезпекою, таких як управління ризиками та інцидентами.

Описи рекомендованих практик - це набір практичних кроків, які організації можуть вживати для забезпечення кібербезпеки. Ці практики включаються у п'ять категорій: ідентифікація, захист, виявлення, відповідь та відновлення.

CSF може бути корисним інструментом для оцінки кібербезпеки виробів, що розробляються в автомобільній галузі згідно з ISO 21434 та відповідними стандартами A-SPICE. Використання цього фреймворку може допомогти визначити кібербезпеки цілі та розробити практичні кроки для їх досягнення, що забезпечує безпеку автомобільних виробів та захист від кіберзагроз [13].

Реорганізація системних специфікацій, вимог та імплементації з урахуванням ISO 21434

Для досягнення відповідності системних специфікацій, вимог та імплементацій згідно з A-SPICE до вимог ISO 21434 необхідно враховувати вплив цього стандарту на три основні складові процесу розробки автомобільних систем:

вимоги та специфікації,

архітектуру,

розробка та тестування.

Зазначений вище список реорганізації представлений на V-моделі як показано на рис. 2 по порядку спадання.

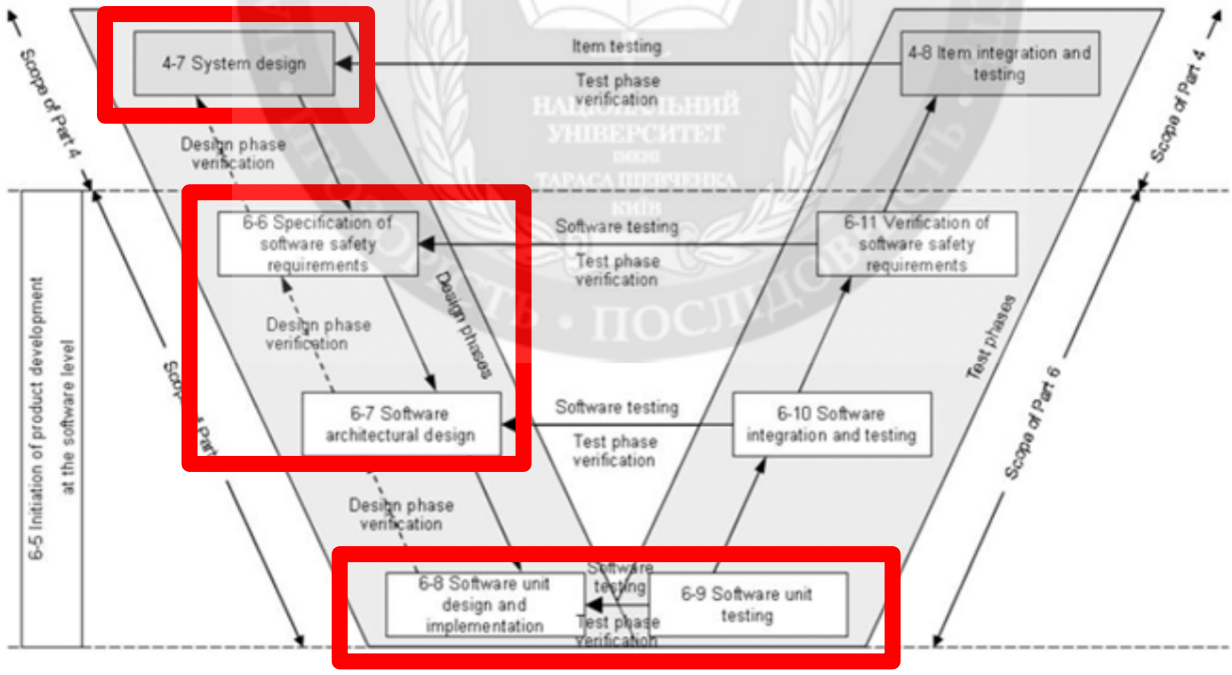

Рисунок 2 - Структурна реорганізація вимог,специфікацій, арітектури та імплементації автомобільного виробу для відповідності ISO 21434

Рекомендації до формування вимог та специфікацій з врахування ISO 21434

- Використання контексту системи та її інтерфейсів. Необхідно, аби команда проекту визначила контекст системи та всі зовнішні системи та структури, з якими вона має взаємодіяти. Це допоможе зрозуміти всі потенційні загрози та ризики, пов'язані з безпекою та іншими факторами, що впливають на систему.

- Використання структурованих методик розробки. Необхідно використовувати структуровані методики розробки систем для забезпечення якості та безпеки. Рекомендується використовувати процес розробки, який відповідає вимогам ISO 21434.

- Використання методології відслідковування вимог. необхідно використовувати методологію відслідковування вимог, щоб переконатися, що всі вимоги, що встановлені в специфікації, пов'язані з вимогами ISO 21434.

- Визначення стандартів безпеки. Необхідно визначити стандарти безпеки, які необхідні для розроблюваної системи. Необхідно, аби команди проекту дотримуватися цих стандартів та включати їх у системні специфікації.

- Використання інструментів верифікації. Необхідно використовувати інструменти верифікації, щоб переконатися, що всі вимоги специфікації були виконані. Відповідні інструменти мають бути сертифіковані згідно з ISO 21434.

Рекомендації до зміни у архітектурі програмного забезпечення з урахуванням ISO 21434

- Визначення основних вимог до архітектури системи згідно з вимогами ISO 21434.

- Використання структурованих методики проектування архітектури, такі як моделювання системи, щоб забезпечити високу якість архітектури та підвищити її пере використовування.

- Дотримання принципів безпеки при проектуванні архітектури, зокрема, при взаємодії компонентів системи та інтерфейсів між ними.

- Використання стандартизованих інтерфейсів та протоколів обміну даними між компонентами системи.

- Забезпечення можливості відстеження вимог до архітектури та її змін.

Проведення верифікації та валідації архітектури для підтвердження відповідності вимогам та відповідності стандартам безпеки.

Рекомендації до розробки та тестування програмного забезпечення з урахуванням ISO 21434

- Визначення вимоги до безпеки та критичності для програмного забезпечення згідно з вимогами ISO 21434.

- Використання структурованої методики проектування програмного забезпечення, такі як моделювання поведінки, щоб забезпечити високу якість коду та підвищити його перевикористовування.

- Дотримання принципів безпеки при розробці програмного забезпечення, зокрема, при взаємодії функцій та інтерфейсів між ними.

- Використання стандартизованих інтерфейси та протоколи обміну даними між компонентами програмного забезпечення.

- Забезпечення можливість відстеження вимог до програмного забезпечення та її змін.

- Врахування вимог до безпеки при виборі технологій та платформ для розробки та тестування програмного забезпечення.

- Забезпечення можливість валідації та верифікації програмного забезпечення для підтвердження відповідності вимогам безпеки та стандартам.

- Використання автоматизованих засобів тестування, такі як тести безпеки, тести навантаження та тести на відмову, для забезпечення якості програмного забезпечення.

- Забезпечення високої якість коду шляхом використання методів тестування, аудиту коду та іншими методами контролю якості.

- Забезпечення постійного моніторингу та оновлення програмного забезпечення, зокрема, щодо виявлення та усунення вразливостей та помилок.

Висновки. У заключенні можна зазначити, що включення критеріїв ISO 21434 до процесу розробки відповідних програмних засобів для автомобільної галузі значно впливає на якість та безпеку виробів. Дослідження показало, що застосування критеріїв ISO 21434 дозволяє більш системно та структуровано підходити до розробки програмного забезпечення. Це забезпечує надійність та безпеку програмних продуктів, а також відповідність регулятивним вимогам автомобільної галузі. У ході статті показаний аналіз стандартів, методів та підходів які використовуються в автомобільній промисловості. Також у статті визначено вплив стандарту ISO 21434 на фреймворк A-SPICE, визначаючи його позицію в моделі. В остаточному підсумку, публікація сприяє розвитку знань в галузі кібербезпеки автомобільної промисловості.

ЛІТЕРАТУРА (REFERENCES)

1. ISO 21434 Road vehicles - cybersecurity engineering : of 2021.08. URL: https://www.iso.org/standard/70918.html.

2. Synopsys, Inc. What is ASIL (Automotive Safety Integrity Level)? – Overview | Synopsys Automotive. *Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions.* URL: https://www.synopsys.com/automotive/what-is-asil.html.

3. Draft regulatory provisions on Cyber Security and Cyber Security Management System for Vehicles : of 11.03.2021. URL: https://unece.org/transport/events/wp29-world-forum-harmonization-vehicle-regulations-183rd-session.

4. Humennyi D., Starovierov K. Preparation of the acceptance criteria for functional safety software. Verification and Qualification of the product according to ISO 26262. *Abstracts of reports of participants of the first international scientific and practical conference " Law and Public Administration-the latest development trends"* : Scientific publication, Kyiv, 30–31 March 2022. Kyiv, 2022. P. 35–36.

5. A systematic review of security and privacy in connected vehicles / A. M. Abad et al. IEEE Communications Surveys & Tutorials. 2019. Vol. 21, no. 1. P. 607–631.

6. Humennyi D., Veselska O. Matlab Simulink model testing based on ISO 26262-6. *Abstracts of reports of participants of the first international scientific and practical conference " the latest technological trends in the intellectual industry and the internet of things"* : Scientific publication, Kyiv, 19–20 January 2022. Kyiv, 2022. P. 32–34.

7. Böhme R., Härder T., Köpsell S. Requirements and challenges for a trustworthy vehicle-to-everything communication. In Trustworthy Manufacturing and Utilization of Secure Devices. P. 165–183.

8. Robert Bosch GmbH. Software updates and cybersecurity. Bosch Mobility. URL: https://www.bosch-mobility.com/en/mobility-topics/software-updates-and-cybersecurity/.

9. Cyber Situational Awareness / ed. by S. Jajodia et al. Boston, MA : Springer US, 2010. 252 p. URL: https://doi.org/10.1007/978-1-4419-0140-8.

10. Kouns J., Pachecco F. Introduction to Risk Analysis in Cybersecurity.

11. Stoneburner G., Goguen A., Feringa A. Risk Management Guide for Information Technology Systems. Washington : Nist special publication, 800(30), 2002. 65 p. URL: https://doi.org/10.6028/NIST.SP.800-30r1.

12. Peltier T. R., Peltier J., Blackley J. Information Security Fundamentals. New York : Taylor & Francis Group, 2004. 262 p. URL: https://doi.org/10.1201/9780203488652.

13. The Art of Service - Cyber Security Risk Management Publishing. Cyber Security Risk Management A Complete Guide. The Art of Service - Cyber Security Risk Management Publishing, 2020. 318 p.

14. Alharbi M. S., Bourini A. G., Shouman M. M. A Survey on Cyber Security Risk Assessment Frameworks. *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA).* 2018. P. 1–6.

15. Teng J. H., Chung J. Y. Developing a Strategic Information Security Management Plan Using the ISO 27001 Standard. *Journal of Management and Sustainability.* 2015. Vol. 5, no. 3. P. 120–132.

16. van den Berg P. A., Dhillon G. S. Towards an integrated framework for cyber risk assessment. *Computers & Security*. 2018. No. 78. P. 230–243.

:

Ph.D. **Humennyi D.O., Kuzin O.M.,** D.Sci.Tech., prof. **Khlaponin Y.I.,**

USING THE ISO 21434 CRITERIA FOR GENERATING SYSTEM SPECIFICATIONS IN A-SPICE PROCESSES FOR CARS

With the increasing presence of electronics and autonomous systems in modern automobiles, cybersecurity has become a critical concern. Automotive manufacturers and other stakeholders are actively seeking ways to ensure reliable protection against cyber attacks. One approach involves the utilization of ISO 21434, a standard designed to enhance cybersecurity in the automotive industry. This research article investigates the ISO 21434 standard and its application in the field of automotive production, specifically in software development under the A-SPICE standard. The publication describes the methods and concepts used to enhance cybersecurity in the automotive industry and establishes the role of ISO 21434 within the A-SPICE model. The study's findings are valuable for companies and professionals involved in the development and implementation of cybersecurity measures in the automotive sector. Implementing the ISO 21434 standard can mitigate the risk of cyber attacks and improve the quality and reliability of automobiles, thus making the automotive industry safer and more trustworthy for consumers. The article provides an overview of key cybersecurity standards in the automotive industry. ISO 26262 sets out processes and requirements for functional safety in automotive systems, including cybersecurity considerations. SAE J3061 focuses on cybersecurity management in electronic systems of vehicles and is widely used in the industry. ISO/SAE 21434, introduced in 2020, replaces the previous ISO 26262 standard and specifies cybersecurity requirements in the automotive industry. These standards are closely related as they aim to ensure the safety and security of automotive products. Furthermore, the Automotive SPICE (Software Process Improvement and Capability Determination) framework is widely employed for evaluating and enhancing software development processes in the automotive sector. A-SPICE, a specific variant of Automotive SPICE, provides a framework for improving software development processes in automotive organizations. ISO 21434 guides cybersecurity activities within the A-SPICE framework, emphasizing the importance of a systematic and standardized approach to cybersecurity.

To effectively implement cybersecurity in automotive products developed under A-SPICE, compliance with the ISO 21434 standard is crucial. However, mere adherence to the standard may be insufficient for achieving a high level of cybersecurity. Additional tools such as risk analysis methodologies and cybersecurity management can be employed to ensure robust cybersecurity measures. Risk analysis results can help identify vulnerabilities in the security system, enabling the development of effective mitigation measures. Cybersecurity management ensures compliance with the standard throughout the product development lifecycle. ISO 21434 can be applied at various stages of the V-model software development process, including requirements definition, design, and testing. During requirements definition, cybersecurity requirements are identified and incorporated into the system or software specifications. In the design phase, architectures are developed considering the cybersecurity requirements outlined in the standard. The testing phase addresses the fulfillment of cybersecurity requirements and evaluates the effectiveness of cybersecurity measures. In conclusion, the inclusion of ISO 21434 criteria in the development process of automotive software significantly impacts the quality and safety of products. The research demonstrates that applying ISO 21434 criteria allows for a systematic and structured approach to software development, ensuring the reliability, safety, and compliance of software products with regulatory

requirements in the automotive industry. The article presents an analysis of standards, methods, and approaches used in the automotive industry and highlights the influence of ISO 21434 on the A-SPICE framework, defining its position within the model. Ultimately, this publication contributes to the advancement of knowledge in automotive cybersecurity.

Keywords: Automotive, Cybersecurity, A-SPICE framework, ISO 21434 standard, System specification