СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] В. С. Харченко, О. Н. Одарущенко, Ю. Л. Поночовний, Е. Б. Одарущенко и др., *Технологии высокой готовности для программно-технических комплексов космических систем:* монография, под ред. В. С. Харченко, Б. М. Конорева, Харьков, Украина: Нац. аэрокосм. ун-т им. Н. Е. Жуковского «ХАИ», 2010.

[2] A. Boyarchuk, V. Kharchenko, O. Odarushchenko and Y. Ponochovny. “Basic Models for Dependable Web-Services: Technique for Development and Research”, in *Dependability of Networks*: collective monograph, T. Walkowiak, J. Mazurkiewicz, J. Sugier, W. Zamojski, Eds. Wroclaw, Poland: Oficyna Wydawnicza Politechnki Wroclawskiej, 2010, pp. 27-38.

[3] Ю. Л. Поночовный и Е. Б. Одарущенко, “Имитационное моделирование процесса оценки надежности отказоустойчивых компьютерных систем информационно-управляющих комплексов”, *Радіоелектронні і комп’ютерні системи*. № 7, с. 68-74, 2007.

[4] А. А. Фурманов, В. С. Харченко и Ю. Л. Поночовний, “Метрики диверсности web-приложений с учётом уязвимостей”, *Вісник Хмельницького національного університету*, №4, с. 239-244, 2008.

[5] Ю. Л. Поночовный и А. О. Ивасюк, “Имитационное моделирование потоков злонамеренных воздействий на информационные системы”, *Системи обробки інформації*, Вип. 3, с. 123-125, 2008.

[6] Ю. Л. Поночовний, “Вибір методу комплексування показників надійності компонент інформаційних систем за похибкою, що вноситься”, *Системи озброєння і військова техніка*, № 4, с. 156-158, 2008.

[7] А. В. Боярчук, Ю. Л. Поночовный и В. С. Харченко, “Разработка и исследование базовых моделей отказоустойчивых WEB-сервисов”, *Радіоелектронні і комп’ютерні системи*, № 5. с. 42-49, 2010.

[8] В. С. Харченко, М. В. Замирець, С. О. Засуха та Ю. Л. Поночовний, “Елементи методології оперативної коригувальної верифікації програмних

засобів інформаційно-управляючих систем космічних апаратів", *Авіаційно-космічна техніка і технологія*, № 6, с. 81-95, 2011.

[9] С. А. Засуха и Ю. Л. Поночовный, "Модель готовности двухканальной информационно-управляющей системы космического аппарата с оперативной верификацией программных средств", *Наука і техніка Повітряних Сил Збройних Сил України*, № 2, с. 144-149, 2011.

[10] С. А. Засуха, Ю. Л. Поночовный и В. С. Харченко, "Методология оперативной верификации программного обеспечения космических систем: модели готовности и выбор сценариев", *Вісник ХНУ ім. В. Н. Каразіна*, № 1015, вип. 19, с. 131-147, 2012.

[11] Ю. Л. Поночовный, С. А. Засуха и В. С. Харченко, "Исследование имитационных моделей готовности двухканальной информационно-управляющей системы космического аппарата", *Радіоелектронні і комп'ютерні системи*, № 7, с. 41-47, 2012.

[12] А. М. Абдул-Хади, Ю. Л. Поночовный и В. С. Харченко, "Разработка базовых марковских моделей для исследования готовности коммерческих веб-сервисов", *Радіоелектронні і комп'ютерні системи*, № 5, с. 186-191, 2013.

[13] В. С. Харченко, А. М. Абдул-Хади и Ю. Л. Поночовный, "Формирование подмножеств уязвимостей доступности коммерческих веб-сервисов", *Системи обробки інформації*, Вип. 7, с. 112-115, 2013.

[14] Ю. Н. Соколов, В. С. Харченко и Ю. Л. Поночовный, "Инструментированное оценивание надежности программно-технических комплексов при росте интенсивности отказов", *Системи обробки інформації*, Вип. 2, с. 205-211, 2014.

[15] V. Kharchenko, Y. Ponochovnyi and A. Boyarchuk, "Availability Assessment of Information and Control Systems with Online Software Update and Verification", *Communications in Computer and Information Science*, vol. 469. pp. 300-324, 2014. doi: 10.1007/978-3-319-13206-8_15.

[16] Ю. Л. Поночовный, А. А. Сиора и В. С. Харченко, "Модели

готовности двухканальной информационно-управляющей системы с учетом обновления программных средств", *Радіоелектронні і комп'ютерні системи*, № 6, с. 135-139, 2014.

[17] Ю. Л. Поночовный, В. С. Харченко, Т. П. Межиборец, К. А. Ревенко и К. А. Шуст, "Применение дискретных законов распределения в модели доступности информационного ресурса с профилактическими мерами аудита безопасности", *Системи обробки інформації*, Вип. 9, с. 111-114, 2014.

[18] Ю. Л. Поночовный, А. В. Боярчук и В. С. Харченко, "Модели готовности веб-системы с учетом программных отказов и атак на уязвимости конфигурации службы DNS", *Системи обробки інформації*, Вип. 7, с. 122-127, 2015.

[19] Ю. Л. Поночовный, А. В. Боярчук и В. С. Харченко, "Имитационное моделирование веб-системы при атаках на уязвимости компонент и конфигураций", *Системи обробки інформації*, Вип. 8, с. 102-105, 2015.

[20] Ю. Л. Поночовный, А. В. Боярчук и В. С. Харченко, "Многофрагментные марковские модели отказоустойчивых Web-сервисов с устранением проектных дефектов", *Системи обробки інформації*, Вип. 11, с. 140-145, 2015.

[21] В. С. Харченко, Ю. Л. Поночовный, А. А. Фурманов и К. А. Васильев, "Модели развития уязвимостей IT-продуктов: патологические цепочки в контексте марковского анализа", *Системи обробки інформації*, Вип. 12, с. 114-119, 2015.

[22] А. О. Ивасюк, Ю. Л. Поночовный и Е. Н. Бульба, "Процедуры тестирования модулей информационно-управляющих систем на основе самодиагностируемых программируемых платформ с использованием засева дефектов", *Радіоелектронні і комп'ютерні системи*, № 6, с. 82-87, 2016.

[23] В. С. Харченко, Ю. Л. Поночовний, К. С. Вшивцева та К. Д. Безугла, "Розрахунок показників безвідмовності для IT-систем з

хмарною послугою NaaS”, *Системи обробки інформації*, Вип. 9, с. 177-181, 2016.

[24] В. С. Харченко, Мустафа Кахтан Абдулмунем Аль-Судани и Ю. Л. Поночовный, “Марковские модели готовности информационно-управляющей системы "умного" дома при раздельном и общем обслуживании по надежности и безопасности”, *Системи управління, навігації та зв'язку*, Вип. 4, с. 88-94, 2015.

[25] Мустафа Кахтан Абдулмунем Аль-Судані, В. С. Харченко та Ю. Л. Поночовний, “Метод мінімізації часу усунення дефектів і вразливостей в інформаційно-управляючій системі "розумного" будинку при загальному обслуговуванні по надійності і безпеці”, *Вісник ХНТУ ім. П. Василенка,* Вип. 176, с. 63-65, 2016.

[26] V. Kharchenko, Y. Ponochovnyi, A.-S. M. Q. Abdulmunem and A. Boyarchuk, “Security and availability models for smart building automation systems”, *Computing*, Vol. 16, Issue 4, pp. 194-202, 2017.

[27] В. С. Харченко, Ю. Л. Поночовний, А. В. Боярчук, І. О. Черницька та В. С. Воронянський, “Оцінювання готовності інформаційно-керуючої системи космічного апарату з усуненням програмних дефектів після проведення оперативної онлайн-верифікації”, *Радіоелектронні і комп’ютерні системи*, № 3, с. 49-55, 2017.

[28] Ю. Л. Поночовний, С. Ю. Рогочий, О. І. Шарай, В. О. Кнуренко та В. С. Воронянський, “Дослідження баз вразливостей для параметризації марковських моделей оцінювання доступності веб-ресурсів”, *Системи та технології*, № 1, с. 68-80, 2019. doi: 10.32836/2521-6643-2019-1-57-5.

[29] Ю. Л. Поночовний, “Аналіз концепцій управління кібербезпекою розподілених IT інфраструктур”, *Системи та технології*, № 2, с. 87-101, 2019. doi: 10.32836/2521-6643-2019-2-58-5.

[30] V. Kharchenko, S. Dotsenko, Y. Ponochovnyi and O. Illiashenko, “Cybernetic Approach to Developing Resilient Systems: Concept, Models and Application”, *Information & Security*, vol. 47, Issue 1, pp. 77-90, 2020. doi:

10.11610/isij.4705.

[31] Ю. Л. Поночовний та В. С. Харченко, “Методологія забезпечення гарантоздатності інформаційно-керуючих систем з використанням багатоцільових стратегій обслуговування”, *Радіоелектронні і комп’ютерні системи*, № 3, с. 43-58, 2020. doi: 10.32620/reks.2020.3.05.

[32] Ю. Л. Поночовний, С. В. Волошко та А. В. Боярчук, “Дослідження відмовостійких web-сервісів”, на *VI наук.-практ. сем. Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення*, Київ, 2011, с.164.

[33] V. Kharchenko, A.M. Abdul-Hadi, A. Boyarchuk and Y. Ponochovny, “Web Systems Availability Assessment Considering Attacks on Service Configuration Vulnerabilities”, In *IX Int. Conf. on Dependability and Complex Systems*. Brunów, Poland, 2014, pp. 275-284. doi: 10.1007/978-3-319-07013-1_26.

[34] V. Kharchenko, Y. Ponochovny, A. Boyarchuk and A. Gorbenko, “Scenario-Based Markovian Modeling of Web-System Availability Considering Attacks on Vulnerabilities”, In *XI Int. Conf. on ICT in Education, Research and Industrial Applications*, Lviv, 2015, pp. 566-577.

[35] V. Kharchenko, Y. Ponochovnyi, A. Boyarchuk and E. Brezhnev, “Resilience Assurance for Software-Based Space Systems with Online Patching: Two Cases”, In *XI Int. Conf. on Dependability and Complex Systems*, Brunów, Poland, 2016, pp. 267-278. doi: 10.1007/978-3-319-39639-2_23.

[36] Y. Bulba, Y. Ponochovny, V. Sklyar and A. Ivasiuk, “Classification and Research of the Reactor Protection Instrumentation and Control System Functional Safety Markov Models in a Normal Operation Mode”, In *XII Int. Conf. on ICT in Education, Research and Industrial Applications*, Kyiv, 2016, pp. 308-321.

[37] V. Kharchenko, Y. Ponochovnyi, A. Abdulmunem and A. Andrashov, “Availability Models and Maintenance Strategies for Smart Building Automation Systems Considering Attacks on Component Vulnerabilities”, In *XII Int. Conf. on Dependability and Complex Systems*, Brunów, Poland, 2017, pp. 186-195. doi: 10.1007/978-3-319-59415-6_18.

[38] Ю. Л. Поночовний, “Принцип успадкування характеристик, методів і моделей надійності, функціональної та інформаційної безпеки”, на *69-й наук. конф. професорів, викладачів, наукових працівників, аспірантів та студентів університету*, Полтава, 2017, с.139-140.

[39] Ю. Л. Поночовний, “Принцип динамічного моніторингу і прогнозування параметрів вразливостей компонент IT-інфраструктури”, на *VII міжн. наук.-техн. конф. Сучасні напрями розвитку ІКТ та засобів управління*, Кропивницький, 2017, с. 55.

[40] V. Kharchenko, Y. Ponochovnyi, A.-S.M.Q. Abdulmunem, A. Ivasiuk and O. Ivanchenko, “Model of Information and Control Systems in Smart Buildings with Separate Maintenance by Reliability and Security”, In *XIV Int. Conf. on ICT in Education, Research and Industrial Application*, Kyiv, Ukraine, 2018, pp. 583-595.

[41] Y. Ponochovniy, E. Bulba, A. Yanko and E. Hozbenko, “Influence of diagnostics errors on safety: Indicators and requirements”, In *IX Int. Conf. on Dependable Systems, Services and Technologies*, Kyiv, Ukraine, 2018, pp. 53-57. doi: 10.1109/DESSERT.2018.8409098.

[42] V. Kharchenko, Y. Ponochovnyi, A. Boyarchuk, E. Brezhnev and A. Andrashov, “Monte-Carlo Simulation and Availability Assessment of the Smart Building Automation Systems Considering Component Failures and Attacks on Vulnerabilities”, In *XIII Int. Conf. on Dependability and Complex Systems*, Brunów, Poland, 2018, pp. 270-280. doi: 10.1007/978-3-319-91446-6_26.

[43] V. Kharchenko, Y. Ponochovnyi, A. Boyarchuk and A. Andrashov, “Multi-Fragmental Markov Models of Information and Control Systems Safety Considering Elimination of Hardware-Software Faults”, In *XV Int. Conf. on ICT in Education, Research and Industrial Applications*, Kherson, 2019, pp. 738-748.

[44] V. Kharchenko, Y. Ponochovnyi, A. Andrashov, E. Brezhniev and E. Bulba, “Modelling and Safety Assessment of Programmable Platform Based Information and Control Systems Considering Hidden Physical and Design Faults”, In *XIV Int. Conf. on Dependability of Computer Systems*, Brunów, Poland, 2019, pp. 264-273. doi: 10.1007/978-3-030-19501-4_26.

[45] V. Kharchenko, Y. Ponochovnyi, A. Boyarchuk, A. Andrashov and I. Rudenko, “Multi-fragmental Markov’s Models for Safety Assessment of NPP I&C System Considering Migration of Hidden Failures”, In *Communications in Computer and Information Science, CCIS-1175*, Kherson, 2020, pp. 302-326. doi: 10.1007/978-3-030-39459-2_14.

[46] V. Kharchenko, Y. Ponochovniy, A. M. Q. Abdulmunem and I. Shulga, “AvTA Based Assessment of Dependability Considering Recovery After Failures and Attacks on Vulnerabilities”, In *X Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems*, Metz, France, 2019, pp. 1036-1040. doi: 10.1109/IDAACS.2019.8924251.

[47] A. Avizienis, J. C. Laprie, B. Randell and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing”, in *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11-33, 2004, doi: 10.1109/TDSC.2004.2.

[48] International Electrotechnical Commission. (2015-02-26). *IEC 60050-192. International electrotechnical vocabulary – Part 192: Dependability*. [Online]. Available: https://webstore.iec.ch/publication/21886.

[49] В. С. Харченко, “Гарантоздатні системи та багатоверсійні обчислення: аспекти еволюції”, *Радіоелектронні і комп’ютерні системи*, № 7, с. 46-59, 2009.

[50] V. Kharchenko, V. Sklyar and A. Siora, “Dependability of Safety-Critical Computer Systems through Component-Based Evolution”, In *2009 Fourth Int. Conf. on Dependability of Computer Systems*, Brunow, Poland, 2009, pp. 42-49. doi: 10.1109/DepCoS-RELCOMEX.2009.22.

[51] Dongyan Chen, S. Garg, C. Kintala and K. S. Trivedi, “Dependability enhancement for IEEE 802.11 wireless LAN with redundancy techniques”, In *2003 Int. Conf. on Dependable Systems and Networks*, San Francisco, CA, USA, 2003, pp. 521-528. doi: 10.1109/DSN.2003.1209962.

[52] D. M. Nicol, W. H. Sanders and K. S. Trivedi, “Model-based evaluation: from dependability to security”, in *IEEE Transactions on Dependable*

and Secure Computing, vol. 1, no. 1, pp. 48-65, 2004. doi: 10.1109/TDSC.2004.11.

[53] A. Avizienis, J-C. Laprie and B. Randell, “Fundamental Concepts of Dependability”, *Newcastle University Report*, no. CS-TR-739, 2001.

[54] В. С. Харченко та ін., *Забезпечення функціональної безпеки критичних інформаційно-керуючих систем: монографія*, Харків, Україна: Константа, 2019.

[55] Г. С. Теслер, “Концепция построения гарантоспособных вычислительных систем”, *Мат. машини і системи*, № 1, с. 134-145, 2006.

[56] Г. С. Теслер, “Решение проблем гарантоспособности и отказоустойчивости систем в аспекте базисов компьютерной науки”, *Математичні машини і системи*, № 4, с. 171-188, 2008.

[57] Г. С. Теслер, “Концепция создания вычислительных средств с высоким уровнем отказоустойчивости”, *Математичні машини і системи*, № 2, с. 176-183, 2002.

[58] В. Глухов, “Оцінювання гарантоздатності криптографічних комп'ютерних систем”, *Вісн. Нац. ун-ту "Львів. політехніка"*, № 616, с. 66-72, 2008.

[59] В. С. Глухов и Р. Ильяс, “Кодирование состояний управляющих автоматов в гарантоспособных системах”, *Радіоелектронні і комп’ютерні системи*, № 5, с. 91-95, 2009.

[60] В. С. Глухов и М. В. Ногаль, “Спеціалізований однорозрядний процесор для захисту інформації в гарантоздатних системах”, *Радіоелектронні і комп’ютерні системи,* № 5, с. 104-108, 2008.

[61] А. В. Федухин и Б. Г. Мудла, “Гарантоспособность компьютерных систем – мода или объективная необходимость”, *Математичні машини і системи*, № 4, с. 179-188, 2014.

[62] А. В. Федухин и Н. В. Сеспедес-Гарсия, “Моделирование надежности невосстанавливаемой системы со структурой типа "k из n" с реконфигурацией”, *Радіоелектронні і комп’ютерні системи*, № 7, с. 82-84, 2009.

[63] А. В. Федухин и Н. В. Сеспедес-Гарсия, “Атрибуты и метрики гарантоспособных компьютерных систем”, *Математичні машини і системи*, № 2, с. 195-201, 2013.

[64] В. В. Ковтун, *Моделі атрибутів гарантоздатності інформаційної системи критичного застосування із автентифікацією суб’єкта за голосом: монографія,* Вінниця, Україна: ВНТУ, 2020.

[65] А. О. Береза, Т. В. Грищук та В. В. Ковтун, “Оцінювання надійності сеансу розпізнавання особи автоматизованою системою розпізнавання мовця критичного застосування”, *Вісник Хмельницького національного університету. Технічні науки*, № 6(1), с. 143-150, 2018.

[66] И. Б. Шубинский, *Функциональная надежность информационных систем. Методы анализа,* Ульяновск, РФ: Печатный двор, 2012.

[67] И. Б. Шубинский, *Надежные отказоустойчивые информационные системы. Методы синтеза*, Ульяновск, РФ: Печатный двор, 2016.

[68] И. Б. Шубинский, “Методы обеспечения функциональной надежности программ”, *Надежность*, №4(51), с. 87-94, 2014.

[69] С. М. Лисенко, В. С. Харченко, К. Ю. Бобровнікова та Р. В. Щука, “Резильєнтність комп’ютерних систем в умовах кіберзагроз: таксономія та онтологія”, *Радіоелектронні і комп’ютерні системи*, № 1, с. 17-28, 2020. doi: 10.32620/reks.2020.1.02.

[70] National Institute of Standards and Technology. (2020-09-23). *Special Publication 800-53. Security And Privacy Controls For Federal Information Systems And Organizations*, 2020. doi: 10.6028/NIST.SP.800-53r5.

[71] National Institute of Standards and Technology. (2002-01-07). *Special Publication 800-30. Guide For Conducting Risk Assessments,* 2012. doi: 10.6028/nist.sp.800-30r1.

[72] Держстандарт України. (1996-01-01). *ДСТУ 2860-94. Надійність техніки. Терміни та визначення*. [Електронний ресурс]. Доступно: https://er.nau.edu.ua/bitstream/NAU/30417/3/DSTU%202860-94u.doc.

[73] K. S. Trivedi and A. Bobbio, *Reliability and Availability Engineering. Modeling, Analysis and Applications,* Cambridge, United Kingdom: Cambridge University Press, 2017. doi: 10.1017/9781316163047.

[74] А. В. Горбенко, “Проблемы и задачи создания гарантоспособных сервис-ориентированных web-систем”, на*ука і техніка Повітряних Сил Збройних Сил України*, № 3, с. 171-176, 2013.

[75] О. О. Ілляшенко, М. О. Колісник, А. А. Стрєлкіна та І. В. Коцюба, *Методи та технології розроблення та впровадження гарантоздатних систем на основі Інтернету речей. Наукова робота представлена на здобуття премії Президента України для молодих учених*. [Електронний ресурс]. Доступно: http://www.kdpu-nt.gov.ua/sites/default/files/work_files/prezentaciya_1.pdf. Дата звернення: 15-10-2020.

[76] International Electrotechnical Commission. (2010-04-30). *IEC 61508-1:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*. [Online]. Available: https://webstore.iec.ch/publication/5515.

[77] В. В. Скляр, “Анализ функциональной безопасности информационно управляющих систем с использованием логических моделей ошибок контроля и управления”, *Радіоелектронні і комп’ютерні системи*, № 7, с. 267-271, 2010.

[78] Society of Automotive Engineers International. (1996-12-01). *ARP4761. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment.* [Online]. Available: https://www.sae.org/standards/content/arp4761.

[79] International Civil Aviation Organization. (2013-11-14). *Operation of Aircraft. Convention on International Civil Aviation. Part I – International Commercial Air Transport – Aeroplanes.* [Online]. Available: https://www.icao.int/safety/fatiguemanagement/FRMS%20Tools/Amendment%2037%20for%20FRMS%20SARPS%20(en).pdf.

[80] Society of Automotive Engineers International. (2019-08-20).

ARP5151A. Safety Assessment of General Aviation Airplanes and Rotorcraft in Commercial Service. [Online]. Available: https://www.sae.org/standards/content/arp5151a.

[81] International Organization for Standardization. (2018-12-01). *ISO 26262-1:2018. Road vehicles – Functional safety – Part 1: Vocabulary.* [Online]. Available: https://www.iso.org/standard/68383.html.

[82] Society of Automotive Engineers International. (2020-07-08). *J2945/1A_202007. Vehicle Level Validation Test Procedures for V2V Safety Communications.* [Online]. Available: https://www.sae.org/standards/content/j2945/1a_202007.

[83] International Organization for Standardization. (2018-12-01). *ISO 26262-4:2018. Road vehicles – Functional safety – Part 4: Product development at the system level.* [Online]. Available: https://www.iso.org/standard/68386.html.

[84] European Committee for Electrotechnical Standardization. (2010-09-01). *CENELEC – EN 50159 Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems.* [Online]. Available: https://standards.globalspec.com/std/1285055/EN%2050159.

[85] British Standards Institution. (2020-02-25). *BSI – BS EN 50126-1 – TC. Tracked Changes (Redline) – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Part 1: Generic RAMS Process.* [Online]. Available: https://standards.globalspec.com/std/14321159/bs-en-50126-1-tc.

[86] British Standards Institution. (2020-02-25). *BSI – BS EN 50126-2 – TC. Tracked Changes (Redline) – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Part 2: Systems Approach to Safety.* [Online]. Available: https://standards.globalspec.com/std/14326588/bs-en-50126-2-tc.

[87] International Electrotechnical Commission. (2011-08-25). *IEC 61513:2011. Nuclear power plants – Instrumentation and control important to safety – General requirements for systems.* [Online]. Available:

https://webstore.iec.ch/publication/5532.

[88] International Electrotechnical Commission. (2019-09-25). *IEEE/IEC 62582-6-2019. Nuclear power plants. Instrumentation and control important to safety. Electrical equipment condition monitoring methods – Part 6: Insulation resistance.* [Online]. Available: https://standards.ieee.org/standard/62582-6-2019.html.

[89] International Electrotechnical Commission. (2006-05-09). *IEC 60880:2006. Nuclear power plants. Instrumentation and control systems important to safety. Software aspects for computer-based systems performing category A functions.* [Online]. Available: https://webstore.iec.ch/publication/3795.

[90] International Electrotechnical Commission. (2010-04-30). *IEC 61508-4:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations.* [Online]. Available: https://webstore.iec.ch/publication/5518.

[91] International Electrotechnical Commission. (2019-11-13). *IEC 62645:2019. Nuclear power plants. Instrumentation, control and electrical power systems. Cybersecurity requirements.* [Online]. Available: https://webstore.iec.ch/publication/32904.

[92] Raggad, *Information Security Management: Concepts and Practice*, London, United Kingdom: CRC Press, 2010.

[93] G. Gluschke, *Cyber security policies and critical infrastructure protection*. Potsdam, Germany: Institute for Security and Safety (ISS) Press, 2018.

[94] International Organization for Standardization. (2004-11 -01). *ISO/IEC 13335-1: 2004. Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*. [Online]. Available: https://www.iso.org/standard/39066.html.

[95] T. Limba, T. Plėta, K. Agafonov and M. Damkus, "Cyber security management model for critical infrastructure", *Entrepreneurship and Sustainability Issues*, vol. 4, no. 4, pp. 559-573, 2017. doi: 10.9770/jesi.2017.4.4(12).

[96] Верховна Рада України. (2016-03-15). *Указ Президента України; Стратегія від 15.03.2016 № 96/2016. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України".* [Електронний ресурс]. Доступно: https://zakon5.rada.gov.ua/laws/show/96/2016.

[97] International Electrotechnical Commission. (2009-07-30). *IEC TS 62443-1-1:2009 Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*. [Online]. Available: https://webstore.iec.ch/publication/7029.

[98] L. Maglaras, K. Kim, H. Janicke, M. Ferrag, S. Rallis, P. Fragkou, A. Maglaras and T. Cruz, "Cyber security of critical infrastructures", *ICT Express*, vol. 4, no. 1, pp. 42-45, 2018. doi: 10.1016/j.icte.2018.02.001.

[99] International Organization for Standardization. (2014-01-01). *ISO/IEC 15408-1:2009. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.* [Online]. Available: https://www.iso.org/standard/50341.html.

[100] International Organization for Standardization. (2011-05-01). *ISO/IEC 15408-2:2008. Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 2: Security functional components.* [Online]. Available: https://www.iso.org/standard/46414.html.

[101] International Organization for Standardization. (2011-05-01). *ISO/IEC 15408-3:2008. Information technology. Security techniques. Evaluation criteria for IT security. Part 3: Security assurance components.* [Online]. Available: https://www.iso.org/standard/46413.html.

[102] International Organization for Standardization. (2018-02-01). *ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary*. [Online]. Available: https://www.iso.org/standard/73906.html.

[103] International Organization for Standardization. (2013-10-01). *ISO/IEC 27001:2013. Information technology. Security techniques. Information security*

management systems. Requirements. [Online]. Available: https://www.iso.org/standard/54534.html.

[104] International Organization for Standardization. (2015-12-01). *ISO/IEC 27013:2015. Information technology. Security techniques. Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*. [Online]. Available: https://www.iso.org/standard/64138.html.

[105] International Electrotechnical Commission. (2010-11-10). *IEC 62443-2-1:2010. Industrial communication networks. Network and system security. Part 2-1: Establishing an industrial automation and control system security program*. [Online]. Available: https://webstore.iec.ch/publication/7030.

[106] International Electrotechnical Commission. (2009-07-30). *IEC/TR 62443-3-1:2009 Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems*. [Online]. Available: https://webstore.iec.ch/publication/7031.

[107] International Electrotechnical Commission. (2013-08-07). *IEC 62443-3-3:2013. Industrial communication networks. Network and system security. Part 3-3: System security requirements and security levels.* [Online]. Available: https://webstore.iec.ch/publication/7033.

[108] Держстандарт України. (1996-01-01). *ДСТУ 2861-94. Надійність техніки. Аналіз надійності. Основні положення.* [Електронний ресурс]. Доступно: https://dnaop.com/html/43858/doc-ДСТУ_2861-94.

[109] В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко та С. В. Толюпа, *Інформаційна та кібербезпека: соціотехнічний аспект: підручник*, Київ, Україна: ДУТ, 2015.

[110] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby and K. Stoddart, “A review of cyber security risk assessment methods for SCADA systems”, *Computers & Security*, vol. 56, pp. 1-27, 2016. doi: 10.1016/j.cose.2015.09.009.

[111] N. Teodoro, L. Goncalves and C. Serrao, “NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive

Requirements", *2015 IEEE Trustcom/BigDataSE/ISPA*, 2015. doi: 10.1109/Trustcom.2015.402.

[112] R. Yeun, P. Bates and P. Murray, "Aviation safety management systems", *World Review of Intermodal Transportation Research*, vol. 5, no. 2, p. 168, 2014. doi: 10.1504/WRITR.2014.067234.

[113] J. Caldwell, M. Mallis, J. Caldwell, M. Paul, J. Miller and D. Neri, "Fatigue Countermeasures in Aviation", *Aviation, Space, and Environmental Medicine*, vol. 80, no. 1, pp. 29-59, 2009. doi: 10.3357/ASEM.2435.2009.

[114] International Civil Aviation Organization. (2019-11-07). *Annex 19. Convention on International Civil Aviation. Safety Management*. [Online]. Available: https://caainternational.com/wp-content/uploads/2018/05/AN19_2ed-publication.pdf.

[115] G. Kozachenko, O. Lyashenko and V. Bezbozhnyy, "Enterprise economic security management conception", *TEKA Kom. Mot. i Energ. Roln. – OL PAN*, no.10A, pp. 263-270, 2010.

[116] О. Г. Череп та О. В. Степаненко, "Концепція управління економічною безпекою машинобудівних підприємств", *Сталий розвиток економіки*, № 4, с. 110-114, 2013.

[117] В. Ф. Шаньгин, *Информационная безопасность компьютерных систем и сетей : учеб. пособие*, Москва, РФ: ИД «ФОРУМ», 2017.

[118] EU initiatives on Cloud Computing. [Online]. Available: https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2018/RDF/Workshop%20Presentations/Session3/ITU%20Workshop%20Algiers%202018%20-%20Cloud%20Computing-final-INES.pdf. Accessed on 15-10-2020.

[119] Київська Міська Рада. IV сесія XXIV скликання. (2003-07-10). *Рішення від 10 липня 2003 року N 616/776. Про затвердження Концепції безпеки міста Києва*. [Електронний ресурс]. Доступно: http://kmr.ligazakon.ua/SITE2/l_docki2.nsf/alldocWWW/7837ECB4633AE190C22573C000526ACF.

[120] Верховна Рада України. (2007-10-17). *Розпорядження Кабінету Міністрів України; Концепція від 17.10.2007 № 880-р. Про схвалення Концепції національної екологічної політики України на період до 2020 року.* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/880-2007-р.

[121] Концепція, *Енциклопедія Сучасної України*. [Електронний ресурс] Доступно: http://esu.com.ua/search_articles.php?id=3256. Дата звернення: 15-10-2020.

[122] О. І. Судакова, Т. П. Медведовская, Є. В. Гарбуз та О. В. Лутченко, “Управління безпекою взаємодії підприємства з контрагентами, діючими в загальному життєвому просторі”, *Глобальні та національні проблеми економіки*, № 19, с. 256-261, 2017.

[123] В. Б. Дудикевич, Г. В. Микитин та А. І. Ребець, “До проблеми управління комплексною системою безпеки кіберфізичних систем”, *Вісник Національного університету "Львівська політехніка". Інформаційні системи та мережі*. № 901, с. 10-21, 2018.

[124] В. Б. Дудикевич, Г. В. Микитин та Т. Б. Крет, “Концепція та базовий підхід до побудови системи захисту інформації в багаторівневій інтелектуальній системі керування”, *Системи обробки інформації*, Вип. 8, с. 105-110, 2016.

[125] В. Б. Дудикевич, В. М. Максимович та Г. В. Микитин, “Парадигма та концепція побудови багаторівневої комплексної системи безпеки кіберфізичних систем”, *Вісник Національного університету "Львівська політехніка". Автоматика, вимірювання та керування*, № 821, с. 3-7, 2015.

[126] Е. В. Брежнев и В. С. Харченко, “Методология обеспечения безопасности критических инфраструктур в условиях неопределенности: концепция и принципы”, *Радіоелектронні і комп’ютерні системи*, №1, с. 25-32, 2015.

[127] Є. В. Брежнєв, Г. В. Фесенко та В. С. Харченко, “Методологічні засади оцінювання та забезпечення безпеки критичних інформаційних

інфраструктур", *Радіоелектронні і комп'ютерні системи*, № 4, с. 78-85, 2018.

[128] V. Dudykevych, G. Mykytyn, T. Kret and A. Rebets, "Security of Cyber-Physical Systems from Concept to Complex Information Security System", *Advances in cyber-physical systems*, vol. 1, Num. 2, pp. 67-75, 2016.

[129] J. von Neumann, "Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components", *Automata Studies*, C. E. Shannon and J. McCarthy, eds., Princeton Univ. Press, 1956, pp. 43-98.

[130] А. А. Гордеев и В. С. Харченко, "Элементы методологии профилеориентированного оценивания качества программного обеспечения информационных систем", *Проблеми інформатизації та упр.: зб. наук. пр.*, № 3, вип. 47, с. 24-30, 2014.

[131] А. А. Гордеев, "Модель качества отдельного требования программного обеспечения", *Радіоелектронні і комп'ютерні системи*, № 2, с. 48-58, 2020. doi: 10.32620/reks.2020.2.04.

[132] І. М. Сіроклин, В. П. Мороз, В. М. Петухов та А. О. Каргін, "Концепція побудови комплексної системи визначення технічного стану рухомого складу: напольні пристрої", *Залізничний транспорт України*, № 2, с. 13-21, 2018.

[133] International Organization for Standardization. (2011-03-01). *ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*. [Online]. Available: https://www.iso.org/standard/44374.html

[134] В. В. Скляр, "Элементы методологии анализа функциональной безопасности информационно-управляющих систем", *Радіоелектронні і комп'ютерні системи*, № 6, с. 75-79, 2009.

[135] Національне космічне агентство України. (2012-10-16). *Настанова СОУ-Н ДКА 0061:2012. Галузева система управління якістю. Процеси життєвого циклу програмного забезпечення програмно-технічних комплексів критичного призначення.* [Електронний ресурс]. Доступно: http://scasu.com/literature/SOU-N%200061_small.pdf.

[136] Національне космічне агентство України. (2009-08-12). *Настанова СОУ-Н НКАУ 0058:2009. Галузева система управління якістю. Вимоги до функціональної безпеки програмного забезпечення програмно-технічних комплексів критичного призначення.* [Електронний ресурс]. Доступно: http://scasu.com/literature/nastanova058.pdf.

[137] Національне космічне агентство України. (2010-02-08). *Настанова СОУ-Н НКАУ 0060:2010. Галузева система управління якістю. Гарантоздатність програмно-технічних комплексів критичного призначення.* [Електронний ресурс]. Доступно: http://www.scasu.com/literature/nastanova060.pdf.

[138] Аналіз функціональної безпеки програмного забезпечення програмно-технічних комплексів критичного застосування (Атомна енергетика, космос, залізничний та автомобільний транспорт, медичне обладнання) [Електронний ресурс]. Доступно: http://scasu.com/literature/metod_func_bezop.pdf. Дата звернення 2020-10-15.

[139] Государственный Комитет СССР по стандартам. (1987-01-07). *ГОСТ 26843-86. Реакторы ядерные энергетические. Общие требования к системе управления и защиты.* [Електронний ресурс]. Доступно: http://vsegost.com/Catalog/12/12184.shtml.

[140] Е. С. Бахмач, А. А. Сиора, В. В. Скляр, В. И. Токарев и В. С. Харченко, “Обеспечение и оценка безопасности информационных и управляющих систем АЭС на базе ПЛИС”, *Радіоелектронні і комп'ютерні системи*, № 7, с. 75-82, 2007.

[141] International Electrotechnical Commission. (2010-04-30). *IEC 61508-6:2010. Functional safety of electrical/electronic/programmable electronic safety related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3.* [Online]. Available: https://webstore.iec.ch/publication/5520.

[142] International Electrotechnical Commission. (2010-04-30). *IEC 61508-7:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures.* [Online]. Available:

https://webstore.iec.ch/publication/5521.

[143] E. Babeshko, V. Kharchenko, O. Odarushchenko and V. Sklyar, “Toward automated FMEDA for complex electronic products”, In *2015 Int. Conf. on Information and Digital Technologies,* Zilina, 2015, pp. 22-27, doi: 10.1109/DT.2015.7222945.

[144] Babeshko, V. Kharchenko and A. Siora, “Reliability assessment of FPGA-based NPP I&C: experience, methods and tools”, *Радіоелектронні і комп’ютерні системи*, № 5, с. 113-119, 2016.

[145] О. А. Ильяшенко, В. С. Харченко и Я. А. Чуйков, “Оценка безопасности систем на FPGA с использованием XMECA для V-модели жизненного цикла”, *Радіоелектронні і комп’ютерні системи*, № 6, с. 141-147, 2016.

[146] Y. Bulba, Y. Ponochovny, V. Sklyar and A. Ivasiuk, “Classification and Research of the Reactor Protection Instrumentation and Control System Functional Safety Markov Models in a Normal Operation Mode”, In *Proceedings of the 12th Int. Conf. on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer,* Kyiv, Ukraine, June 21-24, 2016, pp. 308-321.

[147] National Institute of Standards and Technology. (2013-05-24). *NIST SP 500-291, Cloud Computing Standards Roadmap*. [Online]. Available: https://www.nist.gov/publications/nist-sp-500-291-nist-cloud-computing-standards-roadmap.

[148] National Institute of Standards and Technology. (2011-11-01). *NIST Special Publication 800-145. The NIST Definition of Cloud Computing*. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-145/final.

[149] National Institute of Standards and Technology. (2011-12-01). *NIST Special Publication 800-144. Guidelines on Security and Privacy in Public Cloud Computing.* [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-144/final.

[150] International Organization for Standardization. (2014-10-15). *ISO/IEC*

17788:2014 Information technology – Cloud computing – Overview and vocabulary. [Online]. Available: https://www.iso.org/standard/60544.html.

[151] Cloud Computing Services. Google Cloud. [Online]. Available: https://cloud.google.com. Accessed on 15-10-2020.

[152] Choosing an App Engine environment. [Online]. Available: https://cloud.google.com/appengine/docs/the-appengine-environments. Accessed on 15-10-2020.

[153] App Engine Service Level Agreement (SLA). [Online]. Available: https://cloud.google.com/appengine/sla. Accessed on 15-10-2020.

[154] Cloud Computing Services. Microsoft Azure. [Online]. Available: https://azure.microsoft.com/en-us. Accessed on 15-10-2020.

[155] L. Qaisi and I. Aljarah, "A twitter sentiment analysis for cloud providers: A case study of Azure vs. AWS", *2016 7th International Conference on Computer Science and Information Technology (CSIT)*, 2016. doi: 10.1109/CSIT.2016.7549473.

[156] С. І. Шматков, Н. Г. Кучук, Ж. О. Коломієць, "Аналіз інформаційних технологій у системах мобільного навчання", *Системи управління, навігації та зв'язку*, Вип. 4, с. 143-149, 2017.

[157] Amazon Web Services (AWS) – Cloud Computing Services. [Online]. Available: https://aws.amazon.com. Accessed on 15-10-2020.

[158] Amazon turns surprise Q3 profit as AWS cloud growth soars. [Online]. Available: http://www.computerweekly.com/news/4500256048/Amazon-turns-surprise-Q3-profit-as-AWS-cloud-growth-soars. Accessed on 15-10-2020.

[159] T. Lorido-Botran, J. Miguel-Alonso and J. Lozano, "A Review of Auto-scaling Techniques for Elastic Applications in Cloud Environments", *Journal of Grid Computing*, vol. 12, no. 4, pp. 559-592, 2014. doi: 10.1007/s10723-014-9314-7.

[160] Gorelik, *Cloud computing models*. Cambridge, United Kingdom: Massachusetts Institute of Technology, 2013.

[161] B. S. Brad and M. Murar, "Smart Buildings Using IoT Technologies",

Construction of Unique Buildings and Structures, № 5 (20), pp. 15-27, 2014.

[162] M. R. Alam, M. B. I. Reaz and M. A. M. Ali, "A Review of Smart Homes – Past, Present and Future," in *IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews)*, vol. 42, no. 6, pp. 1190-1203, Nov. 2012, doi: 10.1109/TSMCC.2012.2189204.

[163] S. Budijono, J. Andrianto and M. Axis Novradin Noor, "Design and implementation of modular home security system with short messaging system", *EPJ Web of Conferences*, vol. 68, iss. 25, 2014. doi: 10.1051/epjconf/20146800025.

[164] International Organization for Standardization. (2010-11-01). *ISO 16484-1:2010. Building automation and control systems (BACS) – Part 1: Project specification and implementation.* [Online]. Available: https://www.iso.org/standard/37300.html.

[165] International Organization for Standardization. (2014-10-10). *ISO/IEC 17789:2014 Information technology – Cloud computing – Reference architecture.* [Online]. Available: https://www.iso.org/standard/60545.html.

[166] International Telecommunication Union. (2014-08-13). *Recommendation ITU-T Y.3500. Information technology – Cloud computing – Overview and vocabulary.* [Online]. Available: https://www.itu.int/rec/T-REC-Y.3500-201408-I.

[167] International Telecommunication Union. (2013-05-22). *Recommendation ITU-T Y.3501. Cloud computing framework and high-level requirements.* [Online]. Available: https://www.itu.int/rec/T-REC-Y.3501/en.

[168] International Telecommunication Union. (2014-08-13). *Recommendation ITU-T Y.3502. Information technology – Cloud computing – Reference architecture.* [Online]. Available: https://www.itu.int/rec/T-REC-Y.3502-201408-I/en.

[169] Cloud Accountability Project (CSA). (2016-03-31). *D15.2 Report on A4Cloud contribution to standards.* [Online]. Available: http://www.cloudaccountability.eu/sites/default/files/D15.2%20Report%20on%20A4Cloud%20contribution%20to%20standards%20%28final%29.pdf.

[170] International Organization for Standardization. (2008-08-15). *ISO/IEC 18045:2008. Information technology – Security techniques – Methodology for IT security evaluation.* [Online]. Available: https://www.iso.org/standard/46412.html.

[171] В. В. Скляр, “Методология и информационные технологии обеспечения функциональной безопасности информационно-управляющих систем”, дис. доктора наук, національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, 2012.

[172] International Electrotechnical Commission. (2006-05-10). *IEC 61165:2006 Application of Markov techniques.* [Online]. Available: https://webstore.iec.ch/publication/4721.

[173] О. В. Іванченко, “Оцінювання рівня безпеки системи SCADA критичної інфраструктури з урахуванням доступності кібернетичних та хмарних активів”, *Системи та технології*, № 2, с. 5-32, 2019. doi: 10.32836/2521-6643-2019-2-58-1.

[174] В. С. Харченко, О. Н. Одарущенко и Е. Б. Одарущенко, “Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем информационно-управляющих комплексов”, *Радіоелектронні і комп’ютерні системи*, № 5, с. 62-70, 2006.

[175] V. Kharchenko, V. Butenko, O. Odarushchenko and V. Sklyar, “Multifragmentation Markov Modeling of a Reactor Trip System”, *Journal of Nuclear Engineering and Radiation Science*, vol. 1, no. 3, 2015. doi: 10.1115/1.4029342.

[176] А. А. Руденко, О. Н. Одарущенко и В. С. Харченко, “Модели оценки надежности программных средств с учетом недетерминированного числа вторичных дефектов”, *Радіоелектронні і комп’ютерні системи*, № 6, с. 197-203, 2010.

[177] V. Kharchenko, V. Butenko, O. Odarushchenko and E. Odarushchenko, “Markov's Modeling of NPP I&C Reliability and Safety: Optimization of Tool-and-Technique Selection”, In *2016 Second International Symposium on Stochastic*

Models in Reliability Engineering, Life Science and Operations Management (SMRLO), Beer-Sheva, 2016, pp. 328-336, doi: 10.1109/SMRLO.2016.61.

[178] R. Sargent, "Verification and validation of simulation models", *Journal of Simulation*, vol. 7, no. 1, pp. 12-24, 2013. doi: 10.1057/jos.2012.20.

[179] В. С. Харченко, "Парадигмы и принципы гарантоспособных вычислений: состояние и перспективы развития", *Радіоелектронні і комп'ютерні системи*, № 2, с. 91-100, 2009.

[180] В. С. Харченко и В. В. Тарасенко, "Абстрактные модели и элементы синтеза многоверсионных автоматов", *Радіоелектронні і комп'ютерні системи*, № 7, с. 52-55, 2006.

[181] В. С. Харченко, "Гарантоздатність комп'ютерних систем: межа універсальності у контексті інформаційно-технічних станів", *Радіоелектронні і комп'ютерні системи*, № 8, с. 7-14, 2007.

[182] A. Gorbenko, V. Kharchenko, P. Popov and A. Romanovsky, "Dependable Composite Web Services with Components Upgraded Online", *Architecting Dependable Systems III*, pp. 92-121, 2005. doi: 10.1007/11556169_5.

[183] A. Gorbenko, V. Kharchenko and A. Romanovsky, "Using Inherent Service Redundancy and Diversity to Ensure Web Services Dependability", *Methods, Models and Tools for Fault Tolerance*, pp. 324-341, 2009. doi: 10.1007/978-3-642-00867-2_15.

[184] E. Babeshko, V. Kharchenko, K. Leontiiev, E. Ruchkov and V. Sklyar, "Reliability assessment of safety critical system considering different communication architectures", In *2018 IEEE 9th Int. Conf. on Dependable Systems, Services and Technologies (DESSERT)*, Kiev, 2018, pp. 17-20, doi: 10.1109/DESSERT.2018.8409091.

[185] O. Illiashenko, V. Kharchenko, A. Kor, A. Panarin and V. Sklyar, "Hardware diversity and modified NUREG/CR-7007 based assessment of NPP I&C safety", In *2017 9th IEEE Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Bucharest, 2017, pp. 907-911, doi: 10.1109/IDAACS.2017.8095218.

[186] V. Sklyar, V. Kharchenko, A. Siora, S. Malokhatko, V. Golovir and Y. Beliy, “Reliability and availability analysis of FPGA-based Instrumentation and Control systems”, In *2011 11th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, Polyana-Svalyava, 2011, pp. 27-33.

[187] E. Brezhnev, V. Kharchenko, V. Manulik and K. Leontiev, “Critical Energy Infrastructure Safety Assurance Strategies Considering Emergent Interaction Risk”, *Advances in Dependability Engineering of Complex Systems*, pp. 67-78, 2017. doi: 10.1007/978-3-319-59415-6_7.

[188] E. Brezhnev and V. Kharchenko, “NPP: Power Grid Mutual Safety Assessment”, *Nuclear Power Plant Instrumentation and Control Systems for Safety and Security*, pp. 397-431, 2014. doi: 10.4018/978-1-4666-5133-3.ch013.

[189] К. О. Сорока, *Основи теорії систем і системного аналізу: навч. посібник,* Харків, Україна: НАМГ, 2004.

[190] Г. Ф. Балькин, Ю. Г. Балькин и Л. А. Крапивянская, *Системный анализ в инфокоммуникациях. Просто о сложном*, Київ, Україна: Біо-Тест-Лабораторія, 2015.

[191] Г. С. Теслер та В. А. Косс, “Методика системного аналізу з позиції методології системного підходу для потреб проектування систем управління”, *Мат. машини і системи*, № 1, с. 139-150, 2008.

[192] J. Neumann and A.W. Burks, *Theory of Self-reproducing Automata*, Urbana, IL: University of Illinois, 1966.

[193] J. Henke, “Dependable software for undependable hardware”, In *7th IEEE International Symposium on Industrial Embedded Systems (SIES'12)*, Karlsruhe, 2012, p. 1, doi: 10.1109/SIES.2012.6356614.

[194] A. Gorbenko, V. Kharchenko and A. Romanovsky, “On composing Dependable Web Services using undependable web components”, *International Journal of Simulation and Process Modelling*, vol. 3, no. 12, p. 45, 2007. doi: 10.1504/IJSPM.2007.014714.

[195] Y. Brezhniev, “Multilevel Fuzzy Logic-Based Approach for Critical Energy Infrastructure’s Cyber Resilience Assessment”, In *2019 10th Int. Conf. on Dependable Systems, Services and Technologies (DESSERT)*, Leeds, United Kingdom, 2019, pp. 213-217, doi: 10.1109/DESSERT.2019.8770034.

[196] J. Laprie, “Resilience for the Scalability of Dependability”, *Fourth IEEE International Symposium on Network Computing and Applications*, Cambridge, MA, 2005, pp. 5-6, doi: 10.1109/NCA.2005.44.

[197] N. Guelfi, “A formal framework for dependability and resilience from a software engineering perspective”, *Open Computer Science*, vol. 1, no. 3, 2011, pp. 294-328. doi: 10.2478/s13537-011-0025-x.

[198] K. Trivedi, D. Kim and R. Ghosh, “Resilience in computer systems and networks”, *Proceedings of the 2009 International Conference on Computer-Aided Design – ICCAD '09*, 2009. doi: 10.1145/1687399.1687415.

[199] V. Kharchenko, V. Sklyar and O. Odaruschenko, “Dependable Computing Systems in Support of Transformation of the Force Information Infrastructure”, *Information & Security: An International Journal*, vol. 22, pp. 75-91, 2007. doi: 10.11610/isij.2208.

[200] C. Gacek and R. de Lemos, “Architectural description of dependable software systems”, *Structure for Dependability: Computer-Based Systems from an Interdisciplinary Perspective*, pp. 127-142, 2006. doi: 10.1007/1-84628-111-3_7.

[201] S. Borkar, “Designing Reliable Systems from Unreliable Components: The Challenges of Transistor Variability and Degradation”, *IEEE Micro*, vol. 25, no. 6, pp. 10-16, 2005. doi: 10.1109/MM.2005.110.

[202] Vaglini, *Security and Dependability*, [Online]. Available: https://elearn.ing.unipi.it/pluginfile.php/7808/mod_resource/content/1/Lezione%2010%20-%20System%20Dependability.pdf. Accessed on 15-10-2020.

[203] J. Henkel, L. Hedrich, A. Herkersdorf, R. Kapitza, D. Lohmann, P. Marwedel, M. Platzner, W. Rosenstiel, U. Schlichtmann, O. Spinczyk, M. Tahoori, L. Bauer, J. Teich, N. Wehn, H. Wunderlich, J. Becker, O. Bringmann, U. Brinkschulte, S. Chakraborty, M. Engel, R. Ernst and H. Härtig, “Design and

architectures for dependable embedded systems", *Proceedings of the VII IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis – CODES+ISSS '11*, 2011. doi: 10.1145/2039370.2039384.

[204] M. Rebaudengo, M. S. Reorda, M. Violante and M. Torchiano, "A source-to-source compiler for generating dependable software", *Proceedings First IEEE International Workshop on Source Code Analysis and Manipulation*, Florence, Italy, 2001, pp. 33-42, doi: 10.1109/SCAM.2001.972664.

[205] О. В. Булыгина, А. А. Емельянов, Н. З. Емельянова и А. А. Кукушкин, *Системный анализ в управлении: учеб. пособие*, Москва, РФ: ФОРУМ, 2017. doi: 10.12737/textbook_5923d5ac7ec116.40684446.

[206] Т. О. Прокопенко, *Теорія систем і системний аналіз: навч. посіб*., Черкаси, Україна: ЧДТУ, 2019.

[207] В. С. Харченко и И. В. Лысенко, *Теория систем и системный анализ: Конспект лекций*, Харьков: НАУ «ХАИ», 2003.

[208] Build deployment rings for Windows 10 updates. [Online]. Available: https://docs.microsoft.com/en-us/windows/deployment/update/waas-deployment-rings-windows-10-updates. Accessed on 15-10-2020.

[209] Windows 10 IoT Enterprise. [Online]. Available: https://www.quarta-embedded.ru/we/10. Accessed on 15-10-2020.

[210] В. В. Скляр, В. С. Харченко и А. С. Панарин, "Тестирование программируемых логических контроллеров на базе ПЛИС с использованием среды функционального программирования" *Системи обробки інформації*, № 1(117), с. 44-55, 2014.

[211] G. Loukas, Diane Gan and Tuan Vuong, "A taxonomy of cyber attack and defence mechanisms for emergency management networks", in *2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, San Diego, CA, 2013, pp. 534-539, doi: 10.1109/PerComW.2013.6529554.doi: 10.1007/978-3-642-13568-2_11.

[212] R. Ross, M. McEvilley and J. Carrier Oren, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of

Trustworthy Secure Systems", *NIST Special Publication 800-160*, 2016. doi: 10.6028/NIST.SP.800-160.

[213] C. Ten, C. Liu and M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees", *2007 IEEE Power Engineering Society General Meeting*, Tampa, FL, 2007, pp. 1-8, doi: 10.1109/PES.2007.385876.

[214] А. С. Гейда и И. В. Лысенко, "Задачи исследования операционных свойств совершенствуемых систем и процессов их функционирования: Концептуальные аспекты", *Прикладная информатика*, № 5 (71), с. 93-106, 2017.

[215] P. Subbiah and B. Ramamurthy, "The study of fault tolerant system design using complete evolution hardware", in *2005 IEEE International Conference on Granular Computing*, Beijing, 2005, pp. 642-645 Vol. 2, doi: 10.1109/GRC.2005.1547370.

[216] L. Kumar and A. Sureka, "Aging Related Bug Prediction using Extreme Learning Machines", in *2017 14th IEEE India Council International Conference (INDICON)*, Roorkee, 2017, pp. 1-6, doi: 10.1109/INDICON.2017.8487925.

[217] D. Menasché, K. Trivedi and E. Altman, "Rejuvenation and the Age of Information", in *2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Berlin, Germany, 2019, pp. 225-231, doi: 10.1109/ISSREW.2019.00076.

[218] J. Bai, X. Chang, F. Machida, K. S. Trivedi and Z. Han, "Analyzing Software Rejuvenation Techniques in a Virtualized System: Service Provider and User Views", in *IEEE Access*, vol. 8, pp. 6448-6459, 2020, doi: 10.1109/ACCESS.2019.2963397.

[219] M. Grottke, A. P. Nikora and K. S. Trivedi, "An empirical investigation of fault types in space mission system software", in *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, Chicago, IL, 2010, pp. 447-456, doi: 10.1109/DSN.2010.5544284.

[220] A. Verma, A. Ghartaan and T. Gayen, "Review of Software Fault-

Tolerance Methods for Reliability Enhancement of Real-Time Software Systems", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 6, no. 3, p. 1031, 2016.

[221] D. F. McAllister and M. A. Vouk, "Fault-tolerant software reliability engineering", In *Handbook of software reliability engineering*, Michael R. Lyu, Ed., New York, USA: McGraw-Hill, 1986, pp. 567–614.

[222] В. С. Харченко, *Теоретические основы дефектоустойчивых цифровых систем с версионной избыточностью*, Харків, Україна, 1996.

[223] B. Randell, "Occurrence Nets Then and Now: The Path to Structured Occurrence Nets", *Applications and Theory of Petri Nets*, pp. 1-16, 2011. doi: 10.1007/978-3-642-21834-7_1.

[224] Al-Sudani Mustafa Qahtan Abdulmunem and V. S. Kharchenko, "Availability and Security Assessment of Smart Building Automation Systems: Combining of Attack Tree Analysis and Markov Models", In *3th IEEE Int. Conf.on Mathematics and Computers in Sciences and in Industry (MCSI)*, Chania, Greece, pp. 302-307, 2016, doi: 10.1109/MCSI.2016.062.

[225] С. І. Доценко, "Принцип цілісної організації інтелектуальних систем", *Радіоелектронні і комп'ютерні системи*, № 1, с. 4-16, 2019. doi:10.32620/reks.2019.1.01.

[226] K. Trivedi and D. Selvamuthu, "Markov Modeling in Reliability", *Encyclopedia of Quantitative Risk Analysis and Assessment*, 2008. doi: 10.1002/9780470061596.risk0492.

[227] K. Trivedi, G. Ciardo, M. Malhotra and S. Garg, "Dependability and performability analysis using stochastic Petri nets', in *11th International Conference on Analysis and Optimization of Systems Discrete Event Systems*, pp. 144-157, 1994. doi: 10.1007/BFb0033543.

[228] О. М. Василевський та О. Г. Ігнатенко, *Нормування показників надійності технічних засобів: навчальний посібник*, Вінниця: ВНТУ, 2013.

[229] В. С. Харченко, "Гарантоспособность и гарантоспособные системы: элементы методологии", *Радіоелектронні і комп'ютерні системи*,

№ 5(17), с. 7-19, 2006.

[230] Держстандарт України. (2003-01-07). *ДСТУ 4178-2003. Комплекси технічних засобів систем керування та регулювання руху поїздів. Функційна безпечність і надійність. Вимоги та методи випробовування*. [Електронний ресурс]. Доступно: https://www.uz.gov.ua/files/file/documents/ДСТУ 4178-2003.pdf.

[231] Держстандарт України. (2019-09-01). *ДСТУ EN 61508-5:2019 Функційна безпечність електричних, електронних, програмованих електронних систем, пов'язаних із безпекою. Частина 5. Приклади методів для визначення рівнів повноти безпеки.* [Електронний ресурс]. Доступно: http://online.budstandart.com/ru/catalog/doc-page.html?id_doc=84388.

[232] С. А. Засуха, "Исследование влияния временных параметров обновления программных средств на готовность двухканальной информационно-управляющей системы космического аппарата", *Збірник наукових праць Харківського університету Повітряних сил*, вип. 3, с. 131-135, 2011.

[233] Common Vulnerabilities and Exposures. [Online]. Available: http://cve.mitre.org. Accessed on 15-10-2020.

[234] SecurityFocus database of computer security. [Online]. Available: http://www.securityfocus.com. Accessed on 15-10-2020.

[235] Microsoft Security Bulletins. [Online]. Available: https://docs.microsoft.com/en-us/security-updates/securitybulletins/security-bulletins. Accessed on 15-10-2020.

[236] CERT Vulnerability Notes Database [Online]. Available: https://www.kb.cert.org/vuls. Accessed on 15-10-2020.

[237] National vulnerability database [Online]. Available: https://nvd.nist.gov. Accessed on 15-10-2020.

[238] А. В. Горбенко, "Модели законов распределения времени обслуживания резервированных сервис-ориентированных систем", *Системи управління, навігації та зв'язку*, № 4(20), с. 221-225, 2011.

[239] One-sample Kolmogorov-Smirnov test – MATLAB kstest. [Online]. Available: https://www.mathworks.com/help/stats/kstest.html. Accessed on 15-10-2020.

[240] R. Lopes, "Kolmogorov-Smirnov Test", *International Encyclopedia of Statistical Science*, pp. 718-720, 2011. doi: 10.1007/978-3-642-04898-2_326.

[241] А. И. Кобзарь, *Прикладная математическая статистика. Справочник для инженеров и научных работников*, Москва, РФ: Физматлит, 2006.

[242] Hassani and E. Silva, "A Kolmogorov-Smirnov Based Test for Comparing the Predictive Accuracy of Two Sets of Forecasts", *Econometrics*, vol. 3, no. 3, pp. 590-609, 2015. doi: 10.3390/econometrics3030590.

[243] Francisco de Castro. Fitmethis finds best-fitting distribution. [Online]. Available: https://www.mathworks.com/matlabcentral/fileexchange/40167-fitmethis. Accessed on 15-10-2020.

[244] Apache HTTP Server. [Online]. Available: http://www.apache.org/foundation. Accessed on 15-10-2020.

[245] В. В. Кульба, Е. А. Микрин, Б. В. Павлов и В. Н. Платонов, *Теоретические основы проектирования информационно-управляющих систем космических аппаратов*, Москва, РФ: Наука, 2006.

[246] J. Xiang, C. Weng, D. Zhao, A. Andrzejak, S. Xiong, L. Li and J. Tian, "Software aging and rejuvenation in android: new models and metrics", *Software Quality Journal*, vol. 28, no. 1, pp. 85-106, 2019. doi: 10.1007/s11219-019-09475-0.

[247] D. Cotroneo, R. Natella, R. Pietrantuono and S. Russo, "Software Aging and Rejuvenation: Where We Are and Where We Are Going", in *2011 IEEE Third International Workshop on Software Aging and Rejuvenation*, Hiroshima, 2011, pp. 1-6, doi: 10.1109/WoSAR.2011.15.

[248] K. Trivedi and K. Vaidyanathan, "Software Rejuvenation – Modeling and Analysis", *Information Technology*, vol. 157, pp. 151-182. doi: 10.1007/1-4020-8159-6_6.

[249] F. Tartanoglu, V. Issarny, A. Romanovsky and N. Levy, “Dependability in the Web Services Architecture”, *Lecture Notes in Computer Science*, vol. 2677, pp. 90-109, 2003. doi: 10.1007/3-540-45177-3_4.

[250] А. Ю. Белобородов и А. В. Горбенко, “Применение баз данных уязвимостей в задачах исследования безопасности программных средств”, *Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка*, № 165, с. 83-85, 2015.

[251] N. Looker, M. Munro and Jie Xu, “WS-FIT: a tool for dependability analysis of Web services”, in *Proceedings of the 28th Annual International Computer Software and Applications Conference, COMPSAC 2004*, Hong Kong, 2004, pp. 120-123, doi: 10.1109/CMPSAC.2004.1342690.

[252] Е. С. Вентцель и Л. А. Овчаров, *Теория случайных процессов и ее инженерные приложения*, Москва, РФ: Высш. школа, 2000.

[253] С. П. Іглін, *grPlot − функція для малювання графів та орграфів засобами MATLAB* [Електронний ресурс]. Доступно: http://www.iglin.epizy.com/All/GrMatlab/grPlot.html. Дата звернення: 15-10-2020.

[254] Y. Langeron, A. Barros, A. Grall and C. Bérenguer, “Combination of safety integrity levels (SILs): A study of IEC61508 merging rules”, *Journal of Loss Prevention in the Process Industries*, vol. 21, no. 4, pp. 437-449, 2008. doi: 10.1016/j.jlp.2008.02.003.

[255] Держспоживстандарт України. (2010-01-01). *ДСТУ IEC 62138: 2008. Атомні електростанції. Інформаційні та керуючі системи, важливі для безпеки. Програмні аспекти систем, які виконують функції категорії B або C*. [Електронний ресурс]. Доступно: http://online.budstandart.com/ru/catalog/doc-page.html?id_doc=62358.

[256] А. О. Андрашов, “Моделі та методи інформаційної технології оцінювання виконання вимог до функціональної безпеки інформаційно-керуючих систем АЕС”, дис. канд. наук, національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків,

2019.

[257] G. Jung, K. R. Joshi, M. A. Hiltunen, R. D. Schlichting and C. Pu, “Performance and availability aware regeneration for cloud based multitier applications”, In *2010 IEEE/IFIP Int. Conf. on Dependable Systems & Networks (DSN)*, Chicago, IL, 2010, pp. 497-506, doi: 10.1109/DSN.2010.5544273.

[258] J. Boulanger, *Safety of computer architectures,* London, United Kingdom: ISTE, 2013.

[259] W. Mechri, C. Simon, F. Bicking and K. Ben Othman, “Fuzzy multiphase Markov chains to handle uncertainties in safety systems performance assessment”, *Journal of Loss Prevention in the Process Industries*, vol. 26, no. 4, pp. 594-604, 2013. doi: 10.1016/j.jlp.2012.12.002.

[260] F. Felgner and G. Frey, “Multi-Phase Markov models for functional safety prediction: Efficient simulation of Markov models used for safety engineering and the online integration of individual systems' diagnostic and maintenance history”, in *2011 3rd International Workshop on Dependable Control of Discrete Systems*, 2011. doi: 10.1109/dcds.2011.5970331.

[261] G. Strand and M. Lundteigen, “Risk control in the well drilling phase: BOP system reliability assessment”, *Safety and Reliability of Complex Engineered Systems*, pp. 753-760, 2015. doi: 10.1201/b19094-101.

[262] И. А. Коняхин, *Методы и средства статистического моделирования ОЭС (анализ надежности): учебное пособие,* Санкт-Петербург, РФ: ИТМО, 2005.

[263] В. Н. Задорожный, *Имитационное и статистическое моделирование: учеб. пособие,* Омск, РФ: Изд-во ОмГТУ, 2013.

[264] С. П. Іглін, *Теорія ймовірностей та математична статистика на базі MATLAB: Навч. посіб.,* Харків, Україна: НТУ "ХПІ", 2006.

[265] Statistics and Machine Learning Toolbox. [Online]. Available: https://www.mathworks.com/products/statistics.html. Accessed on: 15-10-2020.

[266] Student's inverse cumulative distribution function. [Online]. Available: https://www.mathworks.com/help/stats/tinv.html. Accessed on: 15-10-2020.

[267] Random numbers – MATLAB random. [Online]. Available: https://www.mathworks.com/help/stats/prob.normaldistribution.random.html. Accessed on: 15-10-2020.

[268] Аль-Судані Мустафа Кахтан Абдулмунем, “Моделі і метод інформаційної технології забезпечення готовності та кібербезпеки інформаційно-керуючих систем розумних будинків”, дис. канд. наук, національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, 2017.

[269] Model Data Using the Distribution Fitter App. [Online]. Available: https://www.mathworks.com/help/stats/model-data-using-the-distribution-fitting-tool.html. Accessed on: 15-10-2020.

[270] С. В. Черемных, И. О. Семенов и В. С. Ручкин, *Моделирование и анализ систем. IDEF-технологии: практикум*, Москва, РФ: Финансы и статистика, 2006.

[271] В. С. Харченко, З. Г. Мухаметов и В. И. Токарев, “Метод оценки и выбора живучих структур многоярусных резервированных систем обработки информации АСУ”, *Моделювання та інформаційні технології*, № 22, с. 219-222, 2003.

[272] А. В. Боярчук, Е. В. Брежнев, А. В. Горбенко, В. Ю. Дубницкий и А. С. Епифанов, *Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения*, Харьков, Украина: Нац. аэрокосм. ун-т “ХАИ”, 2011.

[273] M. Ge, H. K. Kim and D. S. Kim, “Evaluating Security and Availability of Multiple Redundancy Designs when Applying Security Patches”, in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, Denver, CO, 2017, pp. 53-60, doi: 10.1109/DSN-W.2017.37.