ЗАТВЕРДЖУЮ:

Перший проректор Державного університету інформаційно-комунікаційних технологій

_____ Олександр КОРЧЕНКО

«_26_» ___червня___ 2024 року

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертаційної роботи Погасія Сергія Сергійовича «Моделі і методи захисту в кіберфізичних системах», поданої на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації»

Актуальність теми дослідження.

Проблема захисту кіберфізичних систем від несанкціонованого доступу набула в останнє десятиліття особливу гостроту. Це обумовлено збільшенням числа пристроїв у мережах і кількості каналів зв'язку між ними, що, своєю чергою, підвищує ризик несанкціонованого підключення до мережі та доступу до конфіденційної інформації користувачів.

Бурхливий ріст комунікаційних і обчислювальних технологій дозволяє будувати мережі розподіленої архітектури, що поєднують велику кількість сегментів, розташованих на значній дистанції один від одного.

Архітектурна парадигма, в якій широко поширена робота фізичних пристроїв (датчиків, виконавчих механізмів та мобільних пристроїв з підтримкою датчиків), які надають та отримують інформацію від системи управління, яку обробляє та аналізує певний додаток – кіберфізичні системи (CPS). Проблема захисту кіберфізичних систем від несанкціонованого доступу набула в останнє десятиліття особливу гостроту. Це обумовлено збільшенням числа пристроїв у мережах і кількості каналів зв'язку між ними,

що, своєю чергою, підвищує ризик несанкціонованого підключення до мережі та доступу до конфіденційної інформації користувачів.

Важливою складовою частиною захисту кіберфізичних систем є підсистема криптографічного захисту інформації, що реалізується відповідними протоколами та механізмами.

Оскільки масштаб і природа CPS критичних інфраструктур не дозволяють проводити експерименти, тягар розуміння критичних інфраструктур та їх взаємозв'язків, властивостей і стійкості до зловмисних дій, що виникають, лягає на зусилля по побудові моделей. Зроблено спробу сформувати концепцію побудови систем безпеки, в основі яких лежить безліч моделей, що описують різні сторони об'єктів критичної інфраструктури.

Достовірність та наукова новизна одержаних результатів.

Достовірність одержаних результатів досягнута дисертантом завдяки використанню значного масиву вітчизняної та зарубіжної наукової, нормативної та публіцистичної літератури за темою дослідження. Теоретичні та прикладні аспекти сутності побудови моделей та систем захисту кіберфізичних систем присвячено велику кількість наукових робіт Сідерс Д., Ройчоудурі Р., Генрі Дж., Бончек Т., Рексфорд Д. Питанням проблематики побудови систем безпеки кіберфізичних систем на основі використання як сучасних криптосистем, так й систем на основі постквантових алгоритмів займаються вчені: Корченко О.Г., Грищук Р.В., Хорошко В.О., Дудикевич В.Б., Савченко В.А., Альшу Х., Лаувенс К., Гарві А., Кон Е.

Попри значну кількість досліджень за наведеною тематикою, масштаб і природа кіберфізичних систем критичних інфраструктур не дозволяють проводити експерименти, тягар розуміння критичних інфраструктур та їх взаємозв’язків, властивостей і стійкості до зловмисних дій, що виникають, лягає на зусилля по побудові моделей.

Зв’язок роботи з науковими програмами, планами, темами.

Дисертаційне дослідження виконане відповідно пріоритетності розвитку інформаційних та комунікаційних технологій в Україні до 2024 р. згідно із Законом

України "Про пріоритетні напрями розвитку науки і техніки" із змінами, від 1 лютого 2022 року та від 12 січня 2023 року.

Є частиною досліджень у госпрозрахункової науково-дослідної роботи "Моделі і методи захисту інформації в кіберфізичних системах" (№ держ. реєстрації 0121U114233, ХНЕУ, м. Харків), яку виконував Харківський національний економічний університет імені Семена Кузнеця у 2020 р., частиною досліджень науково дослідницької роботи «Геоінформаційні і інтелектуальні технології підтримки прийняття рішень в задачах оцінки та прогнозування екологічної безпеки територій» (№ держ. реєстрації 0119U03671, ОДЕКУ м. Одеса), яку виконував Одеський Державний екологічний університет у 2023-2024 рр., частиною досліджень науково дослідницької роботи «Розробка симетричної криптосистеми на основі використання згорткової штучної нейронної мережі» (Державний реєстраційний номер 0123U101020, НТУ «ХПІ», м. Харків), яку виконує Національний технічний університет «Харківський політехнічний інститут» 2023-2025рр., частиною досліджень науково дослідницької роботи «Розробка моделей соціо-кіберфізичних систем, спрямованих на побудову систем безпеки та підвищення рівня її ефективності у кібер-просторі» (№ держ. реєстрації 0123U101018, НТУ «ХПІ», м. Харків), яку виконує Національний технічний університет «Харківський політехнічний інститут» 2023–2025 рр.

Мета і завдання дослідження є підвищенні ефективності захищеності інформації на основі запропонованих моделей і методів захисту в кіберфізичних системах шляхом побудови багатоконтурних систем захисту інформації з використанням постквантових алгоритмів.

Досягнення цієї мети зумовило необхідність постановки й вирішення таких основних завдань:

– проаналізувати сучасні моделі, методи забезпечення захисту кіберфізичних систем з метою визначення набору критеріїв та ідентифікуючих і оціночних компонентів, які використовуються для створення та вибору найбільш ефективного інструментарію, орієнтованого на вирішення відповідних завдань захисту інформації;

– розробити концепцію побудови багатоконтурної системи захисту кіберфізичних систем;

– розробити моделі систем захисту на основі моделі Лотки-Вольтери з урахуванням класифікатора загроз на кіберфізичні системи;

– розробити методи забезпечення конфіденційності, цілісності та автентичності інформаційних ресурсів програмно-апаратного комплексу при одночасній дії на них загроз інформаційної безпеки, кібербезпеки та безпеки інформації;

– розробити метод забезпечення закриття каналу мобільного Інтернету та каналу циркуляцію інформації у кіберфізичних системах з забезпеченням необхідного рівня захищеності, серверного програмно-апаратного комплексу;

– удосконалити класифікатор загроз безпеці інформаційних ресурсів кіберфізичних систем;

– розробити методологію побудови багатоконтурної системи безпеки інформаційних ресурсів у кіберфізичних системах, яка забезпечує контроль поточного стану об'єкту захисту та необхідний рівень захищеності в умовах появи повномасштабного квантового комп'ютера.

Об'єктом дослідження є процес забезпечення захисту інформації у кіберфізичних системах на основі багатоконтурної системи безпеки з використанням постквантових алгоритмів.

Предметом дослідження є моделі і методи захисту інформації у кіберфізичних системах.

Методи дослідження.

Теоретико-методологічним базисом дисертаційного дослідження слугували методи теорії множин формалізовано загрози безпеки інформаційних ресурсів, здійснено їх класифікацію та сформований вектор дії кожної загрози, теорії криптографії, кодування та скінченних полів Галуа використані при побудові несиметричних криптосистем на основі постквантових алгоритмів крипто-кодових конструкцій, теорії ймовірностей і математичної статистики використано для дослідження властивостей постквантових алгоритмів, методи експертного

оцінювання використані для визначення вагових коефіцієнтів загроз, оцінювання енергетичних затрат побудовикрипто-кодових конструкцій, методи логіки та теорії автоматів використані при практичній реалізації крипто-кодових конструкцій, побудові серверної частини програмно-апаратного комплексу).

Наукова новизна одержаних результатів полягає у розробці концепції, моделей і методів безпеки кіберфізичних систем та методології створення системи безпеки кіберфізичних систем, в основу яких покладено концепцію побудови багатоконтурної системи безпеки, та які базуються на гібридних крипто-кодових конструкціях зі збитковими кодами на основі модифікованої крипто-кодової конструкції Нідеррайтера на LDPC-кодах.

Найбільш вагомими науковими результатами, які містять елементи наукової новизни, є наступні:

уперше:

- розроблено концепцію побудови багатоконтурної системи захисту кіберфізичних систем, яка за рахунок інтеграції: методу забезпечення конфіденційності, цілісності та автентичності інформаційних ресурсів програмно-апаратного комплексу; методу забезпечення закриття каналу мобільного Інтернету і каналу циркуляції інформації та математичної моделі з урахуванням класифікатора загроз дає можливість створити ефективні системи захисту інформації в кіберфізичних системах та відкрити новий напрямок у побудові системи захисту інформаційних ресурсів внутрішнього та зовнішнього контуру безпеки фізичної платформи та платформи управління кіберфізичних систем.
- розроблено математичну модель безпеки кіберфізичних систем, яка на підставі розробленої концепції за рахунок врахування вагового коефіцієнту, що відображає можливості порушника, час та ймовірності реалізації загрози, дозволяє своєчасно визначити спрямованість загроз, врахувати обчислювальні ресурси нападників.
- розроблено метод забезпечення конфіденційності, цілісності та автентичності інформаційних ресурсів кіберфізичних систем в якому за рахунок

використання гібридних крипто-кодових конструкцій зі збитковими кодами на основі модифікованої крипто-кодової конструкції Нідеррайтера на LDPC-кодах, дозволяє зменшити складність формування (лінійного перетворення) та розкодування у криптограмі, забезпечити достовірність OTP-паролів в протоколі автентифікації в умовах дії гібридних загроз.

- методологію побудови системи безпеки інформаційних ресурсів кіберфізичних систем, яка за рахунок використання концепції побудови багатоконтурної системи безпеки, методу забезпечення конфіденційності, цілісності та автентичності інформаційних ресурсів, методу забезпечення закриття каналу мобільного Інтернету і каналу циркуляцію інформації та математичної моделі з урахуванням класифікатора загроз дозволяє відкрити новий емерджентний підхід побудови діючих та перспективних систем безпеки, що підвищують ефективність захисту інформаційних ресурсів кіберфізичних систем на 5%.

удосконалено:

- метод забезпечення закриття голосового каналу мобільного Інтернету, в якому за рахунок використання алгоритмів постквантової криптографії у крипто-кодових конструкціях Нідеррайтера на еліптичних кодах підвищується стійкість протоколів послуг безпеки у структурі технологій LTE та забезпечується високий рівень захищеності голосового каналу мобільного зв'язку.
- класифікатор загроз безпеці інформаційних ресурсів кіберфізичних систем, який за рахунок врахування рівня критичності загроз, відношення загрози до складової безпеки, послуги безпеки, впливу загрози відповідно до регуляторів та оцінки фінансових можливостей порушника дозволяє оцінювати гібридність загроз та відкриває новий підхід побудови діючих та перспективних систем захисту інформаційних ресурсів кіберфізичних систем..

Нові науково обґрунтовані положення прикладні рекомендації і висновки проведених досліджень схвалені та прийняті до впровадження в Державному підприємстві «Науково-технічний комплекс «Імпульс»(акт від 07.12.2021р.), в ТОВ «Мікрокрипт Технолоджіс (акт від 07.12.2023р.), в ТОВ «Сайфер ІТ» (акт від 10.01.24. в

навчальному процесі кафедри кібербезпеки Національний технічний університет «Харківський політехнічний інститут» при викладанні дисципліни «Основи побудови та захисту мікропроцесорних систем», «Інтернет речей та сервісів» для студентів спеціальності 125 «Кібербезпека та захист інформації» денної форми навчання (акт від 16.09.2022 р.)..

В роботі фактів академічного плагіату, фабрикації, фальсифікації не виявлено.

Апробація результатів дисертації.

Основні теоретичні положення та практичні результати дисертаційної роботи доповідались та обговорювались на міжнародних і всеукраїнських наукових, науково-практичних та науково-методичних конференціях, семінарах і круглих столах, зокрема:

International Congress on Humn-Computer Interaction, Optimization and Robotic Applications (HORA), (Ankara, Turkey, 2022);

CEUR Workshop Proceedings (Kharkiv, Ukraine, 2021);

IEEE 4th International Conference on Modern Electrical and Energy System (MEES),(Kremenchuk, Ukraine, 2022);

IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), (Kharkiv, Ukraine, 2022);

Proceedings of the 6th International scientific and practical conference. BoScience Publisher. (Chicago, USA, 2021);

Proceedings of the 5rd International scientific and practical conference. SPC "Sci-conf.com.ua". (Kharkiv, Ukraine 2021);

The 4th International scientific and practical conference "Innovations and prospects of world science" (Perfect Publishing, Vancouver, Canada2021);

«Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони». (Харків, Україна 2020);

Measurement and Control Systems: Problems and Perspectives (MIMCS) (Baku, Azerbaijan, 2019);

"Економічний розвиток і спадщина Семена Кузнеця" (Харків, Україна, 2019р);

«Modern Information, Measurement and Control Systems: Problems, Applications and Perspectives 2022 (MIMCS'2022)" (Baku, Azerbaijan, 2022).

Основні положення і результати дисертації викладено у 44 наукових працях, з яких дві колективні монографії обсягом 24 друк. арк. (з них 1,95 друк. арк. авторські) одна з яких індексована Scopus, вісім статей Scopus, п'ять статей у періодичних виданнях ЄС, десять статей у наукових періодичних виданнях групи Б обсягом 5,25 друк. арк. (з них 1,82 друк. арк. авторські), 17 публікацій тез доповідей за матеріалами наукових і науково-практичних конференцій12 з яких індексовано в Scopus, загальним обсягом 5,31 друк. арк. (з них 1,645 друк. арк. авторські).

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Pohasii, S., Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et. al.; Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) (2022). Modeling of security systems for critical infrastructure facilities. Kharkiv: Pc Technology Center, 196. URL: https://doi.org/10.15587/978-617-7319-57-2 (12,25 д.а., авторський внесок 1,1 д.а., полягає в формуванні об'єктивного підходу до використання постквантових механізмів безпеки на основі пропонованих моделей Лотки-Вольтери).

2. Pohasii, S., Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: Pc Technology Center, 188. (**Scopus**) URL: http://doi.org/10.15587/978-617-7319-31-2 (11,75 д.а., авторський внесок 0,9 д.а., полягає в розробці методології побудови постквантових алгоритмів для асиметричних криптосистем Нідеррайтера на еліптичних та модифікованих еліптичних кодах, їх математичні моделі та практичні алгоритми).

3. Pohasii, S., Yevseiev, S., Katsalap, V., Mikhieiev, Y., Savchuk, V., Pribyliev, Y., Milov, O., Opirskyy, I., Lukova-Chuiko, N., & Korol, I. (2022). Development of a method for determining the indicators of manipulation based on morphological synthesis . Eastern-European Journal of Enterprise Technologies, 3(9 (117), pp.22–35. (**Scopus**) URL: https://doi.org/10.15587/1729-4061.2022.258675 (0,9 д.а., авторський внесок 0,09 д.а., полягає в визначенні критеріїв ухвалення рішення про наявність ознак маніпуляції).

4. Pohasii, S., Yevseiev, S., Milov, O., Milevskyi, S., Voitko, O., Kasianenko, M., Melenti, Y., Stepanov, H., Turinskyi, O., & Faraon, S. (2020). Development and analysis of game-theoretical models of security systems agents interaction. Eastern-European Journal of Enterprise Technologies, 2(4 (104), pp.15–29. (**Scopus**) (1,0/0,09) URL: https://doi.org/10.15587/1729-4061.2020.201418 (1,0 д.а., авторський внесок 0,09 д.а., полягає визначенні обмеження на ігрові стратегії, у моменті здійснення гравцями ходу, невизначеність у кінцевій меті супротивника).

5. Pohasii, S., Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O., Petrov, O., Rzayev, K., & Khvostenko, V. (2020). Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 3(9 (105), pp.6–19. (**Scopus**) URL: https:// doi: 10.15587/1729-4061.2020.205702 (0,8 д.а., авторський внесок 0,08 д.а., полягає в розробці методика визначення категорії порушника дозволяє систематизувати порушника та на основі аналізу вагових коефіцієнтів).

6. Pohasii, S., Yevseiev, S., Zhuchenko, O., Milov, O., Lysechko, V., Kovalenko, O., Kostiak, M., Volkov, A., Lezik, A., & Susukailo, V. (2022). Development of crypto-code constructs based on LDPC codes. Eastern-European Journal of Enterprise Technologies, 2(9 (116), pp.44–59. (**Scopus**) URL: https://doi.org/10.15587/1729-4061.2022.254545 (0,7 д.а., авторський внесок 0,07 д.а., полягає в формуванні концепції побудови безпеки на основі двох контурів, для забезпечення безпеки бездротових мобільних каналів пропонується використовувати криптокодові конструкції Нідеррайтера.).

7. S., Pohasii, Yevseiev, S., Ryabukha, Y. ., Milov, O., Milevskyi, S., Melenti, Y., Ivanchenko, Y., Ivanchenko, I., Opirskyy, I., & Pasko, I. (2021). Development of a method for assessing forecast of social impact in regional communities. Eastern-European Journal of Enterprise Technologies, 6(2 (114), 30–43. (**Scopus**) URL: https://doi.org/10.15587/1729-4061.2021.249313 (0,8 д.а., авторський внесок 0,08 д.а., полягає в удосконаленні моделі, що дозволяє формувати як прогноз впливу агентів, а й взаємодія різних агентів з урахуванням їх формальних і неформальних впливів).

8. Pohasii, S., Yevseiev, S., Milevskyi, S., Milov, O., Melenti, Y., Grod, I., Berestov, D., Fedorenko, R., & Kurchenko, O. (2021). Development of a method for

assessing the security of cyber-physical systems based on the Lotka–Volterra model. Eastern-European Journal of Enterprise Technologies, 5(9 (113), pp.30–47. (**Scopus**) URL: https://doi.org/10.15587/1729-4061.2021.241638 (1,0 д.а., авторський внесок 0,11 д.а., полягає в удосконаленні моделі захищеності кіберфізичних систем: «хижак-жертва» з урахуванням обчислювальних можливостей та спрямованості цільових кібератак, «хижак-жертва»).

9. S., Pohasii, Yevseiev, S., Biesova, O., Kyrychenko, D., Lukashuk, O., Milevskyi, S., Husarova, I., Goloskokova, A., & Sobchenko, V. (2021). Development of a method for estimating the effect of transformation of the normalized frequency mismatch function of a coherent bundle of radio pulses on the quality of radar frequency resolution . Eastern-European Journal of Enterprise Technologies, 4(4(112), pp.13–22. (**Scopus**) URL: https://doi.org/10.15587/1729-4061.2021.238155 (0,7 д.а., авторський внесок 0,08 д.а., полягає в оцінці потенційної частотної роздільної здатності пучків з різним числом радіоімпульсів з типовими параметрами для когерентного імпульсного радара)

10. Pohasii, S. Yevseiev, S., Rzayev, K., Laptiev, O., Camalova, J., (2022) Development of a hardware cryptosystem based on a random number generator with two types of entropy sources. Eastern-European Journal of Enterprise Technologies 5(9-119), С. 6-16. (**Scopus**) URL: https://doi.org/10.15587/1729-4061.2022.265774 (0,4 д.а., авторський внесок 0,08 д.а., полягає в практичної реалізації генератора випадкових чисел, де як джерело ентропії використовуються два джерела: зовнішнє джерело та внутрішнє джерело.)

11. Pohasii, S. (2021).The mathematical model of information network protection based on hierarchic hypernetworks. Scientific discussion. Praha, Czech Republic.VOL 1, No 61, , pp.31– 36 ISSN 3041-4245 (0,3 д.а., авторський внесок 0,08 д.а., полягає в розробці моделей щодо опису структури сучасної інтегральної інформацій-ної мережі, параметрів її елементів та зв'язків,)

12. Pohasii, S. (2021). Analysis of information security threat assessment of the objects of information activity. International independent scientific journal. Poland. Vol. 1, №34, pp.33 – 39. ISSN 3547-2340 (0,31 д.а., авторський внесок 0,08 д.а., полягає в оцінці основних загроз інформаційної безпеці об'єктів інформаційної діяльності)

13. Pohasii, S. (2021).Information security of the e-government. Journal of science. Lyon. VOL.1, №27, pp 49– 54 ISSN 3547-2340 (0,31 д.а., авторський внесок 0,2 д.а., полягає в розробці системи їх інформаційної безпеки з використанням сучасних технологічних рішень)

14. Pohasii, S. (2021). Detection illegal of means of obtaining of information by the method of determining the deviation of the characteristics of radio signal from the specified parameters. Znanstvena misel journal. Slovenia. VOL., 1№6,1 pp. 23– 29. ISSN 3124-1123 (0,29 д.а., авторський внесок 0,2 д.а., полягає в удосконаленні методу визначення фаз випадкових сигналів від сигналів засобів легально працюючих у цьому радіодіапазоні).

15. Pohasii, S. (2021). The methodology of automatical detection of digital illegal obtaining means of information. Scientific discussion. Praha, Czech Republic.VOL 1, No 62, pp.16– 22 (0,26) ISSN 3041-4245 (0,26 д.а., авторський внесок 0,2 д.а., полягає в розроблені методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації у рамкам розробленої концепції).

16. Погасій, С. (2022). Моделі і методи захисту інформації в кіберфізичних системах. Безпека інформації. Том 28 № 2, С. 67– 79. URL: https://doi.org /10.18372/2225-5036.28.16951 (0,3 д.а.)

17. Погасій, С. (2022). Оцінка рівня безпеки в кіберфізичних системах. Захист інформації. Том 24 № 2, С. 81– 94. URL: https://doi.org/10.18372/2410-7840.24.16933 (0,3 д.а.)

18. Pohasii S., Milov O., Milevskyi S., Rzayev K. Procedural basis of cybersecurity systems. Системи управління, навігації та зв'язку. Полтава : ПНТУ, 2019. Вип. 5(57). С. 81– 86. URL: https://doi.org /10.26906/SUNZ.2019.5.072 (0,32 д.а., авторський внесок 0,07 д.а., полягає в удосконаленні підходу до класифікації та формального представлення процедур, реалізованих у системах безпеки).

19. Pohasii S., Voropay A., Korol O., Milevskyi S., Development of security mechanismsfor scada systems in the postquantium period. Системи обробки інформації, 2022, випуск 2 (169), С. 25– 33. URL: https://doi.org/10.30748/soi.2022.169.03 (0,5 д.а., авторський внесок 0,1 д.а., полягає в розробці механізму постквантової криптографії, які дозволяють забезпечити

стійкість не тільки каналів зв'язку, та й елементів структури системи управління систем).

20. Pohasii, S., Milevskyi, S., Zhuchenko, O., Tomashevsky, B., Rahimova, I. R. qizi and Serhiiev, S. (2021) "Development of Niederriter crypto-code design models on LDPC-codes", Information Processing Systems, (4(167), pp. 58– 68. URL: https://doi.org/10.30748/soi.2021.167.05 (0,5 д.а., авторський внесок 0,1 д.а., полягає в розробці постквантових криптосистем на основі крипто-кодової конструкції Нідеррайтера на кодах з малою щільністю перевірок на парність (LDPC-кодах)).

21. S., Pohasii, Yevseiev, S., & Khvostenko, V. (2021). Development of a protocol for a closed mobile internet channel based on post-quantum algorithms. Information Processing Systems, (3(166), C.35– 40. URL: https://doi.org/10.30748/soi.2021.166.03 (0,2 д.а., авторський внесок 0,07 д.а., полягає в розробці підходу до забезпечення закриття голосового каналу мобільного Інтернету на основі алгоритмів постквантової криптографії – конструкції криптокоду Нідеррейтера на еліптичних кодах).

22. Pohasii, S., Milov, O., Parkhuts, L., and Milevskyi, S. (2019) "Verification of the security systems antagonistic agents behavior model", Information Processing Systems, (4(159), pp. 65– 81. URL: https://doi.org/ 10.30748/soi.2019.159.08 (1 д.а., авторський внесок 0,25 д.а., полягає в реалізації системно-динамічної моделі взаємодії агентів-антагоністів.).

23. Pohasii, S., Milevskyi, S., Tomashevsky, B., & Voropay, N. (2022). Development of the double-contour protection concept in socio-cyberphysical systems. Advanced Information Systems, 6(2), C.57–66. URL: https://doi.org/10.20998/2522-9052.2022.2.10 (0,3 д.а., авторський внесок 0,05 д.а., полягає в розробці підходу до побудови системи безпеки на основі Концепції внутрішнього і зовнішнього контурів безпеки.).

24. Pohasii, S. Rahimova, I., Qubadova, F., &Asker zade, B. (2019). Javascript security using cryptographic hash functions. Advanced Information Systems, 3(4), C.105–108. URL: https://doi.org/10.20998/2522-9052.2019.4.15 (0,18 д.а., авторський внесок 0,04 д.а., полягає в розробці безпечного алгоритму хеш-функцій для захисту додатків на JavaScript).

25. Погасій, С., Лукова-Чуйко, Н., Толюпа, С., Лаптєва , Т., & Лаптєв, С. (2022). Удосконалення моделі захисту інформації в соціальних мережах. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка, (73), С.88–103. URL: https://doi.org/10.17721/2519-481X/2021/73-10 (0,8 д.а., авторський внесок 0,06 д.а., полягає в математичному моделюванні удосконаленої моделі захисту інформації у соціальній мережі).

26. Погасій С., Наконечний В., Лаптєв О., Лазаренко С., Мартинюк Г.,Відбір джерел з неправдивою інформацію методом бджолиної колонії. Наукоємні технології № 4(52), (2021). pp.330– 337. URL: https://doi.org/ 10.18372/2310-5461.52.16379 (0,5 д.а., авторський внесок 0,01 д.а., полягає в реалізації методу бджолиної колонії що гарантує відбір джерел інформації з неправдивою інформацію з високою ймовірністю).

27. Погасій, С. Застосування збиткових LDPC кодів в стандарті LORAWAN. Ukrainian Scientific Journal of Information Security. (2023).№ 29. С.73– 79. URL: https:// 10.18372/2225-5036.29.17871 (0,35 д.а.,).

Опубліковані праці апробаційного характеру:

1. S. Pohasii, S. Tymchenko, V. Kutsenko, S. Yevseiev and S. Milevskyi "Measuring Signals Synthesis Method on the Basis of Triangular Time-Pulse Modulation for Control of Radiotechnic Systems Technical Condition," 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2022, pp. 1-5, (Scopus). URL: https://doi.org/ 10.1109/HORA55278.2022.9799986 (0,3 д.а., авторський внесок 0,06 д.а., полягає в розробці методу синтезу вимірювальних сигналів з трикутним законом модуляції часових параметрів прямокутних імпульсів з подальшою їх вузькосмуговою фільтрацією для формування прецизійних амплітудно-модульованих сигналів.).

2. S. Pohasii, S. Yevseiev, S. Milevskyi, L. Bortnik, V. Alexey and K. Bondarenko "Socio-Cyber-Physical Systems Security Concept," 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2022, pp. 1-8, (Scopus). URL: https://doi.org/ 10.1109/HORA55278.2022.9799957 (0,5 д.а., авторський внесок 0,09 д.а., полягає в

тому, що запропоновано концепцію безпеки соціально-кіберфізичних систем, яка враховує інтеграцію технологій, систем безпеки окремих компонентів розумного міста та інтеграцію кіберзагроз у компоненти безпеки.).

3. Hatsenko, L., Lutsenko, A., Skopintsev, O., Pohasii, S. Investigation of Measurement Errors of Electrical Signals Characteristics of Energy Supply Systems. 2021CEUR Workshop Proceedings 3126, C. 184-191, (Scopus). URL: https://ceur-ws.org/Vol-3126/paper27.pdf ISSN 16130073 (0,4 д.а., авторський внесок 0,1 д.а., полягає в дослідженні методу вимірювання частоти (періоду) синусоїдального сигналу на основі перетворення напруги в частоту імпульсів.).

4. Hatsenko, L., Herasimov, S., Pohasii, S. Investigation of the Effect of Harmonic Interference on the Error with Frequency Conversion of Energy Supply Systems on Water Transport Vehicles . 2021CEUR Workshop Proceedings 3188, C. 237-243, (Scopus). URL: https://ceur-ws.org/Vol-3188/short5.pdf ISSN 16130073 (0,3 д.а., авторський внесок 0,1 д.а., полягає в обґрунтуванні актуальної науково-технічної проблеми розробки прецизійних методів вимірювання параметрів електричних сигналів (як правило, гармонійних напруг).).

5. Milov, O., Melenti, Y., Milevskyi, S., Pohasii, S., Yevseiev, S. Cyber Terrorism as an Object of Modeling. 2021 CEUR Workshop Proceedings 3200, C. 204-210, (Scopus). URL: https://ceur-ws.org/Vol-3200/paper28.pdf ISSN 16130073 (0,4 д.а., авторський внесок 0,1 д.а., полягає в дослідженні питань, пов'язаних з характеристикою кібертероризму, а також суміжних концепцій тероризму та кіберпростору.).

6. Yevseiev, S., Korol, O., Veselska, O., Pohasii, S., Khvostenko, V. Evaluation of Cryptographic Strength and Energy Intensity of Design of Modified Crypto-Code Structure of McEliece with Modified Elliptic Codes. 2021CEUR Workshop Proceedings 3200, C. 135-148, (Scopus). URL: https://ceur-ws.org/Vol-3200/paper20.pdf ISSN 16130073 (0,6 д.а., авторський внесок 0,15 д.а., полягає в пропозиції використовувати метод оцінки криптографічної стійкості різних криптосистем на основі ентропійного підходу.).

7. B. Vorobiov, R. Zaitsev, K. Minakova, M. Kirichenko, S. Milevskyi and S. Pohasii, "Regulation Quality Investigation on Different Plant Model Usage While Neural

Network Training for DC Motor Control," 2022 IEEE 4th International Conference on Modern Electrical and Energy System (MEES), Kremenchuk, Ukraine, 2022, pp. 1-6, (Scopus). URL: https://doi.org/10.1109/MEES58014.2022.10005699 (0.3 д.а., авторський внесок 0.05 д.а., полягає в проведенні порівняльного аналізу роботи системи керування на основі нейроконтролера з використанням моделей різного ступеня складності.).

8. S. Pohasii, R. Korolov, B. Vorobiov, M. Bril, O. Serhiienko and S. Milevskyi, "UAVs Intercepting Possibility Substantiation: Economic and Technical Aspects," 2022 IEEE 4th International Conference on Modern Electrical and Energy System (MEES), Kremenchuk, Ukraine, 2022, pp. 1-6 (Scopus). URL: https://doi.org/10.1109/MEES58014.2022.10005710 (0,3 д.а., авторський внесок 0,09 д.а., полягає в визначенні економічної та технічної доцільності використання керованого БПЛА перехоплювача за методом паралельного заходу на посадку.).

9. S. Pohasii, V. Baranova, O. Bilotserkivskyi, O. Haponenko, O. Serhiienko and B. Vorobiov, "Application of Cost-Effective Acoustic Intelligence to Protect Critical Facilities from Drone Attacks," 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 2022, pp. 1-6, (Scopus). URL: https://doi.org/10.1109/KhPIWeek57572.2022.9916446 (0,3 д.а., авторський внесок 0,09 д.а., полягає в аналізі БПЛА як об'єкта виявлення та видачі цілевказівок засобами акустичного спостереження.)

10. S. Herasymov, V. Olenchenko, S. Yevseiev, S. Milevskyi and S. Pohasii, "Investigation of the Dynamic Filters' Characteristics for the Analysis of Random Signals During Data Transmission," 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 2022, pp. 1-6, (Scopus). URL: https://doi.org/10.1109/KhPIWeek57572.2022.9916327 (0,3 д.а., авторський внесок 0,06 д.а., полягає в отриманні результатів, які дають змогу задавати оптимальні характеристики при проектуванні вузькосмугових динамічних фільтрів аналізаторів спектру випадкового сигналу та пропонуються для використання в системах зв'язку для фільтрації перешкод)

11. Pohasii, S., Vorobiov , B. (2021). Analysis of the applicability of the model of the quality of software systems and the most important parameters of the quality of iot

systems. Modern directions of scientific research development. Proceedings of the 6th International scientific and practical conference. BoScience Publisher. Chicago, USA. pp. 204-212. ISBN 978-1-73981-126-6 (0,25 д.а., авторський внесок 0,125 д.а., полягає в аналізі моделей якості програмних систем та аналізу, проведеного для визначення ключових параметри, які є актуальними для різних типів рішень IoT.)

12. Pohasii, S., Vorobiov, B. (2021). Эволюция киберфизических систем. Topical issues of modern science, society and education. Proceedings of the 5rd International scientific and practical conference. SPC "Sci-conf.com.ua". Kharkiv, Ukraine. pp. 440-446. ISBN 978-966-8219-85-6 (0,25 д.а., авторський внесок 0,125 д.а., полягає в огляді визначень кіберфізичних систем розкриває загальну термінологію інформатики та системної інженерії)

13. Pohasii, S., Vorobiov , B. (2021). Building an ontology of the software architecture of the internet of things. The 4th International scientific and practical conference "Innovations and prospects of world science" (December 1-3, 2021) Perfect Publishing, Vancouver, Canada. pp 252-257. ISBN 978-1-4879-3794-2 (0,25 д.а., авторський внесок 0,125 д.а., полягає в визначені зв'язків між елементами архітектури програмного забезпечення та необхідними параметрами якості системи, що дозволяє в подальшому будувати залежності між зазначеними поняттями)

14. Погасій, С., Гаврилова, А., Використання геш-кодів, створених за допомогою алгоритма UMAC на крипто-кодових конструкціях, для забезпечення необхідного рівня стійкості до зломів. Матеріали регіон. круг. столу «Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони». Харків, 2020. С. 290 – 294. ISBN 978-617-7912-02-5 (0,31 д.а., авторський внесок 0,15 д.а., полягає в удосконаленні механізму автентичності повідомлень можливо на модифікованих (укорочених, і / або подовжених) еліптичних кодах, а також на збиткових кодах з використанням гібридних крипто-кодових конструкцій).

15. Pohasii, S., Milevskyi, S. (2019). Cybersecurity issues in the internet of things. 1st International Conference: Modern Information, Measurement and Control Systems: Problems and Perspectives (MIMCS'2019), p. 33. E-ISBN: 978-9949-01-395-1 (0,125

д.а., авторський внесок 0,07 д.а., полягає в аналізі проблематики, пов'язаною з кібербезпекою в Інтернеті речей їх впровадження в технологію «розумний будинок»)

16. Pohasii, S., Milevskyi, S. (2019).Internet security problems caused by artificial intelligence. Матеріали Міжнародної науково-практичної конференції "Економічний розвиток і спадщина Семена Кузнеця": тези доповідей, 30 – 31 травня 2019 р. – Х.: ХНЕУ імені Семена Кузнеця, С.248-249. http://repository.hneu.edu.ua/handle/123456789/22165 (0,125 д.а., авторський внесок 0,07 д.а., полягає в аналізі альтернативних підходів створення штучного інтелекту та принципів функціонування мозку)

17. Pohasii, S., Milevskyi, S., Voropay, N., Korol, O. (2022). A Multilevel Approach to the Security of the Internet of Things. «Modern Information, Measurement and Control Systems: Problems, Applications and Perspectives 2022 (MIMCS'2022)" URL: https://doi.org/PREFIX: 10.36962/ GBSSJAR (0,3 д.а., авторський внесок 0,09 д.а., полягає в дослідженні системи моніторингу мережевої інфраструктури та пов'язаних з нею операцій обслуговування в режимі реального часу для обміну даними в безпечному режимі)

Структура та обсяг дисертації.

Дисертація складається зі вступу, п'яти розділів, висновків, списку використаних джерел з 255 найменувань, 4 додатків. Повний обсяг роботи – 325 сторінки комп'ютерного тексту, з них 261 сторінок основного тексту. Дисертація містить 108 рисунків, 30 таблиць (19 сторінок – рисунки і таблиці, які повністю займають площу сторінки).

Повнота викладення матеріалів дисертації в публікаціях та особистий внесок у них автора.

Основні наукові положення та результати дослідження опубліковано автором самостійно та у співавторстві у 44 наукових працях загальним обсягом 42,99 друк. арк. (з них 7,38 друк. арк. належить особисто автору), дві колективні монографії обсягом 24 друк. арк. (з них 2,0 друк. арк. авторські), вісім статей у наукових

періодичних виданнях, проіндексованих у базах даних Scopus, п'ять статей у періодичних виданнях ЄС, десять статей у наукових фахових виданнях України категорії "Б", одна стаття в інших наукових періодичних виданнях обсягом 13,68 друк. арк. (з них 3,745 друк. арк. авторські), 17 публікацій тез доповідей за матеріалами міжнародних наукових і науково-практичних конференцій обсягом 5,31 друк. арк. (з них 1,64 друк. арк. авторські), відтворюють основний зміст роботи та наукові результати дисертації і відповідають нормативним вимогам МОН України.

Наукові публікації відповідають вимогам п. 8 Порядку присудження та позбавлення наукового ступеня доктора наук (Постанова Кабінету Міністрів України від 17 листопада 2021 р. № 1197) та наказу МОН України № 1220 від 23.09.2019 р. «Про опублікування результатів дисертацій на здобуття наукових ступенів доктора і кандидата наук».

Оцінка мови та стилю дисертації.

Дисертаційна робота написана грамотною діловою українською мовою з науковим стилем викладення її змісту, характеризується цілісністю, смисловою завершеністю, логічною послідовністю розгляду питань, об'єктивністю викладення, точністю використання спеціальної термінології, ясністю і стислістю, чітко структурована, а стиль викладу матеріалу дослідження, наукових положень, висновків і рекомендацій забезпечує легкість і доступність їх сприйняття. Застосована у роботі наукова термінологія є загальновизнаною, стиль викладення результатів теоретичних та експериментальних досліджень, нових наукових положень, висновків і рекомендацій забезпечує доступність їх сприйняття та використання.

ЗАГАЛЬНИЙ ВИСНОВОК:

Вважати, що дисертаційна робота **Погасія Сергія Сергійовича на тему: «Моделі і методи захисту в кіберфізичних системах»**, яка подана на здобуття ступеня доктора наук, за актуальністю, ступенем новизни, науковим рівнем та практичною цінністю, змістом та оформленням повністю відповідає вимогам п. 7, 9 Порядку присудження та позбавлення наукового ступеня доктора наук (Постанова Кабінету Міністрів України від 17 листопада 2021 р. № 1197) та наказу МОН України № 40 від 12.01.2017 р. «Про затвердження вимог до оформлення дисертації».

Рекомендувати дисертаційну роботу **Погасія Сергія Сергійовича на тему: «Моделі і методи захисту в кіберфізичних системах»** до захисту на здобуття ступеня доктора наук у спеціалізованій вченій раді за спеціальністю 05.13.21 «Системи захисту інформації».

Рецензенти:

д.т.н., професор Галина ГАЙДУР

д.т.н., професор. Володимир АХРАМОВИЧ

д.т.н., професор Віталій САВЧЕНКО

Головуюча:
д.т.н., професор

Галина ГАЙДУР