

## АНОТАЦІЯ

*Стрелкіна Анастасія Андріївна.* Моделі та методи інформаційної технології забезпечення гарантоздатності медичних систем на основі Інтернету речей. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки. – Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, 2019.

Дисертаційна робота присвячена підвищенню гарантоздатності медичних систем на основі Інтернету речей базуючись на розробці та практичному застосуванні моделей та методів інформаційної технології для медичних систем. Об'єктом дослідження є медичні системи на основі Інтернету речей та підходи оцінювання їх функціонування та безпеки. Предметом дослідження є моделі та методи інформаційної технології забезпечення гарантоздатності медичних систем на основі Інтернету речей.

У роботі виконано аналітичний огляд сучасних моделей та методів оцінювання і забезпечення гарантоздатності медичних систем на основі Інтернету речей. Встановлено, що існуючі моделі та методи не враховують специфічних особливостей медичної галузі, недостатньо формалізовані і мають обмаль інструментальних засобів підтримки оцінювання і забезпечення гарантоздатності такого роду систем.

З урахуванням проведеного аналізу в роботі поставлено та вирішено наукове завдання розроблення моделей та методів інформаційної технології забезпечення гарантоздатності медичних систем на основі Інтернету речей з урахуванням атак на вразливості і дефектів програмних та апаратних компонентів, а також процедур функціонування медичного пристрою.

Обґрунтована методика проведення досліджень і математичний апарат, що використовується в дослідженні. При вирішенні наукових задач використовувалися методи системного аналізу, методи теоретико-множинного

опису, теорії ймовірностей, апарат теорії марковських процесів, числові методи розв'язання лінійних систем диференційних рівнянь, технології аналітичного моделювання алгоритмів поведінки відмовостійких систем, методи математичного моделювання і теорії оптимізації, теорії ігор, методи ризик-аналізу, методи об'єктно-орієнтованого програмування, методи функціонального моделювання.

Удосконалено комплекс моделей оцінювання гарантоздатності медичних систем на основі Інтернету речей шляхом врахування різних функціональних станів, типів відмов та кібератак, що дає змогу розраховувати показники готовності, функціональної безпеки, кібербезпеки, визначати їх залежність від параметрів медичних мобільних пристроїв та хмарного середовища.

Вперше одержано модель функціональної поведінки медичного пристрою, яка, на відміну від відомих, враховує різні закони розподілу часу між заявками на обслуговування, а також різні типи відмов за рівнем критичності, що дозволяє визначити вплив показників медичного пристрою на готовність та гарантоздатність медичної IoT системи в цілому.

Набув подальшого розвитку метод забезпечення кібербезпеки медичних систем на основі Інтернету речей шляхом вибору контрзаходів з використанням теорії матричних ігор, що дозволяє вибирати за максіміним критерієм множину засобів захисту.

Удосконалено метод кейс-орієнтованої оцінки кібербезпеки медичних систем на основі Інтернету речей за рахунок формування профільоутворюючої бази стандартів та функціональних вимог, а також процедури вибору інструментів оцінювання, що дозволяє підвищити повноту оцінювання.

Усі теоретичні розробки дисертації доведено до конкретних інженерних методик та алгоритмів із застосуванням запропонованої інформаційної технології оцінювання і забезпечення гарантоздатності медичних систем на основі Інтернету речей. Розроблені методики та інструментальні засоби «IoHTStandard» і «GTC», які є безпосередньо частиною прикладної інформаційної технології оцінювання і забезпечення гарантоздатності медичних систем на основі Інтернету речей, що, в

свою чергу, дозволило підвищити повноту оцінювання гарантоздатності такого роду систем.

Розроблені моделі, методи, інформаційне та програмне забезпечення використані у ТОВ «ХАІ-МЕДИКА» (акт впровадження від 10.09.2019 р.), а також впроваджено під час виконання держбюджетного проекту кафедри комп'ютерних систем, мереж і кібербезпеки (акт впровадження від 04.09.2019 р.), а також у навчальному процесі Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ» та виконанні міжнародних проектів за програмами TEMPUS і ERASMUS+ (акт впровадження від 04.09.2019 р.).

Ключові слова: гарантоздатність, Інтернет речей, марковська модель, теорія ігор, медична система, Safety Case підхід.

#### Список публікацій здобувача за темою дисертації

1. A. Strielkina, D. Uzun, V. Kharchenko and A. Tetskyi, "Modeling and Availability Assessment of Mobile Healthcare IoT Using Tree Analysis and Queueing Theory", in *Dependable IoT for Human and Industry: Modeling, Architecting, Implementation*, River Publishers, 2018, pp. 105-126.

2. A. Strielkina, V. Kharchenko and D. Uzun, "Availability Models of the Healthcare Internet of Things System Taking into Account Countermeasures Selection", *Information and Communication Technologies in Education, Research, and Industrial Applications*, vol 1007, pp. 220-242, 2019. DOI: 10.1007/978-3-030-13929-2\_11.

3. A. Strielkina, A. Tetskyi, B. Selin, O. Solovyov, D. Uzun, "Service for Vulnerabilities Analysis and Security Assessment of Open Source Systems", *CERes Journal*, Volume 1, Issue 2, pp. 53-64, 2015.

4. А. А. Стрелкіна, Д. Д. Узун, "Забезпечення кібербезпеки медичних систем: виклики і рішення в контексті Інтернету речей", *Радіоелектронні і комп'ютерні системи*, № 1, с. 44–50, 2017.

5. А. С. Андрійчук, А. А. Стрелкіна, "Розроблення моделі керування доступом до приватної медичної інформації", *Радіоелектронні і комп'ютерні системи*, № 2, с. 26–32, 2018.

6. Д. Э. Ляхов, А. А. Стрелкина, Д. Д. Узун, "Анализ методов и средств оценивания и обеспечения кибербезопасности IoT системы", *Открытые информационные и компьютерные интегрированные технологии : сб. науч. тр.*, Харьков, вып. 80, с. 182-193, 2018.

7. А. А. Стрелкіна, "Інформаційна технологія оцінювання і забезпечення гарантоздатності медичних IoT систем", *Радіоелектронні і комп'ютерні системи*, №. 3(91), с. 48-54, 2019.

8. A. Strielkina and D. Uzun, "Researching the Applicability of Mathematical Approaches for Modeling Cyber Security Processes", *PhD Symposium at 13th International Conference on ICT in Education, Research, and Industrial Applications ICTERI 2018 co-located with 14th International Conference on ICT in Education, Research, and Industrial Applications (ICTERI 2017)*, pp. 29-35, 2017.

9. A. Strielkina, D. Uzun and V. Kharchenko, "Modelling of healthcare IoT using the queueing theory", *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, pp. 849-852, 2017. DOI: 10.1109/idaacs.2017.8095207.

10. A. Streilkina, V. Kharchenko and D. Uzun, "A Markov Model of Healthcare Internet of Things System Considering Failures of Components", *14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer*, p. 14, 2018.

11. A. Strielkina, O. Illiashenko, M. Zhydenko and D. Uzun, "Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment", *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, pp. 67-73, 2018. DOI: 10.1109/dessert.2018.8409101.

12. A. Strielkina, S. Volochiy and V. Kharchenko, "Discrete-Continuous Stochastic Model of Insulin Pump Functioning for Health IoT System Using Erlang Phase

Method", *5th International Workshop on Theory of Reliability and Markov Modeling for Information Technologies (TheRMIT 2019)*, pp. 794-809, 2019.

13. A. Strielkina, B. Volochiy and V. Kharchenko, "Model of Functional Behavior of Healthcare Internet of Things Device", *2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, pp. 63-69, 2019. DOI: 10.1109/dessert.2019.8770020.

14. А. А. Стрелкіна, "Исследование подходов к обеспечению кибербезопасности медицинских систем в контексте интернета вещей", *Всеукраїнська науково-технічна конференція «Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2016*, Харків: Нац. аерокосм. ун-т "ХАІ", Том 2, с.286-287, 2016.

15. М. О. Жиденко, А. А. Стрелкіна, "Дослідження нормативних документів щодо ризиків кібербезпеки медичних пристроїв", *Міжнародна науково-практична конференція «Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі»*, с. 94, 2017.

16. А. А. Стрелкіна, А. Г. Тецький, О. А. Ілляшенко, "Аналіз можливостей використання вільного програмного забезпечення R для задач моделювання", *Всеукраїнська науково-технічна конференція «Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2017*, Харків: Нац. аерокосм. ун-т "ХАІ", Том 2, с.233, 2017.

17. А. А. Стрелкіна, "Розроблення моделей готовності IoT систем в галузі охорони здоров'я", *Всеукраїнська науково-технічна конференція «Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2018*, Харків: Нац. аерокосм. ун-т "ХАІ", Том 2, с.197, 2018.

## ANNOTATION

*Strielkina Anastasiia.* Information technology models and methods of dependability ensuring of healthcare Internet of things systems.– Manuscript copyright.

Thesis on competition of scientific degree of Doctor of Philosophy by specialty 122 – Computer Science. – National Aerospace University “Kharkiv Aviation Institute”, Kharkiv, 2019.

The dissertation is devoted to the enhancing the dependability of healthcare IoT systems based on the development and practical application of information technology models and methods for healthcare systems.

The scientific results are:

1) the complex of models of evaluation of the healthcare IoT systems dependability by taking into account different functional states, types of failures and cyberattacks has been improved, which allows to calculate indicators of availability, functional safety and cybersecurity, to determine their dependence on the parameters of medical mobile devices and cloud environment;

2) for the first time, a model of functional behavior of a healthcare device has been obtained, which, unlike the known ones, takes into account different laws of time distribution between service requests, as well as different types of failures by the level of criticality, which allows to determine the influence of indicators of the healthcare device on availability and dependability of healthcare IoT system in general;

3) the method of providing cybersecurity for healthcare IoT systems has been further developed by the choice of countermeasures using matrix game theory, which allows to choose the number of protection tools by the maximin criterion.

4) the method of case-based assessment of the healthcare IoT system cybersecurity has been improved through the formation of a profile-based base of standards and functional requirements, as well as procedures for selecting assessment tools to improve the completeness of the assessment.

Key words: dependability, Internet of Things, Markov model, game theory, healthcare system, Safety Case approach.