ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

УДК 004.77.056:61 **doi: 10.32620/reks.2019.3.05**

А. А. СТРЄЛКІНА

Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Україна

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ОЦІНЮВАННЯ І ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ МЕДИЧНИХ IoT СИСТЕМ

Медичні системи, що функціонують в середовищі Інтернету речей, набувають все більшого розповсюдження і за попередніми прогнозами їх вплив буде лише збільшуватися. Проте нові концепції та застосування новітніх технологій несуть певні ризики, включаючи відмови кінцевих користувацьких пристроїв, інфраструктури, що, в свою чергу, може призвести до найгіршого результату. У зв'язку з цим проблеми оцінювання і забезпечення гарантоздатності при використання цієї технології збільшуються. ***Об'єктом*** *дослідження і аналізу в даній роботі є медична система, що функціонує в середовищі Інтернету речей.* ***Метою*** *дослідження даної роботи є опис та розроблення структури і функціональної схеми інформаційної технології (ІТ) оцінювання і забезпечення гарантоздатності медичних систем на основі Інтернету речей, яка базується на моделях, методах та процедурах оцінювання і забезпечення гарантоздатності і формалізованих методах проектування, які містять такі етапи синтезу проектних рішень: вибір моделі, вибір методу, вирішення задачі і прийняття рішень. Процес створення інформаційної технології складається з таких етапів, як визначення: основних процесів, які відбуваються при оцінюванні і забезпеченні гарантоздатності медичних IoT систем; вхідних даних; вихідних даних; елементів механізмів; елементів керування. Розроблена структура інформаційної технології складається з наступних процесів: формування вимог до гарантоздатності медичних систем на основі Інтернету речей; визначення компонент медичних IoT систем, які наражаються на кібератаки та відмови; визначення показників готовності медичних IoT систем; визначення показників функціональності медичних пристроїв; вибір контрзаходів захисту медичної IoT системи від кібератак; кейс-орієнтоване оцінювання кібербезпеки медичних систем, що функціонують в середовищі Інтернету речей. Як* ***результат****, в даній роботі наведена IDEF0-діаграма інформаційної технології оцінки та забезпечення гарантоздатності медичних систем на основі Інтернету речей. А також представлені основні етапи реалізації розробленої інформаційної технології.*

Ключові слова: *IDEF0; гарантоздатність; інсулінова помпа; Інтернет речей; інформаційна технологія; медична система.*

Вступ

Інтернет речей (англ. Internet of Things, IoT) є однією з найпопулярніших і передових технологій за останній час. Одним з найважливіших напрямків, де сучасні технології можуть принести помітну користь суспільству, є сфера охорони здоров'я і медицини. Мережеві медичні пристрої вже набувають все більшого поширення і за попередніми прогнозами до 2022 року їх ринок становитиме близько 410 мільярдів доларів [1].

Для класифікації медичних пристроїв зазвичай використовують Загальну номенклатуру медичного обладнання [2]. З точки зору безпеки, медичні пристрої поділяються на класи I, IIa, IIб і III відповідно до міри потенційного ризику від їх застосування:

1) до класу I – медичні вироби з низькою мірою ризику;

2) до класу IIa – медичні вироби з середньою мірою ризику;

3) до класу IIб – медичні вироби з підвищеною мірою ризику;

4) до класу III – медичні вироби з високою мірою ризику.

Для класифікації по функціональному призначенню виділяють такі критерії, як тривалість застосування, інвазивність, спосіб взаємодії з людським тілом, джерело енергії, виконання життєво важливих функцій тощо. На рис. 1 зображено класифікацію медичних пристроїв за критеріями типу пристроїв, мети застосування і типу використовуваних компонент.

Одним з найбільш затребуваних напрямків у лікуванні, моніторингу, прогнозуванні та медикаментозному лікуванні є діабет. Відповідно до [3], за оцінками, у 2014 році близько 422 мільйони дорослих живуть з цукровим діабетом, порівняно з 108 мільйонами у 1980 році, глобальна поширеність діабету майже подвоїлася з 1980 року, зросла з 4,7 %

Рис. 1. Класифікація медичних пристроїв

до 8,5% у дорослому населенні. спричинило 1,5 мільйона смертей у 2012 році, а високий рівень глюкози в крові спричинив ще 2,2 мільйони смертей, і за прогнозами, діабет стане 7-ою провідною причиною смерті в 2030 році.

Мережеві медичні пристрої зазвичай поєднуються у мережу, яка включає в себе пацієнтів, організації охорони здоров'я, лікарів та інших. Складовими IoT інфраструктури в медичній галузі є: хмара, пристрій (бездротова натільна комп'ютерна мережа, англ. wireless body area network, WBAN), медичні працівники та канали зв'язку між пристроєм і хмарою, і постачальник медичних послуг і хмара (рис. 2) [4-6].

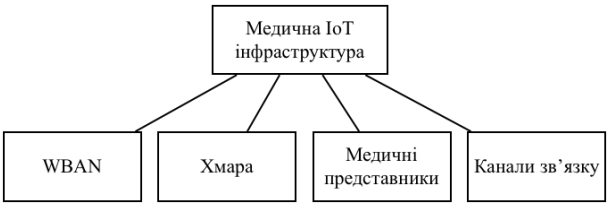

Рис. 2. Компоненти медичної IoT інфраструктури

Зрозуміло, що медична IoT система є системою, з особливими вимогами до безпеки. Якщо інсулінова помпа або будь-який інший важливий елемент інфраструктури не працює або працює неналежним чином, то здоров'ю пацієнтів може бути задана шкода, вони можуть впасти в кому, оскільки рівень цукру в крові занадто високий або низький, або попередні призначення лікарів пацієнт не отримує вчасно тощо. Отже, медична IoT система повинна відповідати вимогам гарантоздатності та надавати цілодобове обслуговування без винятків.

Для таких систем характерна велика кількість відмов через динамічність, багатокомпонентність та багаторівневість. На рис. 3 показано статистику відмов медичних пристроїв за останні роки [7].

Відмови систем можуть відбуватися через різні причини [8] і в більшості випадків пов'язані з проблемами кібербезпеки та конфіденційності, функціонональної безпеки та стандартизації [9]. Забезпечення кібербезпеки, функціональної безпеки, готовності та надійності повинно розглядатися більш широко, не як поодинокі властивості, а як комплексне поняття – гарантоздатність [10].

Рис. 3. Статистика по кількості зареєстрованих збоїв інсулінових помп відносно загальної кількості збоїв медичного обладнання

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Отже, *метою* даної роботи є розроблення структури і функціональної схеми інформаційної технології (ІТ) оцінювання і забезпечення гарантоздатності медичних IoT систем, яка базується на моделях, методах та процедурах оцінювання і забезпечення гарантоздатності і формалізованих методах проектування, які містять такі етапи синтезу проектних рішень: вибір моделі, вибір методу, вирішення задачі і прийняття рішень.

1. Елементи інформаційної технології оцінювання і забезпечення гарантоздатності медичних систем на основі Інтернету речей

Елементи ІТ представлені у таблиці 1 згідно з алгоритмом її реалізації:

– *процес* забезпечення та/або оцінки гарантоздатності медичних IoT систем, який має фіксовану мету і приводить до конкретного результату;

– *вхідні дані*, які використовуються і перетворюються під час виконання процесу для отримання результату (вихідних даних);

– *вихідні дані*, які представляють результат виконання процесу;

– *механізми*, тобто ресурси, які виконують процес;

– *елементи керування* представляють з себе керуючі, регламентуючі і нормативні дані, якими користується процес.

Структура інформаційної технології складається з наступних процесів: формування вимог ТЗ до гарантоздатності МС на основі Інтернету речей; визначення компонент МС на основі Інтернету речей, які наражаються на кібератаки і відповідні відмови;

Таблиця 1

Елементи інформаційної технології оцінювання і забезпечення гарантоздатності медичних IoT

№ п/п	Процес	Вхідні дані	Вихідні дані	Механізми	Керування
1	Формування вимог ТЗ до гарантоздатності МС IoT.	– ТЗ, контекст використання, – вимоги замовника	– результати аналізу документації, – вимоги до МС IoT.	– ЕПР, – БД НД, – ІЗ визначення вимог до МС IoT.	НД.
2	Визначення компонент МС IoT, які наражаються на кібератаки і можуть відмовляти.	– результати аналізу документації, – вимоги до МС IoT, – дані репозиторіїв вразливостей і відмов.	Результати аналізу вразливих елементів.	– ЕПР, – БД компонент МС IoT.	НД.
3	Визначення значення готовності МС IoT.	– результати аналізу вразливих елементів, – дані репозиторіїв вразливостей і відмов, – показники функціональності медичних пристроїв, – контрзахід захисту МС IoT від кібератак.	Показники готовності МС IoT.	– ЕПР, – ІЗ оцінювання готовності.	Комплекс моделей оцінювання гарантоздатності.
4	Визначення показників функціональності медичних пристроїв.	– ТЗ, – вимоги замовника, – результати аналізу вразливих елементів.	Показники функціональності медичних пристроїв.	– ЕПР, – ІЗ побудови САМ.	Комплекс моделей оцінювання гарантоздатності (модель функціональної поведінки).
5	Вибір контрзаходів захисту МС IoT від кібератак.	– ТЗ, – дані репозиторієв вразливостей і відмов, – результати аналізу вразливих елементів, – показники готовності МС IoT.	Контрзахід захисту МС IoT від кібератак.	– ЕПР, – ІЗ вибору контрзаходів.	Метод вибору контрзаходів від кібератак.
6	Кейс-орієнтоване оцінювання кібербезпеки МС IoT.	– показники готовності МС IoT, – контрзахід захисту МС IoT від кібератак.	– звіт по оцінювання гарантоздатності МС IoT, – рекомендації по забезпеченні гарантоздатності.	– ЕПР, – система генерації звітів.	Метод кейс-орієнтованої оцінки.

визначення показників готовності МС на основі Інтернету речей; визначення показників функціональності медичних пристроїв; вибір контрзаходів захисту медичної IoT системи від кібератак; кейс-орієнтоване оцінювання кібербезпеки медичних IoT систем.

У таблиці 1 використані наступні позначення:

ТЗ – технічне завдання;

МС IoT – медична система на основі Інтернету речей;

ЕПР – експерти, що приймають рішення;

БД – база даних;

ДРВВ – дані репозиторієв вразливостей і відмов;

ІЗ – інструментальний засіб;

НД – нормативні документи, стандарти, інструкції;

САМ – структурно-автоматна модель.

2. Етапи реалізації інформаційної технології

Загальна функціональна модель інформаційної технології, яка базується на моделях та методах оцінювання та забезпечення гарантоздатності медичних систем на основі Інтернету речей, наведена на рис. 2 у вигляді IDEF0-діаграми.

Основні етапи реалізації розробленої ІТ:

Eman 1. Відбувається аналіз проектної документації для формування вимог ТЗ до гарантоздатності МС на основі Інтернету речей. Для цього, в першу чергу, необхідно провести аналіз ТЗ з описом системи, контексту використання і вимог замовника. *Результатом* цього виявлення вимог є вихідна інформація про систему, що моделюється, а саме: логіка її функціонування, функції, що виконуються і т. д. А також складається список вимог до гарантоздатності МС на основі Інтернету речей, що досліджується(наприклад, вимоги до критичності відмов).*Eman 2.* Визначення компонент МС на основі Інтернету речей, які можуть відмовити, у тому числі внаслідок кібератак, на основі вихідної інформації, що була отримана на першому етапі даної ІТ, а також даних відкритих репозиторіїв вразливостей та відмов. *Результатом* виконання етапу є список вразливих до кібератак та відмов елементів МС на основі Інтернету речей, можливих кібератак і відмов.

Eman 3. Визначення значення показника готовності МС на основі Інтернету речей, використовуючи моделі готовності, які враховують відмови компонентів медичної IoT інфраструктури, атаки на вразливості компонентів. Результатом виконання етапу є показник готовності [11, 12], а також супровідна інформація про найбільш можливі кібератаки та вразливі компоненти системи, що досліджується.

Eman 4. Визначаються показники функціональності медичних пристроїв на основі ТЗ, вимог замовника, результату аналізу вразливих елементів. *Результатом* виконання етапу є показники функціональності медичних пристроїв (ймовірність виконання завдання медичним пристроєм) [13].

Eman 5. Відбувається вибір контрзаходів захисту медичної IoT системи від кібератак на основі вимог ТЗ, даних відкритих репозиторіїв вразливостей, результатів аналізу вразливих елементів, а також отриманих на попередніх етапах показників готовності МС на основі Інтернету речей. *Результатом* виконання даного етапу буде оптимальний засіб захисту МС на основі Інтернету речей для всього діапазону можливих кібератак [14].

Eman 6. Відбувається кейс-орієнтоване оцінювання кібербезпеки МС на основі Інтернету речей на основі вихідної інформації, що була отримана на попередніх етапах, а саме показників готовності МС і обраного контрзаходу захисту медичної IoT системи від кібератак. *Результатом* виконання цього етапу є висновок про відповідність системи, що досліджується, вимогам до її гарантоздатності та рекомендації щодо по забезпеченні гарантоздатності за результатами оцінювання [15].

Висновки

Отже, в даній статті представлена інформаційна технологія оцінювання і забезпечення гарантоздатності медичних IoT систем, яка базується на моделях та методах оцінювання і забезпечення гарантоздатності. Запропонована ІТ враховує процеси формування вимог до гарантоздатності, визначення компонент МС, які можуть наражатися на кібератаки та відмовити, значення готовності, показників функціональності медичних пристроїв, вибір контрзаходів захисту медичної IoT системи від кібератак і кейс-орієнтованого оцінювання кібербезпеки, що дозволяє підвищити повноту оцінювання і забезпечення гарантоздатності медичних IoT систем.

Подальші дослідження можуть бути спрямовані на модифікацію та удосконалення розробленої інформаційної технології.

Література

1. The global market for IoT healthcare tech will top $400 billion in 2022 [Електронний ресурс] // BI Intelligence. – 2016. – Режим доступу: www.businessinsider.com/the-global-market-for-iot-healthcare-tech-will-top-400-billion-in-2022-2016-5. – 26.08.2019.

2. User Guide [Електронний ресурс] // GMDN Agency. – Режим доступу: http://www.gmdnagency.com/. – 26.08.2019.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

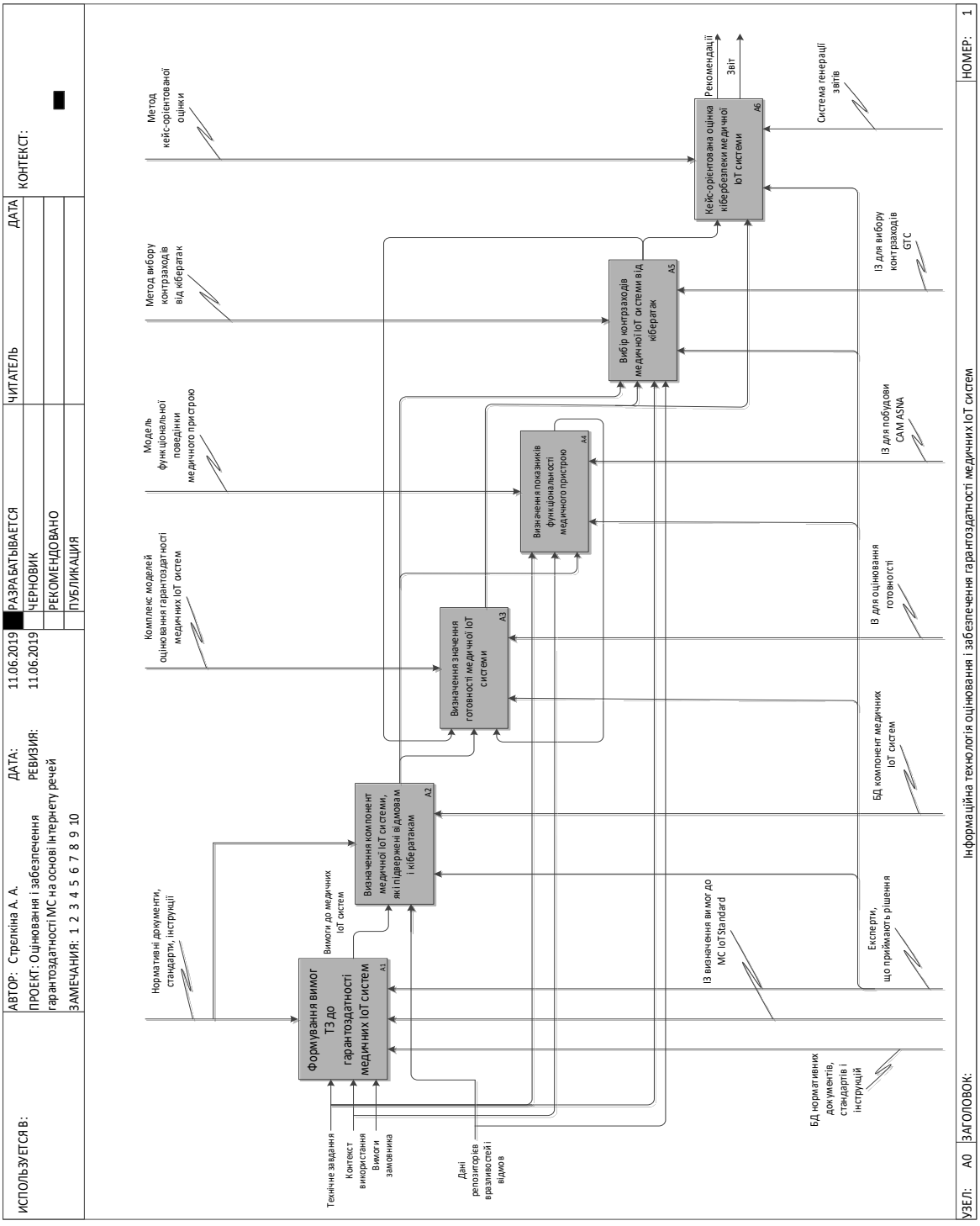

Рис. 2. IDEF0-діаграма інформаційної технології оцінки
та забезпечення гарантоздатності МС на основі Інтернету речей

3. Global report on diabetes // World Healthcare Organization. – 2016. – 88 c.

4. Mohan, A. Cyber Security for Personal Medical Devices Internet of Things [Text] / A. Mohan. // 2014 IEEE International Conference on Distributed Computing in Sensor System. – 2014. – P. 372–374.

5. The Internet of Things for Health Care: A Comprehensive Survey [Text] / S. Islam, D. Kwak, M. Kabir et al. // IEEE Access. – 2015. – Vol. 3. – P. 678-708.

6. Maksimovic, M. A custom Internet of Things healthcare system [Text] / M. Maksimovic, V. Vujovic, B. Perisic // 10th Iberian Conference on Information Systems and Technologies (CISTI). – 2015. – P. 1–6.

7. MAUDE - Manufacturer and User Facility Device Experience [Електронний ресурс] // Accessdata.fda.gov. – 2019. – Режим доступу: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/search.CFM. – 26.08.2019.

8. The internet of things in healthcare: An overview [Text] / Y. Yin, Y. Zeng, X. Chen et al. // Journal of Industrial Information Integration. – 2016. – Vol. 1. – P. 3-13.

9. A survey on facilities for experimental internet of things research [Text] / A. Gluhak, S. Krco, M. Nati et al. // Communications Magazine. – 2011. – Vol. 49, no. 11. – P. 58–67.

10. Dependability for the Internet of Things-from dependable networking in harsh environments to a holistic view on dependability [Text] / C. A. Boano, K. Römer, R. Bloem et al. // Elektrotechnik Und Informationstechnik. – 2016. – Vol. 133(7). – P. 304–309.

11. Strielkina, A. Availability models for healthcare IoT systems: Classification and research considering attacks on vulnerabilities [Text] / A. Strielkina, V. Kharchenko, D. Uzun // 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). – 2018. – P. 58-62.

12. Strielkina, A. A Markov Model of Healthcare Internet of Things System Considering Failures of Components [Text] / A. Strielkina, V. Kharchenko, D. Uzun // 2018 Conference ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. – 2018. – 14 p.

13. Strielkina, A. Model of Functional Behavior of Healthcare Internet of Things Device [Text] / A. Strielkina, B. Volochiy, V. Kharchenko // 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT). – 2019. – P. 63-69.

14. Strielkina, A. Availability Models of the Healthcare Internet of Things System Taking into Account Countermeasures Selection [Text] / A. Strielkina, V. Kharchenko, D. Uzun // Information and Communication Technologies in Education, Research, and Industrial Applications, 2019. – P. 220-242.

15. Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment [Text] / A. Strielkina, O. Illiashenko, M. Zhydenko et al. // 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). – 2019. – P. 67-73.

References

1. BI Intelligence. *The global market for IoT healthcare tech will top $400 billion in 2022*. Available at: www.businessinsider.com/the-global-market-for-iot-healthcare-tech-will-top-400-billion-in-2022-2016-5 (accessed 26 August 2019).

2. GMDN Agency. *User Guide*. Available at: http://www.gmdnagency.com/ (accessed 26 August 2019).

3. Global report on diabetes. *World Healthcare Organization*, 2016. 88 p.

4. Mohan, A. Cyber Security for Personal Medical Devices Internet of Things. *2014 IEEE International Conference on Distributed Computing in Sensor System*, 2014, pp. 372–374.

5. Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain M., Kwak K. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, 2015, vol. 3, pp. 678-708.

6. Maksimovic, M. Vujovic V., Perisic, B. A custom Internet of Things healthcare system. *10th Iberian Conference on Information Systems and Technologies (CISTI)*, 2015, pp. 1–6.

7. Accessdata.fda.gov. *MAUDE - Manufacturer and User Facility Device Experience*. Available at: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/search.CFM (accessed 26 August 2019).

8. Yin, Y., Zeng, Y., Chen, X., Fan, Y. The internet of things in healthcare: An overview. *Journal of Industrial Information Integration*. 2016, vol. 1, pp. 3-13.

9. Gluhak, A., Krco, S., Nati, M., Pfisterer, D., Mitton, N., Razafindralambo, T. A survey on facilities for experimental internet of things research. *Communications Magazine*, 2011, vol. 49, no. 11, pp. 58–67.

10. Boano, C. A., Römer, K., Bloem, R., Witrisal, K., Baunach, M., Horn. M. Dependability for the Internet of Things—from dependable networking in harsh envi-ronments to a holistic view on dependability. *Elektrotechnik Und Informationstechnik*, 2016, vol. 133(7), pp. 304–309.

11. Strielkina, A., Kharchenko, V., Uzun, D. Availability models for healthcare IoT systems: Classification and research considering at-tacks on vulnerabilities. *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2018, pp. 58-62.

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

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

14. Strielkina, A., Kharchenko, V., Uzun, D. Availability Models of the Healthcare Internet of Things System Taking into Account Countermeasures Selection. *Information and Communication Technologies in Education, Research, and Industrial Applications*, 2019, pp. 220-242.

15. Strielkina, A., Illiashenko, O., Zhydenko, M., Uzun, D. Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment. *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2019, pp. 67-73.

Надійшла до редакції 1.09.2019, розглянута на редколегії 23.09.2019

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ОЦЕНКИ И ОБЕСПЕЧЕНИЯ ГАРАНТОСПОСОБНОСТИ МЕДИЦИНСКИХ IoT СИСТЕМ

А. А. Стрелкина

Медицинские системы, функционирующие в среде Интернета вещей, приобретают все большее распространение и, по предварительным прогнозам, их влияние будет только увеличиваться. Однако новые концепции и применения современных технологий несет определенные риски, включая отказа конечных пользовательских устройств, инфраструктуры, что, в свою очередь, может привести к летальному исходу. В связи с этим проблемы оценки и обеспечения гарантоспособности при использовании этой технологии увеличиваются. *Объектом* исследования и анализа в данной работе является медицинская система, функционирующая в среде Интернета вещей. *Целью* исследования данной работы является описание и разработка структуры и функциональной схемы информационной технологии (ИТ) оценки и обеспечения гарантоспособности медицинских систем на основе Интернета вещей, которая базируется на моделях, методах и процедурах оценки и обеспечения гарантоспособности и формализованных методах проектирования, которые содержат следующие этапы синтеза проектных решений: выбор модели, выбор метода, решение задачи и принятия решений. Процесс создания информационной технологии состоит из таких этапов, как определение: основных процессов, происходящих при оценке и обеспечении гарантоспособности медицинских IoT систем; входных данных; исходных данных; элементов механизмов; элементов управления. Разработана структура информационной технологии, которая состоит из следующих процессов: формирование требований к гарантоспособности медицинских систем на основе Интернета вещей; определения компонент медицинских IoT систем, подвергнуты отказам и кибератакам; определения показателей готовности медицинских IoT систем; определение показателей функциональности медицинских устройств; выбор контрмер защиты медицинской IoT системы от кибератак; кейс-ориентированное оценивание кибербезопасности медицинских систем, функционирующих в среде Интернета вещей. Как результат, в данной работе приведена IDEF0-диаграмма информационной технологии оценки и обеспечения гарантоспособности медицинских IoT систем. А также представлены основные этапы реализации разработанной информационной технологии.

Ключевые слова: IDEF0; гарантоспособность; инсулиновая помпа; Интернет вещей; информационная технология; медицинская система.

INFORMATION TECHNOLOGY FOR DEPENDABILITY ASSESSMENT AND PROVIDING OF HEALTHCARE IoT SYSTEMS

A. Strielkina

Healthcare systems operating in the Internet of things are becoming more widespread and their impact is predicted to only increase. However, new concepts and applications of the latest technologies carry some risks, including the failure of end-user devices, infrastructure, which in turn can lead to the worst outcome. In this regard, the problems of evaluation and assurance when using this technology are increasing. The object of research and analysis in this work is a medical system that operates on the Internet of Things. The purpose of this study is to describe and develop the structure and functional scheme of information technology (IT) dependability assessment and providing of healthcare systems based on the Internet of Things, which is based on models, methods and procedures for evaluation and assurance and formalized design methods that contain such stages of synthesis design decisions: model selection, method selection, problem solving and decision making. The process of the information technology creating consists of such steps as determining: the basic processes that occur when evaluating and ensuring the security of medical IoT systems; input data; source data; elements of mechanisms; controls. The developed structure of information technology consists of the following processes: formation of requirements for the warranty of medical IoT systems; identifying components of medical IoT systems that are susceptible to failure and cyberattack; determination of indicators of availability of medical IoT systems; definition of indicators of functionality of healthcare devices; selection of countermeasures to protect the healthcare IoT system against cyberattacks; case-oriented assessment of cybersecurity of healthcare IoT systems. As a result, this paper provides an IDEF0 diagram of the information technology of dependability assessment and providing healthcare systems based on the Internet of Things. The basic stages of the implementation of the developed information technology are also presented.

Keywords: IDEF0; dependability; insulin pump; Internet of Things; healthcare system.

Стрєлкіна Анастасія Андріївна – аспірантка, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Strielkina Anastasiia – PhD student, assistant lecturer of Computer Systems, Networks and Cybersecurity department, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: a.strielkina@csn.khai.edu, ORCID Author ID: 0000-0002-7760-7367, Scopus Author ID: 57194779158.