УДК 004.7:056.5

А. А. СТРЄЛКІНА, Д. Д. УЗУН

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

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ МЕДИЧНИХ СИСТЕМ: ВИКЛИКИ І РІШЕННЯ В КОНТЕКСТІ ІНТЕРНЕТУ РЕЧЕЙ

В даній статті розглядаються основні виклики і рішення в області кібербезпеки медичних систем в контексті Інтернету речей. Авторами виявлено основні вразливості, загрози та ризики мережевих медичних пристроїв. В роботі в загальних рисах описуються основні регламентуючі документи в області забезпечення кібербезпеки, а саме, правила конфіденційності і безпеки HIPAA, вимоги кібербезпеки FDA до і після виходу медичного пристрою на ринок. За результатами дослідження авторами були систематизовані основні напрями забезпечення кібербезпеки медичних пристроїв в контексті Інтернету речей.

Ключові слова: *загрози безпеки, Інтернет речей, кібербезпека, медичні системи, HIPAA, FDA.*

Вступ

Інтернет речей є однією з найпопулярніших і передових технологій за останній час. Можливість впровадження в різні сфери життя дає переваги в цих сферах, і темпи цього грандіозні. За попередніми прогнозами важливість і розповсюдженість Інтернету речей буде зростати [1].

Роберт Пеппер [2] пише: «Інтернет речей – одна з визначальних технологій нашого часу, що перетворює все навколо. Ми можемо змінити на краще життя мільйонів і навіть мільярдів людей в країнах, що розвиваються і запобігти появі чергового цифрового бар'єру».

Одним з найважливіших напрямків, де сучасні технології можуть принести помітну користь суспільству, є охорона здоров'я.

Мережеві медичні пристрої вже набувають все більшого поширення і за попередніми прогнозами до 2022 року їх ринок буде близько 410 мільярдів доларів [3].

Згідно з [4] медичний пристрій – це «інструмент, апарат, прилад, винахід, імплантант, In vitro реагент або інший аналогічний чи споріднений предмет, в тому числі складова частина або додаток, який:

– визначається в офіціальному Національному формулярі, або в Фармакопеї США, або в будь-якому доповненні до цих документів;

– призначено для використання в діагностуванні захворювань або інших станів, або лікування, послаблення, проведення процедур або профілактики захворювань людини або тварин;

– призначено для впливу на структуру або будь-яку іншу частину тіла людини або тварини, і який не досягає своєї первинної призначеної мети через хімічну реакцію всередині або на тілі людини або тварини, і який не залежить від виконання своєї первинної призначеної мети».

Інтернет речей значно поліпшує систему охорони здоров'я. А саме:

– легше отримувати, аналізувати і ділитися даними про здоров'я пацієнта;

– персоналізоване лікування може бути надано на більш детальному рівні;

– індивідуальні пристрої можуть підключатися і взаємодіяти з усією системою охорони здоров'я, тощо.

У звіті Атлантичної ради США 2015 року [5] виділяється чотири основні типи мережевих медичних пристроїв:

– імплантовані, внутрішні;

– для носіння, зовнішні;

– стаціонарні;

– споживацькі для моніторингу здоров'я.

До імплантованих відносяться кардіостимулятори та інші пристрої, які вживлені у пацієнта, але взаємодіють з іншими пристроями за допомогою бездротових інтерфейсів через звичайні пропрієтарні бездротові протоколи або Bluetooth.

Зовнішні для носіння пристрої включають в себе портативні інсулінові помпи, які використовують пропрієтарні протоколи зв'язку.

Стаціонарні медичні пристрої, наприклад, лікарняні станції дозування хіміотерапії, системи кардіомоніторингу для домашнього нагляду за лежачими хворими, зазвичай використовують традиційні бездротові мережі, як Wi-Fi мережі, у лікарнях або домах пацієнтів.

Споживацькі пристрої для моніторингу здо-

ров'я, як FitBit, Nile FuelBand або Withings, зазвичай взаємодіють через Bluetooth з прив'язаними мобільними пристроями. Ці пристрої іноді не відносять до медичних, бо для їх виробництва та використання не потрібне схвалення регулюючих органів.

Мережеві медичні пристрої зазвичай поєднуються у мережу, яка включає в себе пацієнтів, організації охорони здоров'я, лікарів та інших. В більшості випадків, їх взаємодія потребує бездротового та багаторазового зв'язку, який включає розповсюдження клінічних даних та контролювання стану пристрою.

Актуалізацію існуючої загальної архітектури медичної системи згідно з роботою [6] представлено на рис. 1.

Медичний пристрій взаємодіє за допомогою бездротового інтерфейсу зі зчитувачем. Зчитувач призначений для зчитування звітів, контролювання стану, зміни параметрів та оновлення вбудованого програмного забезпечення пристрою. Цей зчитувач через точку доступу (або модем, або маршрутизатор) завантажує зняті показання до сервісу у хмарі. В екстрених ситуаціях медичний пристрій має змогу напряму підключатися до публічної точки доступу, щоб передати дані.

Хмарний сервіс зберігає дані в базі даних особистих записах здоров'я (ОЗЗ). До цієї бази даних можуть отримати доступ лікарні, лікарі невідкладної допомоги та лікуючи лікарі. Хмарний сервіс надає веб-інтерфейс пацієнту, щоб той визначив політику доступу до своїх даних, отриманих з медичного пристрою, у ОЗЗ базі. Детальний опис інтеграції даних з медичного пристрою до хмарної бази даних ОЗЗ представлено в роботі [7].

В роботах [8-9] дослідниками описано та продемонстровано те, що мережеві медичні пристрої вразливі до різних типів атак, що ставлять під загрозу як фізичну, так і кібербезпеку, конфіденційність пацієнта. В [10] автором запропоновано за його ж думкою «нерозважливе» рішення – зловмисники повинні опублікувати конфіденційну інформацію про стан здоров'я пацієнтів, що спонукає виробників виготовляти більш безпечні пристрої.

Таким чином, **метою** даної роботи є аналіз проблем і рішень у забезпеченні кібербезпеки медичних систем в контексті Інтернету речей.

1. Вразливості, загрози та ризики кібербезпеки використання мережевих медичних систем

Мережеві медичні системи вже неодноразово підвергалися кіберзагрозам. Одним з найгучніших був випадок продемонстрований на конференції Black Hat у 2011 році, коли дослідник інформаційної безпеки Джей Редкліф на власній інсуліновій помпі показав, як легко її можна скомпрометувати, знаючи лише ідентифікаційний номер пристрою [11].

Мережевим медичним системам притаманні наступні вразливості:

– незахищені канали зв'язку;
– неповноцінні механізми аутентифікації;
– неповноцінний контроль доступу;
– вразливості програмного забезпечення;
– слабкі механізми аудиту;
– обмежені накопичувачі;
– незадовільні сповіщення тощо.

Таким чином, при використанні мережевих медичних пристроїв виникають такі загрози:

– вилучення даних пацієнта;
– фальсифікації даних пацієнта;
– перепрограмування пристрою;
– багаторазові спроби доступу;
– вимкнення пристрою;
– зміни призначеного лікування;
– зловмисне надання даних;
– переповнення пам'яті тощо.

За нез'ясованих вразливостях і загрозах можуть виникнути ризики:

– безпеки здоров'я пацієнта;
– втрати конфіденційності пацієнта;
– неприпустимого лікарського контролю;
– непрацездатності пристрою тощо.

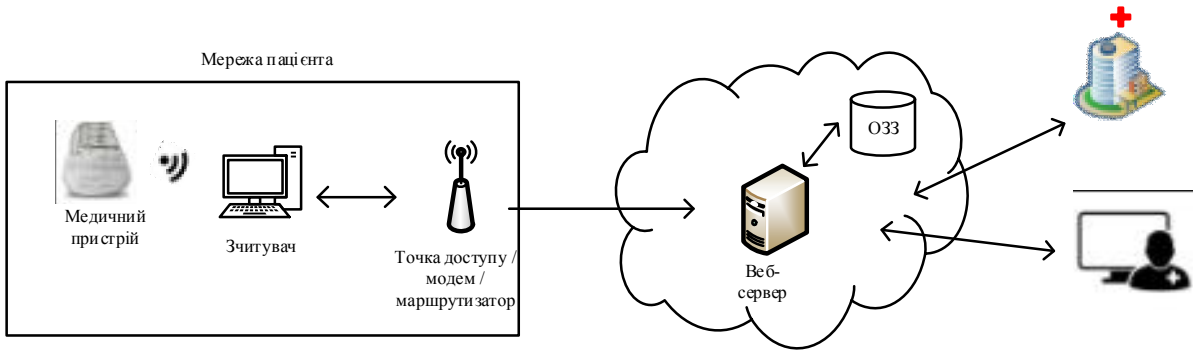

Рис. 1. Архітектура медичної системи в контексті Інтернету речей

До ризиків безпеки здоров'я пацієнта відносяться збої вбудованого програмного забезпечення, зловмисні оновлення призначеного лікування тощо. Під ризиком втрати конфіденційності мається на увазі витік даних з пристрою. Ризиком неприпустимого лікарського контролю є несанкціоноване зчитування і керування даними пацієнта. Мережевий медичний пристрій може утратити свою працездатність через, наприклад, повний розряд батареї, переповнення пам'яті тощо.

2. Регламентуючі документи кібербезпеки медичних систем

Вимоги до кібербезпеки медичних пристроїв в основному регламентуються федеральним законом США «Про відповідальність і перенесення даних про страхування здоров'я громадян» і Управлінням продовольства і медикаментів (англ. Food and Drug Administration, FDA).

Поясненням до федерального закону США «Про відповідальність і перенесення даних про страхування здоров'я громадян» (англ. Health Insurance Portability and Accountability Act, HIPAA) є правила конфіденційності [12] і безпеки [13].

Під дію документів HIPAA попадають медичні організації, такі як медичні заклади, страхові компанії, центри медичних розрахунків. Основним завданням цього нормативного акту є захист персональних даних пацієнтів, заборона розголошення лікарської таємниці і покарання винних у разі умисного чи ні порушення певних правил.

Згідно [12] правило конфіденційності забезпечує федеральний захист персональної інформації, що використовується медичними організаціями, і надає пацієнтам сукупність прав щодо цієї інформації, а також дозволяє розкривати персональну інформацію про здоров'я, необхідну для лікування пацієнтів та використання в інших важливих цілях. Предметом захисту є персональні медичні дані пацієнта, які включають в себе:

– інформацію про фізичне та психічне здоров'я пацієнта;

– історію його звернень до медичних установ;

– фінансову інформацію щодо медичних послуг;

– особисті дані пацієнта, за допомогою яких можна будь-яким чином ідентифікувати особистість пацієнта.

Правило безпеки «визначає ряд адміністративних, фізичних і технічних заходів, які повинні виконувати медичні організації для забезпечення конфіденційності, цілісності та доступності до електронної інформації про здоров'я» [13].

Правило безпеки вимагає, щоб медичні заклади, які зберігають або передають дані в цифровій формі, приймали відповідні заходи захисту адміністративного, технічного та фізичного характеру:

– для забезпечення цілісності і конфіденційності інформації о пацієнтах;

– для відображення будь-яких загроз, спрямованих на дані;

– для попередження несанкціонованого доступу до даних, що захищаються;

– для загального контролю дотримання вимог правил службовцями.

Підтримка відповідності вимог до правил HIPAA є безперервним процесом, який надає можливість забезпечити усесторонню безпеку даних організації, проводячи періодичні оцінки ризиків. Невиконання вимог вищеописаних правил веде до ризиків штрафів, в'язниці та судових процесів.

Центр приладів і радіологічного здоров'я (англ. Center for Devices and Radiological Health, CDHR), який є філіалом FDA, відповідає за передмаркетингове затвердження усіх медичних пристроїв, а також за нагляд за виготовленням, продуктивністю і безпекою цих пристроїв. Управління продовольства і медикаментів вимагає, щоб виробники приладів забезпечували безпеку своєї продукції як на етапі розроблення, так і протягом терміну обслуговування цих пристроїв. З цією метою було випущено три документа: «Guidance for Industry: «Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software» (2005) [14], «Premarket Submissions for Management of Cybersecurity in Medical Devices» (2014) [15], «Postmarket Management of Cybersecurity in Medical Devices» (2016) [16].

У документі «Premarket Submissions for Management of Cybersecurity in Medical Devices» FDA рекомендує виробникам обладнання розробити набір керуючих документів для зменшення ймовірності компрометації функціональних можливостей через неповноцінне забезпечення безпеки і з метою підтримки цілісності функціональності медичних пристроїв і функціональної безпеки. FDA радить виробникам обладнання розглядати:

– ідентифікацію активів, загроз і вразливостей;

– оцінювання впливу загроз і вразливостей на пристрій і кінцевих споживачів;

– оцінювання ймовірностей виникнення загроз і вразливостей;

– визначення рівнів ризиків і можливих стратегій зменшення впливу;

– оцінювання остаточного ризику і критеріїв прийняття ризиків.

Документ «Postmarket Management of Cybersecurity in Medical Devices» наполегливо рекомендує продовжувати контроль, виявлення і усу-

нення потенційних ризиків кібербезпеки після випуску пристрою на ринок. FDA рекомендує виробникам використовувати NIST Framework для управління ризиками, а також інструмент для вразливостей кібербезпеки, який оцінює такі фактори, як:

– вектор атаки;
– складність атаки;
– обов'язкові привілеї;
– взаємодію з користувачем;
– масштаб;
– вплив на конфіденційність;
– вплив на цілісність;
– вплив на доступність;
– рівень виправлень;
– довіра;
– впевненість у звіті.

Цей документ передбачає, що виробники проводять моделювання загроз і аналіз каналів і джерел можливих загроз, що оптимізує безпеку мережі, застосунків і Інтернету шляхом вияву потенційних і можливих вразливостей і розроблення заходів протидії.

В таблиці 1 представлено основні вимоги документів, розроблених FDA.

Окрім того, FDA радить виробникам медичних пристроїв розробляти комплексні програми ризик-менеджменту в сфері кібербезпеки, замість того, щоб реактивно реагувати і усувати недоліки пристрою тільки після того, як вони завдали шкоди комп'ютерним мережам системи охорони здоров'я.

3. Напрямки забезпечення кібербезпеки медичних систем

Напрямки забезпечення кібербезпеки медичних систем в контексті Інтернету речей складаються, але не обмежується такими складовими:

1. *Забезпечення доступності і готовності*. За своєю конструкцією медичні пристрої є ресурсообмеженими, мають обмежене апаратне забезпечення з батареями, строк служби яких становить кілька років. Тобто, будь-яка марнотратна операція забирає час автономної роботи пристрою. У зв'язку з чим необхідно використовувати легковагову криптографію. Для комунікацій необхідно використовувати такі технології з низьким енергоспоживанням, як ZigBee, Bluetooth v4.0.

2. *Механізми управління доступом*. Ці механізми потрібні для того, щоб гарантувати, що до медичної системи входять довірені пристрої і, що ці пристрої можуть довіряти брокеру чи застосунку, що надсилає керуючі команди. Автентифікація може бути по ідентифікатору користувач /паролю, по одноразовому паролю (OTP), по унікальному ідентифікатору серверу, корисному навантаженню повідомлень тощо. Відсутність безпечної автентифікації наражає пристрій на велику різноманітність атак, наприклад, атаку на відмову в обслуговуванні, що призведе до розрядження батареї пристрою шляхом беззмістовних операцій.

Таблиця 1

Основні вимоги документів FDA

Pre-Market Guidance (2014) [15]		Post-Market Guidance (2016) [16]	
Доступність	Дані доступні в разі потреби	Структурований системний підхід до кіберризиків і систем управління якістю	Розробка програмного, цілісного, поточного підходу з комплексною командою для оцінки ризиків кібербезпеки і питань якості
Цілісність	Дані є точними і повними	Управління вразливостями, продуктивність пристрою і критерій прийняття ризиків	Регулярна оцінка вразливостей для визначення продуктивності пристроїв, якщо вони були скомпрометовані, наряду з узгодженими критеріями прийняття ризиків
Конфіденційність	Дані захищені та доступні тільки уповноваженим особам	Безперервний процес виявлення, зменшення та усунення ризиків кібербезпеки	Програма оцінки ризиків наряду з критеріями прийняття ризиків для постійного оцінювання медичних пристроїв протягом усього життєвого циклу
Кібербезпека	Потрібно враховувати питання кібербезпеки від стадії концепції та розробки до кінця життєвого циклу	Управління вразливостями, прийняття ризику, критерій впливу на здоров'я і тяжкості	Документування впливу вразливостей на медичний пристрій і здоров'я пацієнта

3. *Відповідність моделі OSI*. У мережах фізичних об'єктів взаємодії між компонентами здійснюється за допомогою протоколів прикладного рівня: CoAP, MQTT, XMPP, AMQP, JMS, REST/HTTP тощо. Протокол CoAP (Constrained Application Protocol) – обмежений протокол передачі даних, аналогічний HTTP, але адаптований для роботи з "розумними" пристроями низької продуктивності. Протоколи MQTT, XMPP, AMQP, JMS - ці протоколи обміну повідомленнями, які засновано на брокері за схемою: publish / subscribe (публікація / підписка).

4. *Відповідність вимогам безпеки регламентуючих документів.* Окрім вищеописаних документів, існують ще інші керуючи документи в області кібербезпеки медичних пристроїв. Повне дотримання вимог і рекомендацій таких документів дозволить значно підвищити рівень кібербезпеки і протистояти можливим загрозам.

5. *Проведення періодичного моніторингу і управління безпекою.* Контроль безпеки медичних виробів може включати в себе збір інформації, розслідування небажаних реакцій, активне виявлення, вивчення і попередження проблем безпеки, які можуть виникнути під час використання пристроїв (управління ризиками).

6. *Вимоги щодо кваліфікації обслуговуючого персоналу*. Для цього необхідно проводити регулярні різноманітні тренінги, наради, консультації з експертами в області кібербезпеки для усіх співробітників.

Висновки

У даній статті розглянуто основні виклики і рішення в області кібербезпеки медичних систем в контексті Інтернету речей.

В статі описано основні вразливості, загрози та ризики використання мережевих медичних пристроїв, а також представлено основні регламентуючі документи в цій області, надано процес забезпечення кібербезпеки медичних систем.

Атаки на медичні пристрої компрометують користувацькі дані, і, якщо зловмисник отримає доступ до застосунків і пристроїв діагностування, до апаратів, які регулюють дозування ліків, або до систем життєзабезпечення, то це може привести до критичних наслідків. На щастя, досі не відбулося жодної зловмисної атаки на такі пристрої, які призвели до людських жертв. Проте медична галузь є найбільш вразливою з точки зору забезпечення кібербезпеки.

Таким чином, можливості забезпечення кібербезпеки медичних пристроїв в сфері Інтернету речей залежать від виконання чи дотримання як медичними організаціями, так і розробниками і користувачами вищеописаних напрямків забезпечення кібербезпеки медичних пристроїв.

Напрямком подальших досліджень є більш детальне вивчення технологій, протоколів, регламентуючих документів в області кібербезпеки мережевих медичних пристроїв, а також дослідження питань приватності.

Література

1. The Internet of Things. How the Next Evolution of the Internet Is Changing Everthing [Electronic resource] / Cisco Internet Business Solutions Group. – Access mode: http://www.cisco.com/c/dam/en_us/about /ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. – 26.12.2016.

2. Pepper, R. IoT: Using Technology for the Developing World [Electronic resource] / R. Pepper. – Access mode: http://blogs.cisco.com/gov/iot-using-technology-for-the-developing-world. – 26.12.2016.

3. The global market for IoT healthcare tech will top $400 billion in 2022 [Electronic resource] / BI Intelligence. – Access mode: www.businessinsider.com/ the-global-market-for-iot-healthcare-tech-will-top-400-billion-in-2022-2016-5. – 26.12.2016.

4. What is a medical device? [Electronic resource] / U.S. Department of Health and Human Services. – Access mode: http://www.fda.gov/AboutFDA/ Transparency/Basics/ucm211822.htm. – 26.12.2016.

5. Healey, J. The healthcare Internet of things: rewards and risks [Electronic resource] / J. Healey, N. Pollard, B. Woods. – Access mode: http://www. mcafee.com/es/resources/reports/rp-healthcare-iot-rewards-risks.pdf. – 20.12.2016.

6. Mohan, A. Cyber Security for Personal Medical Devices Internet of Things [Text] / A. Mohan // 2014 IEEE International Conference on Distributed Computing in Sensor Systems, 26-28 May 2014. – IEEE, 2014. – P. 372-374.

7. A Patient-centric, Attribute-based, Source-verifiable Framework for Health Record Sharing [Text] / A. Mohan, D. Bauer, D.M. Blough [et. al.] // GIT CERCS Technical Report GIT-CERCS-09-11. – Georgia Institute of Technologies, 2009. – 10 p.

8. MW is Short St. Jude Medical (STJ:US) [Electronic resource] / St. Jude Medical, Inc. – Access mode: http://www.muddywatersresearch.com/research. – 26.12.2016.

9. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses [Text] / D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark [et. al.] // 2008 IEEE Symposium on Security and Privacy, 18-20 May 2008. – IEEE, 2008. – P. 129. – 142 DOI: 10.1109/SP.2008.31.

10. Донохью, Б. Взламывая людей [Електронний ресурс] / Б. Донохью. – Режим доступу: https://blog.kaspersky.ru/vzlamyvaya-lyudej/1530/. – 03.01.2017.

11. Radcliffe, J. Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System [Electronic resource] / J. Radcliffe. – Access mode: https://media.blackhat.com/bh-us-11/Radcliffe/ BH_US_11_Radcliffe_Hacking_Medical_Devices_Slides.pdf. – 28.12.2016.

12. The HIPAA Privacy Rule [Electronic resource] / U.S. Department of Health & Human Services. – Access mode: http://www.hhs.gov/hipaa/ for-professionals/privacy/ – 28.12.2016.

13. The Security Rule [Electronic resource] / U.S. Department of Health & Human Services. – Access mode: http://www.hhs.gov/hipaa/for-professionals/ security/ – 28.12.2016.

14. Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software [Electronic resource] / U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health. – Access mode: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm. – 29.12.2016.

15. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices [Electronic resource] / U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health. – Access mode: http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ ucm356190.pdf. – 29.12.2016.

16. Postmarket Management of Cybersecurity in Medical Devices [Electronic resource] / U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health. – Access mode: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf. – 29.12.2016.

References

1. Cisco Internet Business Solutions Group. *The Internet of Things. How the Next Evolution of the Internet Is Changing Everthing*. Available at: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (accessed 26 December 2016).

2. Pepper, R. *IoT: Using Technology for the Developing World*. Available at: http://blogs.cisco.com/gov/iot-using-technology-for-the-developing-world (accessed 26 December 2016).

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

4. U.S. Department of Health and Human Services. *What is a medical device?* Available at: http://www.fda.gov/AboutFDA/Transparency/Basics/ucm211822.htm (accessed 26 December 2016).

5. Healey, J., Pollard, N. and Woods, B. *The healthcare Internet of things: rewards and risks*. Available at: http://www.mcafee.com/es/resources/reports/rp-healthcare-iot-rewards-risks.pdf (accessed 20 December 2016).

6. Mohan, A. Cyber Security for Personal Medical Devices Internet of Things. *Proceedings of* the *IEEE International Conference on Distributed Computing in Sensor Systems,* 26-28 May, 2014, pp. 372-374.

7. Mohan, A., Bauer, D., Blough, D., Ahamad, M., Bamba, B., Krishnan, R., Liu, L., Mashima, D., Palanisamy, B. A Patient-centric, Attribute-based, Source-verifiable Frameworkfor Health Record Sharing. *GIT CERCS Technical Report GIT-CERCS-09-11*, Georgia Institute of Technology, 2009, 10 p.

8. St. Jude Medical, Inc. *MW is Short St. Jude Medical (STJ:US)*. Available at: http://www.muddywatersresearch.com/research (accessed 26 December 2016).

9. Halperin, D., Heydt-Benjamin, T., Ransford, B., Clark, S., Defend, B., Morgan, W., Fu, K., Kohno, T., Haisel, W. Pacemakers and Implantable Cardiac Defibrillators:Software Radio Attacks and Zero-Power Defenses. *Proceedings of* the *IEEE Symposium on Security and Privacy,* 18-20 May, 2008, pp. 129-142. doi: 10.1109/SP.2008.31.

10. Donohue, B. *Vzlamyvaya lyudey* [Hacking people]. Available at: https://blog.kaspersky.ru/vzlamyvaya-lyudej/1530/ (accessed 03 January 2017). (In Russian).

11. Radcliffe, J. *Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System*, 2011. Available at: https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_Slides.pdf (accessed 28 December 2016).

12. U.S. Department of Health & Human Services. *The HIPAA Privacy Rule*. Available at: www.hhs.gov/hipaa/for-professionals/privacy/ (accessed 28 December 2016).

13. U.S. Department of Health & Human Services. *The Security Rule*. Available at: http://www.hhs.gov/hipaa/for-professionals/security/ (accessed 28 December 2016).

14. U.S. Department of Health and Human Services, Food and Drug Administration and Center for Devices and Radiological Health. *Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software* . Available at: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm (accessed 29 December 2016).

15. U.S. Department of Health and Human Services, Food and Drug Administration and Center for Devices and Radiological Health. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*. Available at: http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf (accessed 29 December 2016).

16. U.S. Department of Health and Human Services, Food and Drug Administration and Center for Devices and Radiological Health. *Postmarket Management of Cybersecurity in Medical Devices*.– Available at: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf (accessed 29 December 2016).

Надійшла до редакції 25.01.2017, розглянута на редколегії 16.02.2017

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ МЕДИЦИНСКИХ СИСТЕМ: ВЫЗОВЫ И РЕШЕНИЯ В КОНТЕКСТЕ ИНТЕРНЕТА ВЕЩЕЙ

А. А. Стрелкина, Д. Д. Узун

В данной статье рассматриваются основные вызовы и решения в области кибербезопасности медицинских систем в контексте Интернета вещей. Авторами выявлены основные уязвимости, угрозы и риски сетевых медицинских устройств. В работе в общих чертах описываются основные регламентирующие документы в области обеспечения кибербезопасности, а именно, правила конфиденциальности и безопасности HIPAA, требования кибербезопасности FDA до и после выхода медицинского оборудования на рынок. По результатам исследования авторами были систематизированы основные направления обеспечения кибербезопасности медицинских устройств в контексте Интернета вещей.

Ключевые слова: угрозы безопасности; Интернет вещей; кибербезопасность; медицинские системы; HIPAA; FDA.

CYBERSECURITY OF MEDICAL SYSTEMS: CHALLENGES AND SOLUTIONS IN THE CONTEXT OF THE INTERNET OF THINGS

A. A. Strielkina, D. D. Uzun

This article reviews the main challenges and solutions in the field of cybersecurity medical systems in the context of the Internet of things. The authors identified key vulnerabilities, threats and risks of health care network devices. The paper describes in general terms the main regulatory documents in the field of cybersecurity providing, such as HIPAA privacy and security rules, FDA requirements for cybersecurity for pre- and post-market of the medical devices. Using the results of research authors systematized basic directions in providing cyber security of medical devices in the context of Internet of things.

Key words: cybersecurity threats; Internet of things, cybersecurity; medical systems; HIPAA; FDA.

Стрєлкіна Анастасія Андріївна – аспірант кафедри комп'ютерних систем та мереж, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Харків, Україна, e-mail: a.strielkina@csn.khai.edu.

Узун Дмитро Дмитрович – канд. техн. наук, доцент, доцент кафедри комп'ютерних систем та мереж, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Харків, Україна, e-mail: d.uzun@csn.khai.edu.

Strielkina Anastasiia Andriivna – postgraduate student of Computer Systems and Networks department, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: a.strielkina@csn.khai.edu.

Uzun Dmytro Dmytrovych – candidate of technical sciences, Assistant Professor, Computer Systems and Networks department, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: d.uzun@csn.khai.edu.