

Information security in IoT medical devices and their impact on patient health

Vinnitsia National Technical University

Анотація

Розвиток Інтернету речей (IoT) у медичній галузі відкриває нові можливості для моніторингу стану здоров'я пацієнтів та надання якісної медичної допомоги. Однак, паралельно з цим з'являються і нові виклики, пов'язані з інформаційною безпекою та конфіденційністю даних пацієнтів. У дослідженні розглядаються можливі загрози інформаційній безпеці при використанні медичних пристроїв IoT, а також потенційний вплив на здоров'я пацієнтів. Аналізуються такі аспекти, як захист конфіденційних даних, кібербезпека, безпека зв'язку між пристроями та ризики для фізичної безпеки пацієнтів у разі зламу системи. Вивчаються існуючі стандарти безпеки та пропонуються рекомендації щодо покращення безпеки медичних IoT-систем.

Ключові слова: Інтернет речей (IoT), медичні пристрої, інформаційна безпека, конфіденційність даних, кібербезпека, безпека пацієнтів.

Abstract

The development of the Internet of Things (IoT) in the medical field opens up new opportunities for monitoring the health status of patients and providing quality medical care. However, in parallel with this, there are new challenges related to information security and confidentiality of patient data. The study examines possible information security threats in the use of IoT medical devices, as well as potential health effects on patients. Aspects such as the protection of confidential data, cybersecurity, security of communication between devices and risks to the physical safety of patients in the event of a system hack are analyzed. It examines existing safety standards and offers recommendations for improving the safety of medical IoT systems.

Keywords: Internet of Things (IoT), medical devices, information security, data privacy, cybersecurity, patient safety.

Introduction

The introduction of the Internet of Things (IoT) in the healthcare industry opens up broad prospects for improving the quality of healthcare services and effectively monitoring patients' health. Connected medical devices, such as fitness trackers, non-contact thermometers, insulin pumps, and implants, allow for the collection, analysis, and transmission of patient data in real time. This helps doctors respond quickly to changes and provide timely care [1-3].

However, despite its advantages, the use of IoT in medicine also carries certain risks and challenges related to information security and patient data confidentiality. Insufficient protection of connected devices can lead to the leakage of sensitive information, breach of confidentiality, or even affect the correct operation of medical systems, which can jeopardize the health and safety of patients.

Research results

Information security in medical IoT devices is critically important, as it is an area that offers many opportunities for improving healthcare, but also carries risks to patient health if data and device protection is not properly managed [4-8]. The study shows that:

1. Threats to information security of medical IoT devices.

One of the main threats to information security when using medical IoT devices is the leakage of confidential patient data. Due to insufficient encryption or vulnerabilities in protection systems, attackers can gain access to personal information, medical history, test results, etc. [9-12]. This not only violates the right to privacy, but can also lead to fraud or use of data for illegal purposes.

In addition, there is a risk of cyberattacks on medical IoT devices and systems. Attackers can attempt unauthorized access, install malicious software, or influence the operation of devices in order to disrupt their correct functioning [13]. This can have critical consequences for the health and lives of patients [14-17].

2. Impact of cybersecurity on the physical safety of patients.

A breach of cybersecurity of medical IoT devices can directly affect the physical safety of patients. For example, if an attacker can gain access to an insulin pump or implant, he can potentially change their settings or operating modes, which can endanger the patient's life [18-21].

In the case of patient monitoring systems, a cyberattack can lead to the receipt of incorrect data, due to which doctors will not be able to timely detect critical changes in the patient's health and take the necessary measures.

3. Analysis of existing security standards.

To date, there are certain standards and requirements for ensuring the security of medical IoT devices, such as HIPAA (Health Insurance Portability and Accountability Act) in the USA and GDPR (General Data Protection Regulation) in the European Union. However, these standards often do not keep up with the rapid development of IoT technologies and require constant updating and improvement.

4. Recommendations for improving security.

To increase the level of information security of medical IoT devices, comprehensive measures must be taken. First, it is important to ensure that data transmitted between devices and storage servers is properly encrypted. Second, reliable authentication and access control methods should be used to prevent unauthorized interference.

In addition, it is necessary to regularly update the software of medical IoT devices to eliminate identified vulnerabilities and respond in a timely manner to potential cybersecurity threats. It is also important to ensure that medical personnel are properly trained in IoT security and adhere to appropriate security protocols [22].

Only with careful planning and implementation of effective security strategies will healthcare institutions be able to fully benefit from IoT technologies, while ensuring the protection of confidential patient information and their physical safety.

Conclusions

Information security plays a critical role in ensuring the effective and safe use of medical IoT devices. Despite the numerous benefits that these innovative technologies provide for improving healthcare, insufficient security can pose a serious threat to the confidentiality of patient data and their health.

As the study shows, there are significant risks of leakage of confidential data, cyberattacks and potential impact on the operation of medical devices themselves due to vulnerabilities in security systems. The consequences of such incidents can be catastrophic, as they can directly threaten the lives and health of patients.

To prevent these risks, it is necessary to comply with existing security standards, such as HIPAA and GDPR, as well as take comprehensive measures to improve the protection of medical IoT systems. This includes the use of strong data encryption, multi-level authentication, regular software updates and proper training of medical personnel.

Research in this area must continue as IoT technologies are rapidly developing and information security threats are constantly evolving. Only by continuously monitoring and improving security systems can we ensure the safe and effective use of medical IoT devices for the benefit of patients.

REFERENCES

1. Лемешев М. С. Основи охорони праці для фахівців менеджменту : навчальний посібник / М. С. Лемешев, О. В. Березюк. – Вінниця : ВНТУ, 2009. – 206 с.
2. Березюк О. В. Удосконалення математичної моделі питомих енерговитрат очищення ґрунтів полігонів твердих побутових відходів від забруднення важкими металами / О. В. Березюк // Матеріали II Міжнародної науково-практичної конференції «Екологічна безпека як основа сталого розвитку суспільства. Європейський досвід і перспективи». – Львів: ЛДУ БЖД, 2015. – С. 185-187.
3. Березюк О. В. Удосконалення математичної моделі концентрацій забруднювальних речовин у фільтраті полігонів твердих побутових відходів / О. В. Березюк // Вісник ВПІ. – 2016. – № 4. – С. 28-31.
4. Ткачук К. Н. Основи охорони праці: підручник / К. Н. Ткачук, В. В. Зацарний, Д. В. Зеркалов, О. І. Полукаров, В. С. Коз'яков, Л. О. Мітюк, Ю. О. Полукаров, Т. Є. Луц. За ред. К. Н. Ткачука. – Київ : Основа, 2014. – 456 с.
5. Березюк О. В. Впровадження практичного заняття «Дослідження забруднення навколишнього середовища твердими побутовими відходами та розрахунок параметрів машин та обладнання для мінімізації негативного впливу на нього» з дисципліни безпека життєдіяльності / О. В. Березюк // Педагогіка безпеки. – 2018. – № 1. – С. 29-36.

6. Березюк О. В. Залежність рівня бактеріологічного забруднення ґрунтів від відстані до полігону твердих побутових відходів / О. В. Березюк, І. М. Климчук, Т. Б. Васенко, С. М. Горбатюк // Наукові праці Вінницького національного технічного університету. – 2021. – № 2. – 6 с. – Режим доступу до журналу: <https://praci.vntu.edu.ua/index.php/praci/article/view/631/593>
7. Березюк О. В. Залежність рівня мікробіологічного забруднення загальними коліформами ґрунтових вод від відстані до полігону твердих побутових відходів / О. В. Березюк, С. С. Хлестова, Н. М. Гринчак, С. М. Горбатюк // Наукові праці Вінницького національного технічного університету. – 2021. – № 3. – 7 с. – Режим доступу до журналу: <https://praci.vntu.edu.ua/index.php/praci/article/view/638/599>
8. Березюк О. В. Вплив наближення до полігону твердих побутових відходів на рівень мікробіологічного забруднення ґрунтових вод за загальним мікробним числом / О. В. Березюк, С. С. Хлестова, І. М. Климчук, Л. Л. Березюк // Наукові праці Вінницького національного технічного університету. – 2023. – № 1. – 7 с. – Режим доступу до журналу: <https://praci.vntu.edu.ua/index.php/praci/article/view/675/639>
9. Голінько В. І. Охорона праці в галузі інформаційних технологій : навч. посіб. / В. І. Голінько, М. Ю. Іконніков, Я. Я. Лебедєв. – Дніпро : НГУ, 2015. – 246 с.
10. Березюк О. В. Регресійна залежність показників захворюваності на хвороби органів дихання від продуктивності сміттєспалювального заводу / О. В. Березюк, Т. Б. Васенко, С. М. Горбатюк, Т. І. Шевчук // Наукові праці Вінницького національного технічного університету. – 2023. – № 1. – 6 с. – Режим доступу до журналу: <https://praci.vntu.edu.ua/index.php/praci/article/view/673/637>
11. Березюк О. В. Залежність показників захворюваності населення працездатного віку на церебральний інсульт від продуктивності сміттєспалювального заводу / О. В. Березюк, С. М. Горбатюк, І. М. Климчук, Т. І. Шевчук // Наукові праці Вінницького національного технічного університету. – 2021. – № 4. – 6 с. – Режим доступу до журналу: <https://praci.vntu.edu.ua/index.php/praci/article/view/641/602>
12. Березюк О. В. Удосконалення математичної моделі впливу викидів дрібнодисперсного пилу на захворюваність хворобами системи кровообігу / О. В. Березюк, Н. М. Гринчак, О. В. Спрут, В. О. Березюк // Наукові праці Вінницького національного технічного університету. – 2023. – № 1. – 7 с. – Режим доступу до журналу: <https://praci.vntu.edu.ua/index.php/praci/article/view/674/638>
13. Закон України "Про охорону праці" від 14.10.1992 № 2694-ХІІ. [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/2694-12>
14. Гудзевич Л. С. Показники зовнішнього дихання у здорових міських підлітків з різним соматотипом / Л. С. Гудзевич // Вісник морфології. – 2003. – № 9(1). – С. 135-138.
15. Березюк О. В. Залежність загальної захворюваності населення на алергічний риніт від продуктивності сміттєспалювального заводу / О. В. Березюк, С. М. Горбатюк, Л. С. Гудзевич, Т. І. Шевчук // Наукові праці Вінницького національного технічного університету. – 2023. – № 3. – 6 с. – Режим доступу до журналу: <https://praci.vntu.edu.ua/index.php/praci/article/view/695/660>
16. Шевчук Т. І. Антропогенна зміна довкілля як фактор поширення паразитарних захворювань людини / Т. І. Шевчук, В. М. Шкарупа, С. С. Хлестова // Довкілля і здоров'я : Матеріали наук.-практ. конф., Тернопіль, 27-28 квіт. 2017 р. – Тернопіль, 2017. – С. 220-222.
17. Березюк О. В. Залежність захворюваності дорослого населення на транзиторні ішемічні атаки від продуктивності сміттєспалювального заводу / О. В. Березюк, Т. Б. Васенко, С. М. Горбатюк, І. М. Климчук // Наукові праці Вінницького національного технічного університету. – 2023. – № 2. – 6 с. – Режим доступу до журналу: <https://praci.vntu.edu.ua/index.php/praci/article/view/685/650>
18. IoT в охороні здоров'я: Застосування, переваги та виклики у 2023 році. [Електронний ресурс] – Режим доступу до ресурсу: <https://stfalcon.com/uk/blog/post/iot-in-healthcare-benefits-challenges>
19. Чорна В. В. Показники захворюваності і поширеності та сучасні погляди на профілактику хвороб / В. В. Чорна, С. С. Хлестова, Н. І. Гуменюк // Вісник Вінницького національного медичного університету. – 2020. – Т. 24, №1. – С. 158-164.
20. Піскун Р. П. Ультроструктура кори головного мозку при експериментальній дисліпопротеїдемії та її фармакокорекції / Р. П. Піскун, С. М. Горбатюк // Biomedical and biosocial anthropology. – 2007. – № 9. – С. 274-275.
21. Горбатюк С. М. Лігногумат натрію як модифікатор мутагенних ефектів мітоміцину С / С. М. Горбатюк, Н. М. Гринчак, К. В. Мусатова [та ін.] // Матеріали I Міжнародної науково-практичної конференції "Ліки – людині. Сучасні проблеми фармакотерапії і призначення лікарських засобів", 30-31 березня 2017. – Харків : Національний фармацевтичний університет, 2017. – Т. 2. – С. 97.
22. Інтернет речей: вплив та наслідки для надання медичної допомоги. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7685921/>

Костишин Павло Віталійович – студент групи 4КН-21б, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, Вінниця, e-mail: kostishinpavlo24@gmail.com

Науковий керівник: **Березюк Олег Володимирович** – доцент, доктор технічних наук, професор кафедри безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, Вінниця, e-mail: berezyukoleg@i.ua

Kostyshyn Pavlo – student of the 4CS-21b group, Faculty of Intellectual Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: kostishinpavlo24@gmail.com

Supervisor: **Bereziuk Oleh** – Associate Professor, Doctor of Technical Sciences, Professor of the Department of Life Safety and Safety Pedagogy, Vinnitsa National Technical University, Vinnitsa, e-mail: berezyukoleg@i.ua