УДК 681. 28

Березовський М.А.,
Маліновський В.І.

АНАЛІЗ ФАКТОРІВ КІБЕРЗАГРОЗ І ПІДХОДИ ДО ЗАХИСТУ ПРОЦЕСУ ПЕРЕДАВАННЯ І ОБРОБЛЕННЯ ІНФОРМАЦІНИХ ДАНИХ ДЛЯ ІНТЕЛЕКТУАЛЬНИХ БІОМЕДИЧНИХСИСТЕМ

Вінницький національний технічний університет

Аннотація. Розглянуто аспекти і проведемо короткий аналіз проблем кібербезпеки, що виникають у сучасних біомедичних приладах і системах, які досить часто підключаються і керуються через мережу Інтернет. Розглядяються основні чинники впливу появи інформаційних загроз та наслідки при їх успішному прояві. Розглянуто перспективи розвитку і підходи до методу захищеної передачі даних і захищеної криптографічної обробки інформації у IoT медичного застосування .

Ключові слова: біомедичні прилади, біомедичні IoT, канали зв'язку, Інтернет речей (IoT).

Abstract. Are considered a some aspects and a brief analysis of cybersecurity problems that arise in modern biomedical devices and systems, which are often connected and controlled via the Internet. The main factors of data threats and the consequences that may occur in their successful manifestation are considered..

Keywords: biomedical devices, biomedical IoT, communication channels, Internet of Things (IoT).

Сучасні біомедичні технології і прилади є високоінтелектуальними, майже повністю автоматичними або автоматизованими і передбачають обмін даними через мережу передачі даних (МПД) на базі глобальної мережі Інтернет. Також сучасні інтелектуальні біомедичні технології, а також останні тенденції до впровадження технологій телемедицини та телеконференцій дозволяють організовувати високоефективне, комфортне і автоматизоване керування та моніторинг біомедичних процесів і систем через організовані канали віддаленого зв'язку на базі мережі Інтернет, що відповідає концепції біомедичного застосування Інтернету речей (Internet of Thinks або IoT). Разом з тим, це несе значні ризики від впровадження інформаційних технологій, пов'язані із кібербезпекою та інформаційною безпекою цілісності таких біомедичних IoT систем і мереж.

Тренди сучасних років говорять, що основними кіберзагрозами у біомедичних IoT є:

- перехоплення і спотворення даних;
- влаштовування «ін'єкція» шкідливого коду або перехопленого спотвореного коду керування в інформаційні потоки і функіонал керування мережами IoT;
- таргетовані/цілеспрямовані кібератаки атаки на системи біомедичних IoT і вивід їх із ладу;
- перехоплення керування та/або перехоплення потоків даних моніторингу.

Тому тренди останніх років і тенденції кіберзагроз свідчать, що у 2020-2021 велика частка до 15-25% загроз у глобальній мережі припадає саме на галузь Інтернету речей, 20-40% із якої спрямовано саме на біомедичні пристрої і системи із комунікаційними можливостями та/або старт функціями. В подальшому прогнозується збільшення числа атак на біомедичні IoT-пристрої і на сферу IoT взагалі, охоплюючи системи "розумний будинок" і "розумний кабінет лікаря» окремі компоненти автоматизації та телемедицини та інші біомедичні прилади. З'явиться більше проблем для систем безпеки, заснованих на штучному інтелекті, які допоможуть компаніям покращити захист, адже ступінь захисту і наслідків відповідальності вищий. Також значними є ризики для хмарних («cloud based») сервісів та їх гнучкий функціонал. Однак, коли справа доходить до захисту хмарних сервісів і апаратної інфраструктури, вся ця гнучкість та легкість можуть повернутися пізніше. Найбільша вразливість для хмарних обчислень — прості невірні конфігурації. Також трендами 2020-2021рр. є атаки на комунікації та комунікаційні канали і інтерфейси звязку пристроїв : Wi-Fi, 3/4/5G, провідні комунікації на базі Ethernet, які активно інтегровані у функціонал біомедичних пристроїв.

Підвищення безпеки мобільних платформ і пристроїв.Із зростанням популярності смарт-пристроїв збільшується інтерес до них з боку кіберзлочинців, які постійно шукають нові способи атак користувачів.

- канали передачі Wi-Fi та Bluetooth та кабельні комунікації;

- ядро і компоненти вводу-виводу на суміжних мобільних операційних систем пристроїв керування/моніторингу біомедичної системи(Android і др.), а також неперевірені додатки;
- підмінене оновлення ПЗ або постачання ПЗ із додатковим шкідливим функціоналом;
- порушення прав розмежування доступу/отримання перевищення адмін. прав;
- недосконаліть і вразливості операційної системи біомедичного пристрою;
- відсутність захищених IPS та VPN/ Proxy та мережевого екрану;
- використання експлойтів і „пробиття“ для порушення штатного функціоналу - ПЗ/ядра операційної системи пристрою/системи, що призводить до порушення/додання/модифікування/зрізання системних програмних функцій ПЗ;
- порушення безпеки пограничних пристроїв та модулів зв'язку у пристрої (маршрутизатори, комутатори, обладнання радіозв'язку та інше), у сукупності із - вразливостями проміжних протоколів зв'язку і передачі даних;
- порушення механізму встановлення захищеного з'єднання та атаки MITM;
- недосконаліть і кіберзагрози опорної архітектури і суміжних пристроїв;
- віруси, троянські коні і бекдори, які адаптовані спеціально під конкретну інфраструктуру мережі біомедичних IoT і архітектуру системи;
- недосконаліть мережевих і хмарних сервісів, програмних інтерфейсів API і недосконаліть налаштування безпеки мобільних пристроїв.

Враховуючи це, необхідною є розробка нового метода і моделі захисту даних для критичної інфраструктури IoT біомедичного спрямування, які б забезпечували повну безпеку функціоналу і захищену передачу даних та їх обробку для забезпечення сталості і надійності функціоналу. Нова модель і метод повинні базуватись на поєднані функціоналу віртуалізації в контейнерах для окремих потоків інформації із змішаним додаткових неінформативним функціоналом або створеннями додаткових інформаційних потоків із надійним вдосконаленим шифруванням із зміщенням та у поєднанні із розпаралелюванням обчислювального процесу на різних розмежованих у правах доступу рівнях обчислень віртуальних обчислювальних середовищах(оболонок) для різних процесів.

Сьогодні, в століття цифрової епохи інформаційних технологій, для кожного користувача біомедичних систем із інтелектуальними функціями, або функціями керування із ПК/мобільного пристрою який входить до концепції IoT важливо розуміти необхідність безпечної експлуатації передавання, оброблення та зберігання даних, а також безпеку і кібербезпеку і наслідки від її порушення в цілому.

Березовський Максим Анатолійович – студент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна.

Науковий керівник: ***Маліновский Вадим Ігоревич*** – к.т.н.**,** доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна.

Beresovskyi Maxim — barselour of Data Protection Department in Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine.

Supervisor: ***Malinovskyi Vadym*** — PhD (Eng), Associated Professor of Data Protection Department in Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine.