УДК 004.415.056:658.115

А. О. Азарова
В. О. Вальчук

Публічне управління процесами розподіленого доступу в галузі телемедицини засобами СУБД

Вінницький національний технічний університет

Анотація У даній роботі досліджуються ризики безпеки, пов'язані з використанням телемедичних послуг і технічних рекомендацій щодо захисту медичних карток з точки зору їх конфіденційності, цілісності і доступності.
Ключові слова: телемедицина, кібербезпека, захист конфіденційних даних

Abstract This article examines the security risks associated with the use of telemedicine services and technical recommendations for the protection of medical records in terms of their confidentiality, integrity and availability.
Key words: telemedicine, cyber security, protection of confidential data

Вступ

Широке й повсюдне використання інформаційних технологій впливає на життя людей у всіх вимірах. Одним з них є охорона здоров'я, яке змінює спосіб співпраці як пацієнтів, так і медичних працівників. Це матеріали з швидким розвитком телемедицини та електронної охорони здоров'я, які стали стандартною медичною практикою і щодня використовуються в десятках країн, і наразі в Україні. Телемедицина відноситься до практики медичних працівників з оцінки, діагностики та лікування пацієнтів у віддалених районах з використанням телекомунікаційних технологій. Це також дає можливість пацієнтам, які знаходяться у віддалених місцях, швидко, ефективно і без поїздок отримати доступ до медичної експертизи. Однак реалізація телемедичних додатків пов'язана виключно з необхідністю обробки конфіденційних персональних даних пацієнтів, зазвичай зберігаються в електронних медичних картах (Емі), до яких тепер можна отримати доступ з інтернету. Персональні дані пацієнтів, включаючи медичні та діагностичні звіти, повинні бути належним чином захищені від несанкціонованого доступу. Інформаційні технології, які забезпечують застосування телемедицини, включають всі стандартні загрози, відомі з Інтернету, які застосовуються до систем, обладнання та програмного забезпечення.

Результати дослідження. Керування інформацією зв'язку, що передається по мережі, може піддаватися, наприклад, підслуховуванню і модифікації. Інформація про релізі накладає необхідність забезпечити: цілісність оприлюднення інформації – переконавшись, що інформація не була змінена у бік клієнта, і конфіденційність – переконавшись, що інформація не була доступна ніяким іншим сторонам, ніж дозволено під час її передачі запитуючій стороні. Цілісність може бути реалізована за допомогою цифрового підпису на основі кваліфікованих сертифікатів. Цифровий підпис додається до запитуваної інформації. Він розраховується з використанням асиметричної криптографії та ключів згенерованих з сертифіката (так званий відкритий ключ доступний публічно, а закритий ключ, який повинен зберігатися надійно власником – зазвичай на смарт-карті, захищеної секретним PIN-кодом)[9] Алгоритм дозволяє відправнику створити хеш з повідомлення, а потім зашифрувати його своїм закритим ключем (відомим тільки відправнику). Потім, якщо віддалений сайт здатний розшифрувати підпис, він вважає, що це дійсний цифровий підпис від відправника . Він дає одержувачу підставу вважати, що повідомлення було створено відомим відправником, що він не може заперечувати надсилання повідомлення і що його не було змінено в дорозі (цілісність). Інформація, що передається по мережі, може бути підслухана.[2] Це особливо важливо, коли пристрої використовують бездротові з'єднання із загальним бездротовим середовищем (часто незахищеною гарячою точкою WiFi) і коли трафік може бути легко захоплений і прочитаний. Конфіденційність інформації може бути забезпечена шифруванням самої інформації або шифруванням каналу зв'язку. Це також можна зробити за допомогою цифрових сертифікатів.

Відкритий ключ запитувача може використовуватися для шифрування інформації. Після цього тільки запитувач зможе розшифрувати повідомлення (з його закритим ключем). Сертифікати також можуть використовуватися для шифрування каналу зв'язку.[3-5]

Конфіденційні медичні записи зазвичай зберігаються в базах даних, захист яких має вирішальне значення[1]. Рекомендується застосовувати шифрування даних при зберіганні, яке забезпечує конфіденційність і цілісність, а також робить спроби читання вкраденої бази даних безуспішними. Звичайно, конфіденційні дані після отримання від служби також зберігаються на призначених для користувача пристроях[6-7]. Це можуть бути як офісні комп'ютери, які використовуються в лікарнях та інших медичних установах, так і смартфони, все частіше-приватні пристрої, використовувані також для офіційних справ. Таке ставлення зазвичай називається "принесіть свій пристрій" і сприймається фахівцями з безпеки як особливо ризикована з-за дуже швидкого зростання загроз, спрямованих на мобільні пристрої і дуже недбалого використання смартфонів, які слід розглядати як персональні комп'ютери. Кожен мобільний пристрій повинен мати хоча б антивірусне програмне забезпечення.[10] Також настійно рекомендується застосовувати для використання телемедичних послуг так званий захищений профіль, який дозволяє шифрувати дані, що обробляються під час його активації. [8]

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон Про захист персональних даних (від13.01.2011 №2939-VI)
2. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2017. – 120 с.
3. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин ; под ред. В. Ф. Шаньгина. – 2-е изд., перераб. и доп. – М. : Радио и связь, 2001. – 376 с.
4. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа [Текст] / А.Ю. Щеглов. – СПб.: Наука и техника, 2004. – 384 с.
5. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма „Захист інформації від несанкціонованого копіювання шляхом прив'язки до унікальних параметрів вінчестера і використання ключа активації" / Азарова А. О., Азарова Л. Є., Каплун І. С., Щербатюк А. В. Заявка від 05.06.2018 р. №80958. Дата реєстрації 11.06.2018 р.
6. Свідоцтво про реєстрацію авторського права на твір №80464. Комп'ютерна програма „Мобільний додаток для захищеного передавання конфіденційних даних у смартфонах" / Азарова А. О., Азарова Л. Є., Бадя Ю. В. Заявка від 12.06.2018 р. №81238. Дата реєстрації 24.07.2018 р.
7. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма „Програмний модуль ідентифікації користувача за відбитками пальців через смартфон з подальшою авторизацією" / Азарова А. О., Азарова Л. Є., Мисько Ю. О., Колган В. А. Заявка від 05.06.2018 р. №80951. Дата реєстрації 11.06.2018 р.
8. Безпека та конфіденційність електронних медичних записів, MacAfee white paper, 2011 7.
9. . T. L. Робертс, електронні медичні записи: успіх вимагає культури інформаційної безпеки, читальний зал Інституту SANS InfoSec, 12/2012 4
10. Шосте щорічне базове дослідження з Конфіденційності та безпеки даних охорони здоров'я, Ponemon Institute LLC, травень 2016

Азарова Анжеліка Олексіївна – к.т.н., проф. каф. МБІС, заст. декана Факультету менеджменту та інформаційної безпеки з наукової роботи та міжнародного співробітництва Вінницького національного технічного університету, м. Вінниця , e-mail: azarova.angelika@gmail.com.

Вальчук Віталій Олегович – студент гр. УБ-15б факультету менеджменту та інформаційної безпеки, м. Вінниця, e-mail: vitalik_valchuk@mail.com.

Azarova Anzhelika O. — Ph.D., Professor, Deputy dean of the Faculty of management and information security by scientific work and international cooperation Vinnytsia National Technical University, Vinnytsia.

Valchuk Vitalii O. – Department of management and security of information systems, Vinnytsia National Technical University, Vinnytsia.