ОСОБЛИВОСТІ ОЦІНКИ РИЗИКІВ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ IDIS2GO

Уманська А.О., Смірнов А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Управління ризиками безпеки програмного забезпечення - це процес виявлення, оцінки та мінімізації ризиків, пов'язаних із розробкою, впровадженням та використанням програмного забезпечення. Його мета - зменшити ймовірність виникнення проблем (наприклад, збоїв, помилок, загроз безпеці) та їхній вплив, забезпечуючи стабільність, якість і безпеку роботи програмного забезпечення. Сучасні інформаційні технології відіграють ключову роль у розвитку медицини, забезпечуючи ефективне управління пацієнтськими даними, автоматизацію діагностики та моніторинг стану здоров'я. Програмне забезпечення, що використовується в медичній сфері, вимагає особливо високих стандартів безпеки та надійності, оскільки від його роботи залежить не лише якість медичних послуг, а й життя пацієнтів [1]. Оцінка ризиків безпеки є критичним етапом у розробці та впровадженні медичних програмних продуктів. Вона дозволяє виявити потенційні загрози, що можуть вплинути на конфіденційність, цілісність і доступність медичних даних, а також уникнути збоїв у роботі систем, які можуть призвести до критичних наслідків. Загрози безпеці програмного забезпечення можуть включати як технічні аспекти, такі як помилки програмного коду чи кібератаки, так і організаційні фактори, наприклад, недоліки у використанні програмного забезпечення або неналежне управління доступами [2, 3].

Метою доповіді є розробка стратегії безпеки оцінки ризиків програмного забезпечення IDIS2GO в сучасних медичних сервісних системах. В доповіді наводиться, що управління ризиками в програмному забезпеченні IDIS2GO є ключовим етапом для забезпечення його стабільної, безпечної та ефективної роботи. Враховуючи, що система працює з медичними даними, особливу увагу потрібно приділити конфіденційності, цілісності та доступності інформації, а також безперервності її функціонування. Виявлені загрози у процесі аналізу визначено, що найбільші ризики для IDIS2GO пов'язані з технічними аспектами (помилки коду, збої в алгоритмах, вразливості безпеки, можливі кіберзагрози), організаційними чинниками (недостатня підготовка користувачів, некоректне управління доступами, ризики втрати даних), операційною безпекою (відсутність механізмів резервного копіювання, відмовостійкості, планів відновлення після збоїв). Для мінімізації потенційних загроз запропоновані були наступні заходи: технічні рішення: регулярне оновлення програмного забезпечення, впровадження механізмів шифрування та автентифікації, автоматизоване тестування на помилки та вразливості; організаційні заходи: навчання медичного персоналу щодо безпечного використання системи, визначення ролей і рівнів доступу для користувачів, розробка політики реагування на інциденти та планів відновлення; моніторинг

і контроль: використання систем логування та аналізу безпеки (SIEM). Не менш важливим аспектом є механізми самодіагностики та моніторингу: вбудована система перевірки коректності зібраних даних, виявлення аномалій та автоматичне сповіщення адміністратора, логування всіх критичних подій у системі. Організаційні заходи: навчання персоналу: регулярні тренінги для лікарів та технічного персоналу щодо використання IDIS2GO, ознайомлення з протоколами кібербезпеки, симуляційні навчання щодо дій у разі збоїв системи [2, 4].

Впровадження розробленої стратегії дозволить зменшити ймовірність збоїв і атак завдяки вдосконаленій архітектурі безпеки та підвищити якість та надійність програмного забезпечення шляхом покращення тестування та контролю, а також забезпечити відповідність нормативним вимогам медичної сфери та законодавства у сфері захисту даних. Ці заходи допоможуть знизити фінансові та репутаційні ризики для медичних установ, що використовують IDIS2GO.

На основі зазначених ризиків можна виділити декілька рекомендацій щодо вдосконалення, таке як: резервування, безперервне навчання персоналу, тестування, впровадження SIEM (використовувати системи моніторингу подій безпеки для швидкого виявлення загроз) та регулярний аудит (проводити технічні й безпекові аудити, оцінюючи ризики на основі оновлених даних). Управління ризиками є критично важливим етапом у процесі розробки програмного забезпечення (ПЗ), що дозволяє мінімізувати можливі негативні наслідки, пов'язані з невизначеністю, що може вплинути на якість, безпеку, бюджет та строки виконання проєкту [5].

Отже, розробка та впровадження ефективної системи управління ризиками для IDIS2GO забезпечить високий рівень безпеки, надійності та стабільності роботи програмного забезпечення. Це дозволить розширити сфери його використання, покращити довіру серед лікарів та пацієнтів, а також сприятиме успішній інтеграції системи в сучасну медичну інфраструктуру.

Список літератури

1. PQCrypto 2017. Netherlands, 26--28 June 2017. [Електронний ресурс] – Режим доступа: https://2017.pqcrypto.org/conference/ - 02.06.2018.

2. Tkachov, A., Hapon, A., Balagura, D., Sievierinov, O., Bukatych, I., & Havrylova, A. (2024, November). Analysis of the Software Security Protection. In 2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-8). IEEE.

3. Сєвєрінов, О.В., Переметчик О.В.. Комбінований метод аналізу ризиків інформаційної безпеки. Diss. НТУ «ХПІ», 2020.

4. Овчаренко М.Ю., Сєвєрінов О.В. Аналіз сучасних систем управління інформаційною безпекою та інцидентами безпеки. ЧДТУ, НТУ" ХПІ", ВА ЗС АР, УТіГН, ДП" ПД ПКНДІ АП", 2019.

5. Krishnan M. Soumya Software Development Risk Aspects and Success Frequency on Spiral and Agile Model. InternationalJournal of Innovative Research in Computer and Communication Engineering. 2015. № 3(1). P. 301-310.