

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В МЕДИЧНИХ ЗАСТОСУНКАХ ТА ЗАСТОСУНКАХ ДЛЯ ПІДТРИМКИ ЗДОРОВОГО СПОСОБУ ЖИТТЯ

Київський Авіаційний Інститут,
м. Київ, Україна

Анотація

У статті розглядаються основні законодавчі акти, які регулюють обробку персональних даних у сфері охорони здоров'я, зокрема GDPR (Загальний регламент про захист даних), HIPAA (Закон США про збереження конфіденційності медичних даних) та український закон «Про захист персональних даних». Особлива увага приділяється порівнянню цих нормативних актів і їх впливу на розробку медичних застосунків, що працюють з чутливими даними. Окрім того, у статті представлені методи оцінки кіберстійкості медичних додатків, зокрема моделювання загроз, аналіз впливу та оцінка вірогідності атак. Висвітлено принципи побудови стійкої системи кіберзахисту, зокрема принцип процесного підходу та ешелонованого захисту, що сприяють забезпеченню надійного захисту персональних даних у медичних застосунках.

Ключові слова: захист персональних даних, конфіденційність, безпека даних, медичні застосунки.

Abstract

The article examines the main legislative acts that regulate the processing of personal data in the healthcare sector, in particular GDPR (General Data Protection Regulation), HIPAA (US Health Insurance Portability and Accountability Act) and the Ukrainian law "On the Protection of Personal Data". Particular attention is paid to the comparison of these regulatory acts and their impact on the development of medical applications that work with sensitive data. In addition, the article presents methods for assessing the cyber resilience of medical applications, in particular threat modeling, impact analysis and assessment of the likelihood of attacks. The principles of building a resilient cyberdefense system are highlighted, in particular the principle of a process approach and layered protection, which contribute to ensuring reliable protection of personal data in medical applications.

Keywords: personal data protection, confidentiality, data security, medical applications.

Захист персональних даних є критичним аспектом для медичних застосунків і додатків, що сприяють здоровому способу життя. В умовах цифрової трансформації системи охорони здоров'я та застосунки для підтримки здоров'я набувають популярності, адже вони дозволяють ефективно моніторити фізичний стан, давати рекомендації з харчування, тренувань та лікування. Однак разом з цими можливостями виникають і значні ризики для конфіденційності та безпеки особистої інформації користувачів.

В ЄС основним законом про конфіденційність і безпеку даних є **GDPR** (General Data Protection Regulation — Загальний регламент про захист даних). Цей закон застосовується в процесі розробки всіх застосунків, що використовують персональні дані. Основні положення цього документа такі [1]:

- **Стаття 9:** обробка персональних даних, що розкривають расове чи етнічне походження, політичні погляди, релігійні або філософські переконання, членство в профспілках, а також обробка генетичних даних, біометричних даних для унікальної ідентифікації особи, даних про здоров'я чи статеве життя людини або її сексуальну орієнтацію забороняється [1]. Однак у деяких випадках ця норма може бути проігнорована, наприклад, якщо особа дає офіційну згоду на обробку даних або якщо дані необхідні для виконання певних зобов'язань, наприклад, у випадку, коли вони потрібні для медичного лікування тощо.
- **Стаття 6:** обробка даних має здійснюватися лише у певних обмежених ситуаціях. Якщо дані збираються, особа, чий дані обробляються, повинна знати, які саме дані збираються і з якою метою.
- **Статті 15-17:** особа може запросити доступ до збережених даних або вимагати їхнього видалення.
- **Стаття 20:** особа може запросити свої дані у форматі, придатному для машинного читування, у зрозумілому вигляді.
- **Стаття 25:** персональні дані повинні зберігатися безпечно; особа, відповідальна за збереження даних, зобов'язана впроваджувати заходи безпеки для їхнього захисту.
- **Статті 33-34:** якщо персональні дані були розголошені, виробник повинен повідомити **органи захисту даних ЄС** (протягом 72 годин) і сповістити постраждалих осіб, якщо витік спричинив серйозну шкоду.
- **Стаття 35:** у випадку використання нових технологій, де існує високий ризик витоку даних, у деяких випадках необхідно провести **оцінку впливу на захист даних (DPIA — Data Protection Impact Assessment)**.
- **Стаття 22:** якщо рішення ухвалюються автоматично на основі персональних даних, особа, чий дані використовуються, повинна мати можливість **оскаржити рішення або вимагати людського втручання в процес ухвалення рішення**.

HIPAA — це федеральний закон США, створений для забезпечення стандартного захисту **РНІ** (інформації про стан здоров'я пацієнтів). Він гарантує, що лікарні, клініки, страхові компанії та навіть медичні пристрої несуть відповідальність за особисті медичні дані, дотримуючись суворих норм конфіденційності та безпеки. HIPAA містить два основних компоненти:

- **Правило конфіденційності (Privacy Rule)**, яке встановлює обмеження щодо того, хто може отримувати та розкривати медичну інформацію.
- **Правило безпеки (Security Rule)**, яке забезпечує заходи захисту, такі як **шифрування, контроль доступу та періодичні аудити**, щоб запобігти витокам даних.

Порівняння GDPR та HIPAA:

У порівнянні з HIPAA, **GDPR є значно ширшим** і застосовується до всіх галузей, а не лише до охорони здоров'я. Обидва закони зосереджені на захисті даних, але GDPR є **суворішим у деяких аспектах**:

- Пацієнти мають **«право бути забутими»** (вони можуть вимагати видалення своїх даних).
- Компанії повинні **повідомляти про витік даних протягом 72 годин** (HIPAA дозволяє 60 днів).

З іншого боку, HIPAA **більш конкретно** регулює медичні записи, але менш суворо ставиться до індивідуальної згоди, дозволяючи медичним установам передавати **РНІ** за певних умов.

Захист персональних даних в Україні:

Основний закон, що регулює діяльність зі збору та обробки персональних даних в Україні є «Закон про захист персональних даних» [2].

Основні положення даного закону, що можуть стосуватися процесу розробки ПЗ медичного призначення:

- Стаття 7: забороняється збирати біометричні дані та дані, що стосуються здоров'я крім випадків, коли необхідне надання медичної допомоги або коли особа погодила обробку персональних даних, проте згідно статті 6 частини 7 можливо збирання і обробка персональних даних без згоди, коли обробка персональних даних необхідна для забезпечення життєво важливих інтересів суб'єкта.
- Стаття 8: суб'єкт персональних даних має право знати, для чого збираються дані, як вони зберігаються, обробляються і т.д., а також має право знати механізми обробки персональних даних, відкликати згоду на їх обробку, отримати на протязі 30 календарних днів інформацію про те, чи оброблюються персональні дані особи, а також звертатися з вимогами видалити/видати персональні дані.
- Персональні дані мають бути захищеними, не передаватися іншим особам (крім випадків, коли суб'єкт персональних даних підтвердив свою згоду на передачу даних третім сторонам).

Також є окремі укази, закони, нормативні акти і т.д., які регулюють діяльність з обробки персональних даних в медичній галузі, наприклад, таким законом є Постанова Кабінету міністрів №411 від 25.04.2018, яка регулює електронну систему охорони здоров'я. Проте основним фреймворком для створення даних актів є «Закон про захист персональних даних».

Можна побачити, що GDPR та «Закон про захист персональних даних» мають багато спільних рис, а також схожі норми.

Для систематизованого підходу до оцінки кіберстійкості в сфері медичних додатків використовують наступні методи та підходи:

- Моделювання загроз
- Аналіз впливу
- Оцінка вірогідності

Під **моделюванням загроз** розуміють експертну оцінку того, які саме види та варіації кібератак є можливими та релевантними. Формулюється перелік або так званий каталог загроз зі стандартизованою класифікацією по типам.

Наступним етапом є **прогнозування наслідків** для організації від реалізації кібератак. Цей вид аналізу називається аналіз впливу. Необхідно зрозуміти, наскільки сильно постраждає конфіденційність, цілісність та доступність інформації від окремо взятої потенційної атаки.

Завершальним кроком є **оцінка вірогідності** успішного виконання кібератаки. До уваги треба брати як наявність механізмів кіберзахисту, так і технічну складність реалізації кібератаки злочинцями. Також на вірогідність спроб атаки впливає співвідношення ресурсів, які необхідно витратити на атаку, і цінності інформації та інформаційної системи, яку атакують.

Можна виділити наступні принципи побудови стійкої системи кіберзахисту:

- Принцип процесного підходу

Хорошою практикою вважається побудова системи кіберзахисту як сукупності взаємопов'язаних процесів. Популярною моделлю для цього є СУІБ – система управління інформаційною безпекою, побудованою на основі ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). У СУІБ прийнято включати наступний перелік процесів:

- Управління ресурсами
 - Безпека людських ресурсів
 - Фізична безпека та безпека інфраструктури
 - Управління комунікаціями та функціонуванням
 - Контроль доступу
 - Придбання, розроблення та підтримка інформаційних систем
 - Управління інцидентами інформаційної безпеки
 - Управління інцидентами інформаційної безпеки та вдосконаленням
 - Управління безперервністю бізнесу
- Принцип ешелонованого захисту

Окремий принцип побудови стійкої системи кіберзахисту – впровадження декількох заходів захисту від однієї потенційної кіберзагрози. Це обумовлено тим, що будь-яка технологія може давати збій. Якщо заходи захисту передбачають залучення людини, то варто згадати вислів «помилятися – це частина людської природи». Таким чином, недосконалість або відмову в спрацюванні одного рівня захисту необхідно компенсувати побудовою додаткового механізму кібербезпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

- [1]: *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. (2016). THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
- [2]: *Про захист персональних даних*. (n.d.). Офіційний Вебпортал Парламенту України. <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
- [3]: *Принципи побудови стійкої системи кіберзахисту*. (n.d.). [moz.gov.ua. https://moz.gov.ua/uk/principi-pobudovi-stijkoyi-sistemi-kiberzahistu](https://moz.gov.ua/uk/principi-pobudovi-stijkoyi-sistemi-kiberzahistu)

Студенников Владислав Дмитрович, Рудник Денис Миколайович, Факультет комп'ютерних наук та технологій. vladstudennikovwork@gmail.com, 5739122@stud.nau.edu.ua

Studennykov Vladyslav Dmytrovych, Rudnyk Denys Mykolayovych, Faculty of Computer Science and Technology.