УДК 004.056.5:61

ЗАХИСТ ДАНИХ В СИСТЕМІ EHEALTH

З. В. Дерен, О. М. Анісімова

Анотація. У даному дослідженні подана інформація про захист даних в національній системі охорони здоров'я. Розглянуто процес розробки та стан впровадження модулів системи, які відповідають за її безпеку. Проаналізовано особливості процесу збору та обробки персональних даних пацієнтів та заходи захисту цієї інформації. В дослідженні були сформульовані рекомендації та перспективи подальших досліджень у даному напрямку.

Ключові слова: захист даних, електронна система охорони здоров'я, персональні дані, eHealth.

Вступ. Безпека даних пацієнта та лікаря – одна з ключових вимог до електронної системи охорони здоров'я. Адже в системі зберігатиметься особиста інформація пацієнтів. Тому до вже існуючих методів захисту інформації розробляються додаткові, щоб звести нанівець можливість викрадення особистих даних.

Електронне здоров'я – дуже складна система. Тому у процесі розробки її компонентів були залучені фахівці з кібербезпеки декількох незалежних компаній, включаючи одну з компаній з «Великої четвірки» (найбільші у світі компанії, що надають аудиторські й консалтингові послуги). Було проведено низку аудитів кібербезпеки.

Наразі система електронного здоров'я перебуває у стані активної розбудови та нарощення можливостей. Підписання декларацій з лікарями – перший етап її активної роботи.

Виклад основного матеріалу. Електронна система охорони здоров'я – це інструмент для забезпечення прозорості процесів в охороні здоров'я; система, яка дозволяє справедливо розподіляти кошти і забезпечує чесну оплату лікареві за пацієнта, не дозволяє чиновникам різних рівнів використовувати корупційні механізми та мінімізує можливість маніпуляції даними. А найголовніше – це система, якій люди довіряють дані про своє здоров'я.

Система впроваджується в Україні в рамках медичної реформи, яку просуває в.о. міністра охорони здоров'я Уляна Супрун [1].

Персональні дані пацієнтів збираються за їх письмової згоди — вона є частиною декларації про вибір лікаря, затвердженої «Порядком вибору лікаря, що надає первинну медичну допомогу». Тож ставлячи підпис у декларації, людина погоджується на обробку своїх даних у системі «Електронне здоров'я».

Найближчим часом в електронній системі охорони здоров'я будуть обробляти лише так звані «нечутливі» персональні дані – паспортні дані, індивідуальний податковий номер, адресу проживання. Ці дані надаються для отримання більшості послуг в Україні: у банку, у соціальних службах, при оформленні пенсії або субсидії.

Зараз у центральному компоненті системи немає медичних даних або інших так званих «чутливих» даних.

Центральна база даних електронної системи охорони здоров'я знаходиться на території України, у захищеному дата-центрі в місті Києві. Цей дата-центр має комплексну систему захисту інформації (КСЗІ). Дата-центр відповідає міжнародним стандартам (сертифікат відповідності ISO 27001:2013, сертифікат виданий Bureau Veritas №IND17.0398/U) та українським стандартам (атестат відповідності ДССЗЗІ № 14162 від 22.07.16) у сфері захисту даних.

У процесі розробки компонентів електронної системи охорони здоров'я були залучені фахівці з кібербезпеки декількох незалежних компаній, включаючи одну з компаній з «Великої четвірки» (найбільші у світі компанії, що надають аудиторські й консалтингові послуги). Було проведено низку аудитів кібербезпеки.

У вересні 2017 р. на погодження до Державної служби спеціального зв'язку та захисту інформації України було подано технічне завдання на створення КСЗІ для системи.

Оскільки система активно будується, створюються нові модулі, електронна система охорони здоров'я в найближчий час буде працювати з КСЗІ в режимі дослідної експлуатації, що відповідає чинному законодавству.

КСЗІ буде впроваджуватись з урахуванням процедур доступу до даних основного користувача системи — Національної служби здоров'я України. У процесі розбудови НСЗУ будуть напрацьовані організаційні заходи захисту інформації, після чого заплановано проведення державної експертизи КСЗІ [2].

Усі відомості або сукупність відомостей про пацієнта, які вносяться в декларацію про вибір лікаря, є персональними даними пацієнта (ПІБ, дата народження, реєстраційний номер облікової картки платника податків, номер та серія паспорту або інших документів, що посвідчують особу, адреса проживання та інші дані, за якими можна ідентифікувати пацієнта). Згідно з формулюванням у Законі України «Про захист персональних даних», персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Коли у системі почнуть працювати електронний лікарняний та електронна медична картка, персональні дані будуть оброблятися для забезпечення лікувального процесу (для встановлення діагнозу, призначення лікування чи надання інших медичних послуг) та для покращення функціонування електронної системи охорони здоров'я.

Пацієнт (чи його законний представник), шляхом підписання декларації про вибір лікаря, який надає первинну медичну допомогу, підтверджує, що усвідомлює мету збирання і обробки своїх персональних даних. Тобто, підписуючи декларацію з терапевтом, педіатром чи сімейним лікарем, людина погоджується, що її персональні дані (чи дані її дитини/ підопічного (недієздатної особи) в електронній системі будуть доступні для обробки лікарем, з яким укладено декларацію, та лікарями, до яких вона буде звертатися за медичною допомогою за направленням свого лікаря.

Персональні дані пацієнтів у електронну систему охорони здоров'я можуть вводити визначені медзакладом уповноважені особи. Це може бути медичний працівник або інша уповноважена особа закладу охорони здоров'я, лікар-ФОП, який має ліцензію на провадження господарської діяльності з медичної практики та його працівники. На них має поширюватись дія законодавства про лікарську таємницю і вони повинні забезпечувати захист таких персональних даних. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом.

Персоналізовані дані (усі дані про пацієнта, які містяться у декларації, а із запровадженням електронного рецепта і електронної медичної картки – медична інформація і призначення) доступні тільки лікарю, з яким підписана декларація та лікарю, до якого пацієнт приходить по направленню. Коли у системі з'являться медичні дані, пацієнт зможе сам вирішувати, кому він додатково надає доступ.

За недодержання встановленого законодавством порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав пацієнта як суб'єкта персональних даних, передбачена адміністративна відповідальність. А за порушення недоторканності приватного життя (незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації) – кримінальна відповідальність.

Збір та обробка персональних даних пацієнта у системі «Електронне здоров'я» регулюється Законом України «Про захист персональних даних», Законом України «Про державні фінансові гарантії медичного обслуговування населення», Постановою КМУ «Деякі питання електронної системи охорони здоров'я» № 411 від 25.04.2018.

Електронна система охорони здоров'я спроектована для роботи з персональними даними з дотриманням кращих світових практик у сфері захисту даних. Система знаходиться на серверах дата-центру в Україні, який має комплексну систему захисту інформації (КСЗІ) та пройшов атестацію у Державній службі спеціального зв'язку та захисту інформації (ДССЗЗІ).

Наразі електронна система охорони здоров'я активно розбудовується, створюються нові модулі [3].

Безпека української електронної системи охорони здоров'я – це ключовий пріоритет, саме тому цьому приділяється особлива увага. А до існуючих комплексів безпеки розробляються і впроваджуються додаткові заходи та технічні рішення. Перш ніж увійти в систему, лікарі проходять кілька етапів аутентифікації.

В електронній системі eHealth працює етап підтвердження входу – CAPTCHA – автоматизований комп'ютерний тест, який аналізує «поведінку» користувача при вході та може відрізнити людину від бота при спробі несанкціонованого доступу.

На програмному рівні, при вході лікарів у систему, безпечний доступ ґрунтується на технології двофакторної авторизації протоколу Oauth.2. Саме цей протокол забезпечує верифікацію входу та розгалуження прав доступу до даних, а також перелік операцій для обробки цих даних. Технічно вся процедура входу та підтвердження займає декілька секунд, що є зручним для користувачів.

CAPTCHA – це додатковий етап захисту, остання версія якого є технологією нового покоління і є візуально невидимою, а тому не потребує від користувача додаткових дій. Однак, якщо система все-таки виявить підозрілу поведінку, то попросить підтвердити, що ви реальний користувач системи [4].

Висновки. Вся інформація, яку користувач передає до системи, одразу потрапляє до центральної бази даних – захищеного дата-центру, який знаходиться на території України й має комплексну систему захисту інформації (КСЗІ) та відповідає міжнародним і українським стандартам у сфері захисту даних.

По мірі розбудови системи, будуть створені потужніші заходи захисту інформації, щоби там могли зберігатися так звані "чутливі" персональні дані, в тому числі медична інформація – аналізи, історії хвороби, рецепти ліків, тощо.

Важливим пунктом у впровадженні системи «eHealth» є навчання працівників закладів освіти комп'ютерної грамотності. Працівники, які відповідальні за введення даних до системи повинні володіти навичками користування ПК на рівні користувача. Крім того важливо проводити курси навчання роботі безпосередньо в системі. Адже це покращить якість ведення бази та точність введених даних.

Продовження розвитку електронної системи охорони здоров'я потрібне, щоб вона стала ефективним та надійним інструментом для кожного громадянина.

Аннотация. В данном исследовании представлена информация о защите данных в национальной системе здравоохранения. Рассмотрен процесс разработки и состояние внедрения модулей системы, которые отвечают за ее безопасность. Проанализированы особенности процесса сбора и обработки персональных данных пациентов и меры защиты этой информации. В исследовании были сформулированы рекомендации и перспективы дальнейших исследований в данном направлении.

Ключевые слова: защита данных, электронная система здравоохранения, персональные данные, eHealth.

Abstract. This study provides information on data protection in the national health system. The development process and the state of implementation of the system modules responsible for its security are considered. The peculiarities of the process of collecting and processing personal data of patients and measures of protection of this information are analyzed. The research formulated the recommendations and prospects for further research in this direction.

Key words: data protection, electronic healthcare system, personal data, eHealth.

СПИСОК ЛІТЕРАТУРИ

1. eHealth. *Вікіпедія.* URL : https://uk.wikipedia.org/wiki/EHealth. Назва з екрану.
2. Персональні дані надійно захищені в електронній системі охорони здоров'я. *Міністерство охорони здоров'я України.* URL : http://moz.gov.ua/article/reform-plan/personalni-dani-nadijno-zahischeni-v-elektronnij-sistemi-ohoroni-zdorov'ja. Назва з екрану.
3. Як медикам працювати з персональними даними пацієнтів. *Міністерство охорони здоров'я України.* URL : http://moz.gov.ua/article/for-medical-staff/jak-medikam-pracjuvati-z-personalnimi-danimi-pacientiv. Назва з екрану.
4. Як захищений вхід до системи eHealth. *Ezdorovya.* URL : https://www.facebook.com/ezdorovya/posts/безпека-української-електронної-системи-охорони-здоровя-це-ключовий-пріоритет-са/626701057776463/. Назва з екрану.