ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ В МЕДИЧНОМУ ЕЛЕКТРОННОМУ ПАСПОРТІ

Ірина Шакало

Національна медична академія післядипломної освіти ім. П. Л. Шупика,
кафедра медичної інформатики, вул. Дорогожицька, 9, Київ 04112, тел.: 8-044-205-49-55

В останні роки в лікувально-профілактичні заклади, все більше впроваджуються інформаційні технології, зокрема електроні носії інформації [1,2]. Разом з великою користю та значними можливостями нові технології приносять й нові проблеми. Однією з них є проблема захисту медико-біологічних даних в медичному електронному паспорті (МЕП) від несанкціонованого доступу.

Основна задача системи безпеки – це одночасне забезпечення захисту інформації – забезпечення цілісності інформації, унеможливлення несанкціонованого доступу до ресурсів системи та програмам и даним, що в ній зберігаються. Реалізація системи безпеки носить комплексний характер і повинна функціонувати на всіх етапах обробки та передачі інформації [1]. На відміну від глобальних інформаційних систем в яких проблема безпеки стосується серверів, каналів зв'язку та кінцевих приладів (комп'ютери, диски тощо), у медичному електронному паспорті, як незалежному носії інформації, головна увага зосереджується саме на інформації, що зберігається в ньому. Медичний електронний паспорт, як одна із складових медичних інформаційних систем (МІС), несе в собі конфенденційні медико-біологічні дані, в зв'язку з чим для забезпечення захисту інформації повинні використовуватися організаційно-правові заходи та програмно-апаратні методи [1,2]. Зазвичай електронні бази даних використовують функції операційної системи, що веде до появи специфічних загроз і, відповідно, зумовлює необхідність боротьби з ними. Технічні засоби та методи виконують функції створення перешкод в разі спроб несанкціонованого доступу, ідентифікацію та аутентифікацію користувачів, розмежування прав доступу до ресурсів, реєстрацію подій, криптографічний та стеганографічний захист інформації.

Як відомо, до МІС, особливо баз даних лікувально-профілактичних закладів та даних, що зберігаються на МЕП, висуваються підвищенні вимоги щодо збереження та захисту даних. Власники МЕП і оператори МІС несуть відповідну моральну, адміністративну та юридичну відповідальність за збереження конфіденційності інформації, в процесі її запису, використання або передачі іншим вповноваженим користувачам. В зв'язку з тим, що персональні медико-біологічні дані громадян є інформацією обмеженого доступу, їх охорона забезпечується діючим законодавством.

В процесі пошуку технічних рішень щодо захисту даних МЕП слід розглядати два варіанти, а саме: захист носіїв і захист безпосередньо інформації, в усіх можливих місцях її зберігання. Сама концепція МЕП – як мобільного носія, накладає значні обмеження на застосування організаційних та апаратних засобів захисту. З іншого боку, умови практичної діяльності лікувально-профілактичних закладів також не завжди сприяють забезпеченню комплексного захисту МІС та носіїв даних.

Можливими шляхами забезпечення ефективного захисту інформації в МЕП є впровадження та використання стеганографічних та криптографічних засобів. Стеганографія забезпечує скритність щодо самого факту наявності даних, що в свою чергу також забезпечує аутентичність та цілісність файлів [3]. Такий метод захисту інформації забезпечить обмежений доступ до конфенденційної інформації, що заноситься та зберігається в МЕП.

Використання криптографічних засобів захисту інформації забезпечить цілісність, достовірність та конфіденційність. Як відомо, до криптографічних засобів відносяться заходи на основі використання технології електронного цифрового підпису [4,5]. Електронний цифровий підпис (ЕЦП) може виступати як засіб захисту інформації від несанкційованної зміни, підміни та підтвердження особи відправника та отримувача інформації (аутенфікації сторін). Юридична сила документа може підтверджуватися ЕЦП. Юридична сила ЕЦП визнається при наявності програмно-технічних засобів, що забезпечують ідентифікацію підпису, що може розглядатися як засіб захисту від підробки та несанкціонованої зміни інформації, але юридичну силу ЕЦП набуває, якщо він сертифікований.

Для використання засобів ЕЦП необхідні послуги центру, що забезпечує генерацію та контроль ключової інформації, необхідної при використання ЕЦП; готовить сертифікати відкритих ключів користувача; підтверджує достовірність виданих сертифікатів та вирішує конфліктні ситуації. Слід відмітити, що впровадження ЕЦП буде залежати від рівня та масштабів розвитку цієї технології в державі.

За характером використання ключа відомі алгоритми шифрування можливо розподілити на два типи: симетричні (з одним ключем, з секретним ключем), та несиметричні, іноді називають асиметричні (з двома ключами чи з відкритим ключем).

Використання засобів криптозахисту, що реалізують стандартні (тобто офіційно визнанні державою) алгоритми – найбільш розповсюджений засіб захисту інформації. Такі стандарти розробляються фахівцями, їх надійність периодично перевіряється, держава акредитує спеціальні центри по сертифікації (перевірки відповідності стандартам) засобів криптозахисту. В різних державах існують спеціальне законодавство, що регламентує логіку криптографічного захисту. Так, в США в 1991 році прийнято національний стандарт ЕЦП DSS, а з 2006 року затверджено новий симетричний алгоритм блочного шифрування (AES), також використовують алгоритми асиметричного шифрування (RSA), в Росії в 1994 році прийнято національний стандарт ЕПЦ РФ – ГОСТ Р34.10., в Україні ДСТУ 4145 (2002), Республіка Беларусь СТБ1176.2-99.

Формального визнання чужих стандартів недостатньо для коректного вирішення можливих спорів по електронним документам. Не всі параметри стандартів та умови, при яких стандарти зберігають свою криптографічну стійкість, можуть бути відомими фахівцям інших країн. Методики сертифікації засобів криптозахисту, як правило, закрити і їх експорт заборонено.

Література;

[1] Гусев А.В., Романов Ф.А., Дуданов И.П., Воронин А.В. Медицинские информационные системы: Монография. / Петрозаводск: Издательство, ПетрГУ, 2005. - 404 с.
[2] Минцер О.П. Информационная основа медицины третьего тысячелетия - медицинский электронный паспорт // Медичний всесвіт. - 2002. - №1-2. - Том 2. - С. 150 - 160.
[3] Voloshynovskiy S. et al. Attack Modelling: Towards a Second Generation Watermarking Benchmark // Preprint. Uneversity of Geneva.- 2001.- 58 p.
[4] Романцев Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерніх системах и сетях.- М.: Радио и свіязь, 2001.- 376 с.
[5] Яковлев А.В., Бкзбогов А.А., Родин В.В., Шамкин В.Н. Критографическая защита информации, 2006.- 112.