ЗАСТОСУВАННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ АУТЕНТИФІКАЦІЇ ЕЛЕКТРОННИХ ДОКУМЕНТІВ В ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩУ EHEALTH

Жук В.А., Пєнкін Ю.М.
Національний фармацевтичний університет, м. Харків, Україна

Електронна система охорони здоров'я eHealth – це інформаційне середовище реєстрації та фіксації взаємовідносин лікаря і пацієнта. eHealth – складна організаційна система, в якій усі дані, що вводяться до системи, мають бути засвідчені електронним цифровим підписом (ЕЦП). На сьогодні порядок і організація електронного документообігу, а також правовий статус та використання електронного підпису визначаються Законами України «Про електронні документи та електронний документообіг» (22.05.2003р., №851-IV), «Про електронні довірчі послуги» (05.10.2017р., №2155-VIII, набув чинності 07.11.2018) та іншими нормативними документами. Всі суб'єкти, які взаємодіють в рамках системи, повинні мати відповідні навички відносин та розуміти, як система функціонує в рамках своїх повноважень. У зв'язку з цим виникає нагальна потреба в формуванні у майбутніх фахівців галузі охорони здоров'я теоретичних і прикладних знань про сучасні методи забезпечення аутентифікації електронних документів в інформаційних інфраструктурах.

Типова програма з навчальної дисципліни «Інформаційні технології у фармації» складалася до впровадження eHealth в систему охорони здоров'я України і не містить відповідних складових. Пропонується доповнити цю програму новою темою «Процедура електронного підпису в організації юридично значущого документообігу». В результаті вивчення цієї теми студенти повинні оволодіти методологічним інструментарієм забезпечення цілісності електронних документів та підтвердження їх достовірності при обробці і передачі по каналах зв'язку в інформаційно телекомунікаційних системах. А також ознайомитися з методами і засобами правового, організаційно адміністративного, технологічного та програмного, програмно-апаратного забезпечення електронним цифровим підписом в документообігу.

За запропонованою темою на кафедрі фармакоінформатики НФаУ була розроблена практична робота «Електронний цифровий підпис» і в окремих групах студентів першого курсу фармацевтичного факультету були проведені пілотні заняття. Розробка заняття та проведення практичних робіт висвітили ряд проблем та особливостей.

Навчальний процес з дисципліни «Інформаційні технології у фармації» організується засобами пакетів програм Microsoft Office або OpenOffice.org. Кожен з цих пакетів дає можливість засвідчувати створю-

вані документи цифровим підписом. Але перш, ніж «підписувати» документи ЕЦП, необхідно отримати (або створити) особистий цифровий сертифікат і встановити його на свій ПК. Цифровий сертифікат - це захищений паролем файл, в якому зберігається різна інформація - ім'я власника, його e-mail адресу, ключ шифрування, а також найменування організації, що видала цей сертифікат, і дату, після якої цифровий сертифікат вважається недійсним. Більшість організацій, що видають сертифікати (ЕЦП), роблять це на комерційній основі. Другий варіант використання ЕЦП – самопідписаний сертифікат. На нашу думку, використовувати його недоцільно так як може створити хибну думку про процес накладання ЕЦП. "Самопідписаний " сертифікат у "зовнішньому світі" ніхто не зможе перевірити або підтвердити, але він залишається актуальним, якщо у вас є домен і документи циркулюють всередині нього.

Для виконання практичних занять студентами доцільно використовувати цифрові сертифікати, які співвідносяться з Microsoft Office або OpenOffice.org. Для підписання документа Word засобами Office 2007-2016, необхідно встановити утиліту «Крипто Про office signature» з офіційного сайту Крипто http://www.cryptopro.ru/products/office/signature/downloads.

OpenOffice.org передбачає використання цифрового сертифікату «Кореневого Сертифікату» CACert. CAcert.org - це орган сертифікації, який надає сертифікати для широкого загалу безкоштовно. Для того, щоб система перевірки сертифікатів, виданих в CACert функціонувала, необхідно сертифікат CACert внести в список «Кореневих Довірених Центрів». В ОС MS Windows це робиться за допомогою команди certmgr. Центри СА видають призначені для користувача сертифікати своїм клієнтам. У свою чергу користувачі, «зав'язані» на такий Цент Сертифікації, можуть перевіряти сертифікати один одного. Слід зауважити, що кожен особистий ключ користувача повинен бути записаний на окремий носій інформації, тому необхідно передбачити наявність у кожного студента особистого носія інформації (з’ємної флеш-карти, оптичного носія CD/DVD, захищеного носія ключової інформації тощо).

В подальшому планується в рамках практичної роботи студентів за цією темою розглянути використання ключів ЕЦП, виданих від Акредитованого центру сертифікації ключів Інформаційно-довідкового департаменту Державної фіскальної служби України, АЦСК органів юстиції України, АЦСК «Україна», АЦСК ПАТ КБ «ПРИВАТБАНК» та інших.