УДК 004.414.22:004.056:004.413.4

Петро Сергійович Клімушин,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Тетяна Петрівна Колісник,
кандидат педагогічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Безпека національної інфраструктури електронних підписів

Побудова інформаційного суспільства спирається насамперед на довіру. Основою довіри в сучасній концепції інформаційного суспільства є інфраструктура відкритих ключів (PKI) та її юридичне вдосконалення у ЄС кваліфікована інфраструктура відкритих ключів (QPKI) [1].

Вітчизняна національна система електронних підписів (НСЕП) не є інтероперабельною до ЄС, тому актуальним завданням дослідження має бути зведення її до Європейської еталонної моделі QPKI.

Метою дослідження є забезпечення довірчих відносин за рахунок механізму крос-сертифікації, тобто транскордонного визнання сертифікатів відкритих ключів ЕП, виданих у різних країнах.

Розвиток національної інфраструктури центрів сертифікації ключів (ЦСК) пов'язаний з удосконаленням організаційної її структури, а саме моделі удосконалення сертифікаційних шляхів між різними державними відомствами (установами, агентствами) та недержавними організаціями, в тому числі банківським сектором, таким чином, щоб забезпечити високу надійність та високий рівень довірчих відносин, інтеграцію і одночасно криптографічну самостійність кожного з відомств/організацій.

Треба зазначити, що удосконалення національної інфраструктури ЕП є не тільки організаційно-технічним питання, а й питанням національної безпеки. Існуючі світові моделі інфраструктури ЕП можна поділити на ізольовану, ієрархічну, мережну, шлюзову [2].

Ізольований – це ЦСК, що має само-підписаний сертифікат, який не завіряється будь-яким іншим ЦСК вищого рівня. Тут ЦСК-домен складається тільки з ізольованого ЦСК та клієнтів-держателів сертифікатів, яким видано сертифікати цим ЦСК. Приєднати ізольований ЦСК-домен до деякої інфраструктури ЕП можна двома способами: через ієрархічні відносини, як Підпорядкований ЦСК; через відносини рівноправних ЦСК.

В першому випадку вимагається обов'язково перевипуск (заміна) АЦСК-сертифіката, а отже повний перевипуск усіх сертифікатів держателів. В другому випадку це не вимагається – усі сертифікати держателів залишаються чинними після приєднання ізольованого ЦСК до деякого довірчого ЦСК-домену через механізм кроссертифікації.

Ієрархічна модель – це об'єднання ЦСК-доменів в структуру зв'язного графа, тобто «дерева, що має одну головну вершину (кореневий ЦСК), з якої будується структура підпорядкованих ЦСК.

В ієрархічній моделі є один головний ЦСК, якому довіряють усі користувачі – це кореневий ЦСК, тобто для усіх держателів сертифікатів ієрархічної моделі шлях сертифікації починається є одного Кореневого ЦСК. Кореневий ЦСК не випускає сертифікатів для клієнтів, окрім виключно підпорядкованих ЦСК

Недоліки: компрометація «кореня» призводить до компрометації усього ієрархічного «дерева» та необхідності заміни усіх без виключення ключів держателів; єдиний кореневий ЦСК може бути неможливим із «політичних» міркувань – конкуренція, міжвідомчі перепони тощо.

Мережна модель – це модель встановлення довірчих відносин між окремими ізольованими та ієрархічними ЦСК-доменами без довірчого посередника. Довірчі відносини встановлюються через механізм крос-сертифікації.

Перевага: дуже еластична структура - VA=CT 1030B> B>G>: 4>2V@8 (=5 T48=0). 54>;V:: @>7H8@5==O H;OEC A5@B8DV:0FVW T 1V;LH A:;04=8< ?@>F5A><, =V6 2 VT@0@EVG=V9 <>45;V.

Шлюзова модель складається із окремих незалежних ізольованих та ієрархічних доменів, в тому числі інших структур зі шлюзовою моделлю, які об'єднані довірчими відносинами через довірчого посередника (шлюзовий ЦСК) за допомогою механізму крос-сертифікації. Така модель об'єднує переваги ієрархічної та мереженої моделей. Шлюзовий АЦСК не випускає сертифікатів для окремих користувачів, а тільки здійснює крос-сертифікацію між доменами на рівні однорангових відносин. Це

дозволяє встановити прості та прозорі відносини довіри між різними об'єднаннями користувачів.

Переваги шлюзової моделі в порівнянні з мережаною моделлю: можливість застосувати більш сувору процедуру реєстрації учасників, в тому числі з урахуванням вимог для ієрархічних ЦСК; при компрометації будь-якого з ЦСК-учасників, цей ЦСК інформує шлюзовий ЦСК і йому не потрібно «множити» інформацію на всіх ЦСК-учасників, так як цю функцію виконує шлюзовий ЦСК [3].

Національна ієрархічна інфраструктура ЕП повинна трансформуватися до шлюзово-ієрархічної моделі виходячи з питання національної безпеки та можливості забезпечення транскордонної взаємодії в світовому інформаційному просторі.

Список бібліографічних посилань

1. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2155-19 (дата звернення: 30.10.2019)
2. Шевченко В. Л., Берестов Д. С., Зотова І. Г. Вибір моделі побудови інфраструктури відкритих ключів. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України.* 2014. № 1. С. 126–129. URL: http://nbuv.gov.ua/j-pdf/Znpcvsd_2014_1_21.pdf (дата звернення: 30.10.2019).
3. Бєлов С. В., Мартиненко С. В. Моделі побудови національної інфраструктури центрів сертифікації ключів та їх ризики // AMB Group : сайт. URL: http://www.itsway.kiev.ua/pdf/Model-CA_Risks.pdf (дата звернення: 30.10.2019).

Одержано 01.11.2019