УДК 004.056

А.В. Скирда

ДОСЛІДЖЕННЯ НЕОБХІДНОСТІ ТА НОМЕНКЛАТУРИ ЗАХИЩЕНИХ НОСІЇВ ОСОБИСТИХ КЛЮЧІВ В УКРАЇНІ

Вінницький національний технічний університет

Анотація

Розглянуто питання необхідності та номенклатури (доступності) захищених носіїв особистих ключів в Україні.

Ключові слова: особистий ключ, захищений носій, токен.

Abstract

The issue of necessity and nomenclature (availability) of protected holders of private keys in Ukraine is considered.

Keywords: private key, secure media, token

Вступ

З прийняттям в 2017 році в Україні законодавчого акту [1], який замінив поняття «електронного цифрового підпису» та «електронної печатки» на «засіб кваліфікованого електронного підпису чи печатки», актуальною стала проблема зберігання користувачами своїх особистих ключів.

Метою роботи є питання необхідності та номенклатури (доступності) захищених носіїв особистих ключів в Україні при використанні посадовими особами органів органу державної чи регіональної влади та управління кваліфікованого електронного підпису чи печатки.

Результати дослідження

Законодавчо [1] визначено наступні терміни:

- особистий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;
- пара ключів – особистий та відповідний йому відкритий ключі, що є взаємопов'язаними параметрами алгоритму асиметричного криптографічного перетворення;
- засіб кваліфікованого електронного підпису чи печатки - апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення кваліфікованого електронного підпису чи печатки, та/або перевірки кваліфікованого електронного підпису чи печатки, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки.

В принципі, особистий (закритий) ключ, у вигляді файлу може зберігатися на жорсткому диску комп'ютера, або на звичайному флеш-накопичувачі. Але такий спосіб зберігання уразливий відносно прямих та мережевих атак. Захист ключа за допомогою пароля допомагає, але недостатньо ефективно: паролі уразливі відносно багатьох атак. Поза сумнівом, для зберігання особистих (закритих) ключів необхідне використання більш безпечного сховища, тобто захищеного носія особистих ключів.

Пунктом 2 Порядку [2] визначено термін – захищений носій особистих ключів – це засіб кваліфікованого електронного підпису чи печатки, що призначений для зберігання особистого ключа та має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на ньому даних від несанкціонованого доступу, безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.

Часто у побуті захищені носії особистих ключів називають електронними ключами, токенами, апаратними токенами.

Особисті ключі генеруються, зберігаються та використовуються тільки усередині електронного ключа, та жодним способом не потрапляють за його межі. Апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливлює доступ до особистих ключів з боку

апаратно-програмного середовища. Зберігання особистих ключів та інших ключових даних здійснюється у внутрішньому постійному запам'ятовуючому пристрої електронного ключа.

З огляду на використання криптографічних алгоритмів та перетворень в реалізації покладених на електронні ключі функцій, необхідною умовою їх використання є наявність чинних позитивних експертних висновків за результатами державної експертизи у сфері криптографічного захисту інформації, що зареєстровані в Адміністрації Державної служби спеціального зв'язку та захисту інформації України [3].

Найбільш поширені у використанні захищені носії особистих ключів представлені в таблиці 1:

Таблиця 1 – Захищені носії особистих ключів

Назва	Експертний висновок	
	на засіб КЗІ	на засіб КЕП
Електронний ключ «Кристал-1»	№ 04/02/03-171 від 19.01.2018	№ 04/05/02-998 від 14.04.2021
Електронний ключ «Алмаз-1К»	№ 04/05/02-995 від 14.04.2021	№ 04/05/02-996 від 14.04.2021
Електронний ключ «SecureToken-337»	№ 04/05/02-1380 від 12.05.2021	№ 04/05/02-1381 від 12.05.2021
Електронний ключ«Efit Key»	№ 04/05/02-992 від 14.04.2021	№ 04/05/02-1004 від 14.04.2021
Електронний ключ«AvestKey»	№ 04/03/02-3004 від 03.08.2017	-
Смарт-карта «CryptoCard-337»	№ 04/05/02-1382 від 12.05.2021	№ 04/05/02-1383 від 12.05.2021
Безконтактний електронний носій ID-карти паспорту громадянина України	№ 04/05/02-1279 від 29.04.2021	№ 04/05/02-1280 від 29.04.2021
Електронний ключ Алмаз-1К (Bluetooth-пристрій)»	№ 04/05/02-995 від 14.04.2021	№ 04/05/02-996 від 14.04.2021

Висновки

Встановлено, що посадові особи органів органу державної чи регіональної влади та управління зобов'язані використовувати виключно кваліфікований електронний підпис чи печатку, особисті ключі яких повинні зберігатися на захищених носіях. Номенклатура захищених носіїв широко та вільно представлена на ринку України вітчизняними виробниками.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

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/go/2155-19 (дата звернення: 20.12.2021).

2. Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності : Постанова Кабінету Міністрів України; Порядок, Перелік від 19.09.2018 № 749 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/749-2018-%D0%BF (дата звернення: 20.12.2021).

3. Про затвердження Положення про державну експертизу в сфері криптографічного захисту інформації : Наказ; Адміністрація Держспецзв'язку від 23.06.2008 № 100 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/z0651-08 (дата звернення: 20.12.2021).

Скирда Антон Вячеславович – студент групи УБ-21м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: skirdaanton1@gmail.com.

Skyrda A.V. – student, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: skirdaanton1@gmail.com