***В. С. Волошин,*** *к.**е.**н.*

*Національний університет водного господарства та природокористування*

**МЕХАНІЗМИ ЗАХИСТУ ЕКОНОМІЧНОЇ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ЕЛЕКТРОННИХ КЛЮЧІВ**

Проблема захисту економічної інформації з використанням електронних ключів є надзвичайно поширеною в наш час. Ос-новною передумовою, при цьому, стало швидкий розвиток ін-формаційних та електронних технологій, які з одної сторони дозволяють створювати новітні продукти, а з іншої – починають створювати проблеми щодо захисту власних електронних доку-ментів та даних.

Суб’єктами, на яких проблема справляє негативний вплив є учасники електронного документообігу – користувачі послуг електронного цифрового підпису (ЕЦП), зокрема фізичні та юридичні особи незалежно від форми власності [1]. Слід зазна-чити, що центри сертифікації ключів виконують функції техно-логічного посередника у системі електронного документообігу, учасниками якої можуть бути суб’єкти господарювання та орга-ни державної влади [2].

На сьогоднішній день електронні ключі широко застосову-ється у наступних галузях:

– підприємницької діяльності – для внутрішнього викорис-тання та врегулювання відносин у системі B2B (бізнес для бізнесу);

– у суспільному житті – для перевірки надійності джерел подачі інформації у системі C2C (споживач для споживача);

– взаємовідносин бізнесу і населення та держави – B2PR (бізнес для суспільних відносин) та B2G (бізнес для держави);

– державного управління – у відомчих та міжвідомчих си-стемах документообігу, державних реєстрах;

– банківського сектору.

Взагалі, електронний цифровий підпис – це вид електронного підпису, отриманий у результаті криптографічного перетворен-ня набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його ці-лісність та ідентифікувати особу [3]. Схеми побудови цифро-вого підпису можуть бути сформовані на основі алгоритмів симетричного або асиметричного шифрування.

Визначимо методи захисту, які застосовуються до електрон-них даних економічних систем:

– маркування файлів зі списками авторизованих користувачів;

– встановлення паролів для потенційного користувача;

– захист від електромагнітного випромінювання,

– шифрування інформації, що надсилається по каналах зв’язку;

– фізичне блокування кімнати, що містить комп’ютер;

– створення резервних копій;

– використання ліцензійного програмного забезпечення. Систематизуємо основні механізми захисту економічної ін-

1. формації з використанням електронних ключів. Економічний механізм – полягає у виділенні необхідної кількості фінансових ресурсів для вирішення питань безпеки. Цей принцип поширюється на будь-який аспекти економічної системи, та дозволяє знизити помилки розробки та налагоджен-ня програмного забезпечення доступу до даних. При цьому за-стосовуються такі методи, як інтерактивне інспектування про-грамного забезпечення та фізичний огляд обладнання, що реа-лізує механізми захисту.
2. Механізм заборони доступу до інформації – по замовчу-ванню усім особам заборонено доступ, крім тих, які пройшли ідентифікацію з використанням електронних ключів.
3. Загальносистемний контроль доступу – кожний елемент такої системи повинен взаємодіяти з іншими чітко дотримую-чись встановлених інструкцій.
4. Відокремлення механізмів захисту від захисних ключів – захист економічної інформації не повинен залежати від незнан-ня потенційних зловмисників, а, скоріше, від наявності конкрет-них, більш надійно захищених ключів або паролів. Крім того, будь-якому недовірливому користувачеві може бути дозволено переконатись, що система, яку він збирається використовувати відповідає його цілям.
5. Мінімізація прав доступу – кожна програма та кожен ко-ристувач системи повинні працювати з найменшим набором можливостей, необхідних для виконання роботи. У першу чергу, цей принцип обмежує збитки, які можуть бути наслідком аварії або помилок. Це також зменшує кількість потенційних взаємо-дій між інформаційними системами та користувачами.

На сьогоднішній день програмна реалізація асиметричних криптографічних методів захисту можлива у PGP – комп’ютерна програма, також бібліотека функцій, що дозволяє виконувати операції шифрування цифрового підпису повідомлень, файлів та іншої інформації, поданої в електронному вигляді. PGP має без-ліч реалізацій, сумісних між собою і з багатьма іншими програ-мами (GnuPG, FileCrypt та інші) завдяки стандарту OpenPGP (RFC 4880), але вони мають різний набір функціональних мож-ливостей. Існують реалізації PGP для всіх найбільш поширених

операційних систем. Крім вільно розповсюджуваних реалізацій є ще й комерційні [4].

Використання даного програмного забезпечення дозволяє шифрувати електронні повідомлення з інтеграцією у поштові програми, наприклад Mozilla Thunderbird. При цьому використо-вуються два ключа – відкритий та закритий, за допомогою яких листи шифруються і дешифруються. Одержувач повинен знати відкритий ключ, для цього відправник може його розмістити у мережі Інтернет, наприклад на своєму сайті (сторінці у соціаль-них мережах), або розіслати звичайним листом всім потенцій-ним одержувачам електронних повідомлень. Даний механізм реалізований на основі асиметричних методів шифрування.

Наукова і практична новизна розглянутих механізмів захисту економічної інформації з використанням електронних ключів, полягає у систематизації основних сфер застосування ЕЦП та виявлення проблемних аспектів передачі даних у глобальних мережах. Застосування електронних цифрових підписів є не-від’ємною частиною економічного розвитку, а також важливим інструментом впровадження електронного врядування, що є особливо важливим у наш час проведення реформ пов’язаних із децентралізацією органів управління.

***Список використаних інформаційних джерел***

1. Закон України «Про електронні документи та електронний документообіг»: за станом на 03 вер. 2015 р. / Верховна Рада України. – Офіц. вид. – Київ : Парлам. вид-во, 2015.
2. Акредитований центр сертифікації ключів [Електронний ресурс]. – Режим доступу: [https://acskidd.gov.ua.](https://acskidd.gov.ua/) – Назва з екрана.
3. Електронний цифровий підпис // Центр інформаційних тех-нологій ІТ [Електронний ресурс]. – Режим доступу: [http://cit.ks.ua/usts/ecp.html.](http://cit.ks.ua/usts/ecp.html) – Назва з екрана.
4. Программное обеспечение для шифрования PGP [Електрон-ний ресурс]. – Режим доступу: [https://www.symantec.com/ru/ru/encryption.](https://www.symantec.com/ru/ru/encryption) – Назва з екрана.