

- вивчення зарубіжного досвіду протидії кіберзлочинності в окремо взятих країнах і надбань міжнародної спільноти, удосконалення механізму міжнародної взаємодії є важливим, адже більшість кіберзлочинів мають транснаціональний характер;
- кіберзлочинність сьогодні становить загрозу не тільки національній безпеці окремої держави, а загрожує людству загалом, саме тому зазначеній проблемі приділяється значна увага в багатьох державах;
- з огляду на сучасну ситуацію в державі та світі, Україна має постійно вдосконалювати методи боротьби з кіберзлочинністю, удосконалюючи чинне законодавство, у тому числі в галузі адміністративного права, враховуючи надбання окремих зарубіжних держав, міжнародної спільноти загалом, спрямовані на забезпечення кібербезпеки країни;
- важливим є прийняття Закону, який би врегулював основні засади забезпечення кібербезпеки України.

Література

1. Указ «Про введення в дію рішення Ради національної безпеки та оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» <http://zakon2.rada.gov.ua/laws/show/96/2016>.
2. Солодка О. М. Боротьба з комп'ютерною злочинністю як пріоритетний напрям забезпечення інформаційної безпеки України / О. М. Солодка // Актуальні проблеми управління інформаційною безпекою держави : зб. матеріалів наук.-практ. конф., 17 берез. 2010 р., м. Київ. – К.: Нац. акад. СБУ України, 2010. – С. 126-128
3. Перепелиця М. М. Кіберпростір і оперативно-розшукова діяльність / М. М. Перепелиця, О. В. Манджай // Вісн. Луган. держ. ун-ту внутр. справ. Луганськ, 2008. – Ч.1, Спец. вип. 1.
4. Кіберзлочинність у всіх його проявах: види, наслідки та способи боротьби [Електронний ресурс] <http://gurt.org.ua/articles/34602/>.

Електронний цифровий підпис: персоніфікація та захист

Олашина А.О.

викладач правознавчих дисциплін
ДВНЗ ОКЕПГРБ

Можливість захистити свої електронні дані в епоху достатньо стрімкого розвитку інформаційних технологій є не тільки абстрактною можливістю, «умовною опцією», яка використовується, а й вже сучасним необхідним правовим аспектом гарантії належного збереження електронних документів з урахуванням їх законної юридичної сили.

Ст. 8 Закону України "Про електронні документи та електронний документообіг" передбачає, що юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму, але задля того, щоб електронний документ відповідав вимогам, які висуваються чинним законодавством та мав статус такого, що має законну юридичну силу, він повинен бути підписаний електронним цифровим підписом [1].

Задля того, щоб визначитись в чому полягає суттєва відмінність між електронним цифровим підписом та електронним підписом, звернемось до Закону України «Про електронний цифровий підпис», який і надає визначення. Так, електронний підпис – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних [2]. Тобто, електронний підпис, на відміну від електронного цифрового підпису є таким, що не захищає особисті дані особи, він може виявлятися у згоді особи з правилами та умовами певного сайту, у погодженні відповідної особи з передачею її особистих даних третій особі, наприклад, при вчиненні online-замовлення, тобто електронний підпис не створює підстав задля створення умов персоніфікованого захисту даних відповідної особи.

Електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа [2]. На відміну від електронного підпису, електронний цифровий підпис (далі – ЕЦП) дає можливість не тільки ідентифікувати особу, що використала цей підпис, але й захистити зміст даних, які знаходяться у документі, захищеному ЕЦП. Використання ЕЦП вже створює умови для

якісного захисту підписаних даних, що унеможливорює перегляд захищених даних третіми особами. В ЄС електронний цифровий підпис називають «advance electronic signature», тобто «покращений електронний підпис».

Як і власноручний, електронний цифровий підпис дозволяє ідентифікувати особу, яка підписується, гарантує те, що інформація жодним чином не потрапить до третьої особи без дозволу на це «власника» і виступає гарантом аутентифікації, тобто, документ, що підписаний ЕЦП не може зазнати будь-якого корегування з боку третіх осіб.

На відміну від рукописного підпису, який може бути підроблений, бо має фізичну природу, що дає підстави для можливої фальсифікації підпису, електронний цифровий підпис має логічну природу, що виявляється в послідовності символів, що дає можливість пов'язати автора документа із змістом документа та одночасно власником електронного цифрового підпису без додаткової перевірки, зважаючи на чіткий та врегульований механізм дії ЕПЦ. Логічний характер електронного цифрового підпису надає можливість уникати будь-якої залежності із матеріальним аспектом природи документа. Електронний цифровий підпис дає можливість визначати автора документа, незважаючи на відсутність власноручного підпису особи, гарантуючи при цьому справжність авторства. Електронний цифровий підпис на відміну від електронного, має ряд таких переваг:

- персоніфікація – математичний аналіз, що використовується при накладанні ЕЦП, створюючи унікальну послідовність символів ключа дає можливість не тільки захистити дані підписувача, але й захистити та підтвердити авторство електронного документа.

- високі захисні властивості ЕЦП – завдяки логічній природі ЕЦП та структурному математичному аналізу, що використовується при накладанні ЕЦП, унеможливується використання електронних даних третьою особою без згоди на це підписувача.

- унікальність кожного ключа – кожен ключ має особистий, неповторний математичний ряд, який надає можливість підписувачу бути впевненим, що його електронні дані надійно захищені і не будуть використані особою, в якій відсутня інформація стосовно ключа.

- аутентифікація ключа – дає можливість захистити електронний документ від внесення будь-яких змін, таку можливість має тільки особа-підписувач.

- дематеріалізація – ЕЦП ніяким чином не залежить від об'єктів матеріального світу, бо завдяки своїй цифровій та логічній природі надає можливість сторонам підписати договір навіть на відстані.

Звернемо увагу, що у ст. 1 закону України «Про електронний цифровий підпис» зазначається, що компрометація особистого ключа – будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа [2]. В свою чергу до подій, пов'язаних з компрометацією ключів підписувачів, відносяться наступні: втрата носіїв, на які записані особисті ключі; втрата носіїв, на які записані особисті ключі, з наступним виявленням; звільнення співробітників, що мали особисті ключі; порушення правил зберігання особистих ключів; виникнення підозр на несанкціоноване застосування особистого ключа; втрата контролю щодо особистого ключа через компрометацію коду доступу до носія особистого ключа; випадки, коли не можна вірогідно встановити, що відбулося з носіями, що містять ключову інформацію (у тому числі, випадки, коли носій вийшов з ладу й доказово не спростована можливість того, що даний факт відбувся в результаті несанкціонованих дій зловмисника). З чого вбачається необхідним звернути увагу на те, що не правом, а обов'язком підписувача є збереження особистого ключа у таємниці, інформація, яка зберігається особою та потребує надійного захисту за умови дії сучасних інформаційних технологій нажалі все ж таки має можливість бути отриманою особою, яка не має права законного володіння такою інформацією. Електронний цифровий підпис теж може бути підданий фальсифікації. Щоб його фальсифікувати, зловмисник повинен заволодіти доступом до закритого ключа. У таких випадках говорять про компрометацію закритого ключа, з якої випливає компрометація електронного підпису.

Електронний цифровий підпис, беручи до уваги стрімкий розвиток сучасних технологій, є не тільки своєрідною «умовністю», яку необхідно використовувати, а надійний спосіб збереження та перегляду електронних документів. Електронний цифровий підпис надає можливість використовувати, змінювати та передавати інформацію в електронному вигляді, зберігаючи при цьому авторство та змістовність.

Література:

1. Про електронні документи та електронний документообіг : закон України від 22.05.2003 № 851-IV [Електронний ресурс]. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/851-15> – Назва з екрану.
2. Про електронний цифровий підпис: закон України від 22.05.2003 № 852-IV [Електронний ресурс]. – Режим доступу : <http://zakon0.rada.gov.ua/laws/show/852-15> – Назва з екрану.