УДК 340.5
DOI https://doi.org/10.32782/2524-0374/2023-11/91

ЮРИДИЧНІ РИЗИКИ КОМПРОМЕТАЦІЇ КВАЛІФКОВАНОГО ЕЛЕКТРОННОГО ПІДПИСУ

LEGAL RISKS OF COMPROMISING A QUALIFIED ELECTRONIC SIGNATURE

Костенко О.В., д.філос. (Ph.D.) з юр. н.,
завідувач наукової лабораторії теорії цифрової трансформації і права
наукового центру цифрової трансформації і права
Державна наукова установа «Інститут інформації, безпеки і права
Національної академії правових наук України»

Прокопович-Ткаченко Д.І., к.т.н.,
в.о. завідувача кафедри кібербезпеки та інформаційних технологій
Університет митної справи та фінансів

Флоров С.В., к.т.н., доцент,
доцент кафедри кібербезпеки та інформаційних технологій
Університет митної справи та фінансів

Дане дослідження містить важливу інформацію про юридичні наслідки компрометації особистого ключа електронного підпису, про форми та види компрометації, а також про актуальні проблеми, які потребують вирішення. Автор ретельно досліджує правові наслідки компрометації особистого ключа електронного підпису, визначає достатній актуальний огляд типів і форм такої компрометації, а також нагальні проблеми, які потребують вирішення в сфері електронних довірчих послуг, а також формулює правові наслідки. які можуть виникнути внаслідок компрометації та пропонує практичні заходи щодо запобігання таким порушенням. Розглянуто такі юридичні та техніко-юридичні властивості кваліфікованого електронного підпису як: кваліфікована електронна довірча послуга; аналог власноручного підпису; цифрова річ; атрибут ідентифікації та автентифікації; програмний засіб (ключ) доступу до інформаційно-комунікаційних систем; невід'ємний та обов'язковий атрибут електронного документа.

У дослідженні детально визначено випадки компрометації ключа кваліфікованого електронного підпису представника державної установи: на період його відсторонення від виконання посадових обов'язків у разі вчинення ним кримінального правопорушення; на період відсторонення працівника від виконання посадових обов'язків у відповідності до норм Кодексу законів про працю; на період відпустки та його непрацездатності підтвердженої листком непрацездатності або відповідними медичними довідками. Також ситуації пов'язані: із випадками підробки, зміни електронного документа або використання такого електронного документа як справжнього; випадками застосування особистого ключа кваліфікованого підпису у разі його застосування для несанкціонованого доступу та втручання в роботу інформаційно-комунікаційних систем, а також за настанням обставин непереборної сили в наслідок бойових дій, евакуації, епідемій, інших непередбачуваних обставин, що створюють умови несанкціонованого доступу невстановлених осіб до особистих ключів кваліфікованих електронних підписів.

Це дослідження є актуальним посібником для юристів, яким потрібно орієнтуватися в складному юридичному середовищі що стосується цифрової безпеки, електронного підпису та електронних довірчих послуг.

Ключові слова: компрометація, компрометація електронного підпису, незаконне використання, юридичні наслідки компрометації, підробка документів, недійсність електронних правочинів, незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж.

This study contains valuable information about the legal consequences of compromising a personal electronic signature key, the forms and types of compromise, and the current issues that need to be addressed. The study provides answers to the following questions: what legal consequences may arise because of compromising a qualified electronic signature and how to prevent the compromise of a personal electronic signature key.

Compromise of a qualified electronic signature may have serious legal consequences, such as invalidation of a signed document, loss of confidence in electronic transactions, and may contain signs of offenses under the Criminal Code of Ukraine.

Compromise of a qualified electronic signature may have the following dangers:

Invalidity of the signed document: compromise may result in the invalidity of the signed document because the signature was obtained by illegal means or changed without the signature owner's permission.

Loss of trust in electronic transactions: Compromise can undermine trust in electronic transactions because the signature owner may lose control of his or her private key, which can lead to unauthorized use of his or her identity.

Document forgery: compromising a key can lead to document forgery, as attackers can use the key to create fake documents.

Unauthorized access to information: compromising a key can allow attackers to gain unauthorized access to confidential information stored by a government agency.

Illegal use of the key: compromising a key can lead to the illegal use of the key to sign documents or perform other actions on behalf of the key holder.

Criminal offenses: the compromise of a qualified electronic signature may contain signs of a criminal offense that has led to or facilitated unlawful interference with the operation of automated electronic computers, their systems or computer networks.

The article contains the types of prevention of compromise of the private key of a qualified electronic signature, such as maintaining access to the private key information, preventing inactivity of the signatory or illegal activities of third parties regarding illegal access to a qualified electronic signature and information and communication systems, using strong passwords, encrypting key media and restricting access to them, and using secure networks and software.

Key words: compromise, compromise of an electronic signature, illegal use, legal consequences of compromise, forgery of documents, invalidity of electronic transactions, illegal interference with the operation of automated electronic computers, their systems or computer networks.

Постановка проблеми. Масштабне застосування державних електронних сервісів та електронних довірчих послуг в Україні генерує низку правових ризиків порушення законодавства, які мають різні юридичні наслідки. Визначення юридичних наслідків компрометації кваліфікованого електронного підпису і є актуальною проблемою, яка потребує вирішення.

Мета статті. Сформувати форми і види компрометації кваліфікованого електронного підпису та визначити юридичні наслідки компрометації.

Виклад основних положень. З'ясуємо що таке компрометація кваліфікованого електронного підпису та які норми законодавства України регулюють це питання.

Трактування поняття «компрометація кваліфікованого електронного підпису».

1. Поняття Компрометація кваліфікованого електронного підпису у законодавстві України.

Компрометацію електронного підпису або електронного ключа відповідно до п. 26 ст. 1 Закону України «Про електронні довірчі послуги» (далі – Закон 2155-VIII) [1] визначено, що «компрометація особистого ключа – будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа». Зазначене визначення створює підстави довільного трактування вказаної норми закону. Частиною 4 ст. 18 Розділу IV цього ж закону встановлено, що кваліфікований електронний підпис має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису, тобто електронний підпис є аналогом власноручного.

Задля з'ясування чіткого визначення сутності поняття «компрометація кваліфікованого електронного підпису» проведемо дослідження такого питання починаючи з аналізу правового змісту поняття кваліфікованого електронного підпису, яке застосовується в різних нормативно-правових актах законодавства України, що дасть можливість встановити ознаки легітимного або протиправного його використання і визначитися зі змістом компрометації.

Законом 2155-VIII встановлено визначення особистого ключа, а також три градації електронного підпису: електронний підпис, удосконалений електронний підпис та кваліфікований електронний підпис.

Згідно з п. 23 ст. 1 Закону 2155-VIII, кваліфікований електронний підпис – удосконалений електронний підпис, який створюється з використанням «засобу кваліфікованого електронного підпису» і базується на «кваліфікованому сертифікаті відкритого ключа».

Відповідно до абз. 2 п. 2 ст. 17 Закону 2155-VIII органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності, державні реєстратори, нотаріуси та інші суб'єкти, уповноважені державою на здійснення функцій державного реєстратора, для засвідчення чинності відкритого ключа використовують лише кваліфікований сертифікат відкритого ключа та виключно засоби кваліфікованого електронного підпису чи печатки. Тобто використання будь-яких видів електронних підписів в органах державної влади та органах місцевого самоврядування, крім кваліфікованих електронних підписів законодавством не передбачено.

Виходячи з походження, компетенції та порядку використання електронного ключа, існують декілька наукових підходів до визначення актуального поняття «компрометація кваліфікованого електронного підпису», як комплексу будь-яких явних або неявних подій та/або дій (втрата, розголошення, крадіжка, несанкціоноване копіювання тощо) з даними кваліфікованого електронного підпису та засобами криптографічного захисту інформації, що призвела або може призвести до несанкціонованого розголошення, зміни, знищення, блокування, перехоплення, копіювання та використання особистого ключа кваліфікованого електронного підпису, а також інформації, яка обробляється та передається за його допомогою. Явною компрометацією особистого ключа кваліфікованого електронного підпису є втрата доступу до інформації особистого ключа кваліфікованого електронного підпису, за участю або бездіяльністю підписувача або третіх осіб без застосування інформаційно-комунікаційних технічних засобів. Неявною компрометацією особистого ключа кваліфікованого електронного підпису є втрата доступу до інформації особистого ключа кваліфікованого електронного підпису із застосуванням будь-яких технічних засобів без відома та участі підписувача» [2].

Як вказувалося вище, п. 26 ст. 1 Закону 2155-VIII не надає визначення які саме об'єкти або суб'єкти правових відносин вчиняють будь-які події та/або дії, що призводять або можуть призвести до несанкціонованого використання особистого ключа, а з іншого боку її невизначеність створює підстави довільного трактування вказаної норми закону.

2. Поняття Компрометація кваліфікованого електронного підпису: техніко-юридичні аспекти.

Українські технічні спеціалісти в галузі захисту інформації запровадили кілька варіантів визначення «компрометація», як техніко-юридичного терміну. Перше визначення запроваджено Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України у 1999 році при створені НД ТЗІ 1.1.-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» застосовано термін «компрометація» як «компрометація (compromise) – це порушення політики безпеки; несанкціоноване ознайомлення» [3]. Дане визначення «компрометації» спрямоване на врегулювання деструктивних подій в системі безпеки, пов'язаних із порушенням чітких правил використання цифрових підписів. Проте, таке визначення не поширюється на відносини, що відбуваються із використанням особистого ключа поза межами визначеними політикою безпеки, а самі політики безпеки можуть суттєво різнитися. Також, така дефініція не пояснює визначення «несанкціоноване ознайомлення».

Друге визначення акцептовано наказом Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації» в якому визначено більш розширене поняття компрометації – як будь-який випадок (втрата, розголошення, крадіжка, несанкціоноване копіювання тощо) з ключовими документами (ключовими даними) та засобами криптографічного захисту інформації, який призвів (може призвести) до розголошення (витоку) інформації про них, а також інформації, яка обробляється та передається [4].

3. Властивості кваліфікованого електронного підпису.

Враховуючи зазначені вище нормативно-правові акти та новели національного законодавства так як, *ст. 177 Цивільного кодексу України яка передбачає, що об'єктами цивільних прав є речі, гроші, цінні папери, цифрові речі, майнові права, роботи та послуги, результати інтелектуальної, творчої діяльності, інформація, а також інші матеріальні та нематеріальні блага, а також ст. 179-1 ЦК України, якою встановлено,* що *цифровою річчю є благо, що створюється та існує виключно у цифровому середовищі та має майнову цінність,* кваліфікований електронний підпис набуває наступні юридичні та техніко-юридичні властивості:

- кваліфікована електронна довірча послуга;
- нематеріальний (електронний) аналог власноручного підпису як невід'ємна складова електронного документа;
- цифрова річ, як благо, що створюється та існує виключно у цифровому середовищі та має майнову цінність;
- атрибут ідентифікації та автентифікації підтвердження та встановлення електронної ідентифікації та автентифікації фізичної або юридичної особи;
- програмний засіб (ключ) доступу до інформаційно-комунікаційних систем в яких передбачено такий вид доступу;
- невід'ємний та обов'язковий атрибут електронного документа, який має юридичну значимість відповідно до законодавства України.

Як відомо, в Україні функціонує багато державних

інформаційно-комунікаційних систем таких як «Дія», електронні реєстри Міністерства юстиції України, Державної податкової служби України, Центральної виборчої комісії, Державної міграційної служби України, Національного банку України, Державної казначейської служби України, низки банків, регіональних електронних ресурсів тощо. Всі вони застосовують обіг електронних документів різних видів, а доступ до даних забезпечується ідентифікаційними атрибутами [15; 16] – кваліфікованим електронним підписом, Bank-ID тощо. Тобто кваліфікований електронний підпис крім безпосередньо функції «власноручного підпису» має додаткову важливу функцію – атрибута автентифікації та ідентифікації фізичної або юридичної особи.

Законом 2155-VIII визначено поняття автентифікації та ідентифікації особи, а також підписувача – фізичної особи, яка створює електронний підпис.

Пунктом 2 ст. 12 цього ж закону встановлено зобов'язання користувачів електронних довірчих послуг, однак, законодавством не передбачено жодних заходів державного примусу за порушення або невиконання зобов'язань користувача електронних довірчих послуг.

Статтею 25 Закону 2155-VIII встановлено, що правочин, вчинений в електронній формі, може бути визнаний судом недійсним у разі, коли під час його вчинення використовувався кваліфікований електронний підпис чи печатка, кваліфікований сертифікат якого/якої не містить відомостей, передбачених частиною другою цієї статті, або містить недостовірні відомості.

Законом України «Про електронні документи та електронний документообіг» визначено, що електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством. Статтею 6 цього ж закону встановлено, що для ідентифікації автора електронного документа може використовуватися електронний підпис. Накладанням електронного підпису завершується створення електронного документа.

Різновиди компрометації кваліфікованого електронного підпису.

Специфічні проблеми надання електронних довірчих послуг в галузі електронного підпису, що пов'язані із компрометацією особистого ключа кваліфікованого електронного підпису, полягають у достатньо складній структурі та видах компрометації, у зв'язку із чим компрометація особистого ключа кваліфікованого електронного підпису поділяється на явну та неявну компрометацію. Розглянемо вказані види компрометації.

1. Явна компрометація кваліфікованого електронного підпису.

Явною компрометацією кваліфікованого електронного підпису слід вважати втрату доступу до інформації особистого ключа, що гарантовано підтверджується наявними фактами порушень політики безпеки та несанкціонованого ознайомлення із ключовою інформацією, отримання доступу та застосування кваліфікованого електронного підпису третіми особами.

В свою чергу, явну компрометацію кваліфікованого електронного підпису можливо поділити на:

− компрометацію кваліфікованого електронного підпису, що відбулася за участю або з волі підписувача;

− компрометація кваліфікованого електронного підпису, яка здійснена сторонніми особами без відома підписувача.

Так, до явної компрометації кваліфікованого електронного підпису, що відбулася за участю або за волею підписувача слід віднести наступні фактори:

− втрата (викрадення) ключових носіїв (USB-флеш-накопи́чувач, токени (token), компакт диск, зовнішній жорсткий диск тощо);

− викрадення кваліфікованого електронного підпису сторонніми особами;

− втрата ключів (кодів) від сейфів у момент зберігання в них ключових носіїв та втрата ключів (кодів) із наступним їх знаходженням;

− свідома або шляхом зловживання довірою передача кваліфікованого електронного підпису сторонній особі;

− зберігання особистого кваліфікованого електронного підпису у відкритому, незашифрованому вигляді, безпосередньо на HDD комп'ютера користувача;

− створення копій кваліфікованого електронного підпису та їх розміщення не на ключовому носію, на якому безпосередньо відбувалась генерація електронного ключа;

− використання створених копій кваліфікованого електронного підпису;

− використання скомпрометованого кваліфікованого електронного підпису, особою, що не має встановлених законом службових повноважень по займаній посаді;

− компрометація кваліфікованого електронного підпису, яка здійснена сторонніми особами без відома підписувача та доступ сторонніх осіб до ключової інформації;

− порушення цілісності печаток на сейфах із ключовими носіями у разі якщо застосовується процедура опечатування сейфів;

− доступу до ключових носіїв шляхом несанкціонованого копіювання;

− викрадення кваліфікованого електронного підпису в наслідок відповіді на електронний лист-запит, надісланий електронною поштою із ознаками шахрайства або підробки;

− виготовлення кваліфікованого електронного підпису за підробленими документами;

− підробка електронних документів;

− застосування скомпрометованого кваліфікованого електронного підпису для несанкціонованого доступу та втручання в роботу інформаційно-комунікаційних систем;

− застосування скомпрометованого кваліфікованого електронного підпису для повторного (дистанційного) формування сертифікатів за електронним запитом.

2. Неявна компрометація кваліфікованого електронного підпису.

На відміну від явної компрометації особистого ключа кваліфікованого електронного підпису неявна компрометація базується на подіях, що створили або створюють умови для компрометації особистого ключа кваліфікованого електронного підпису із використанням сторонніми особами технічних засобів, програмного забезпечення тощо. До неявної компрометації можливо віднести:

− виникнення підозри у користувача особистого ключа кваліфікованого електронного підпису або відповідального підрозділу на витік інформації щодо ключових даних;

− випадки коли неможливо достовірно встановити що саме відбулося з ключовими носіями (в тому випадку коли ключові носії вийшли з ладу і доказово не спростовують можливість того, що даний факт відбувся в результаті неконтрольованих дій сторонніх осіб);

− будь-які інші події, які дають привід вважати що ключова інформація стала відома або доступна стороннім особам;

− перехоплення спеціальними технічними засобами звукової інформації, електромагнітного або радіовипромінювання комп'ютерів, на яких обробляється інформація із застосуванням особистих ключів;

− перехоплення спеціальними технічними засобами, спеціалізованим або шпигунським програмним забезпеченням інформації, яка циркулює в Internet або локальній мережі, в яких обробляється інформація із застосуванням особистого ключа кваліфікованого електронного підпису.

Неявна компрометація із застосуванням технічних методів та пристроїв несанкціонованого доступу до особистого ключа кваліфікованого електронного підпису підписувачів на сьогодні більш обмежена у протиправних

можливостях через доволі складний механізм криптозахисту даних [11; 12; 13].

Компрометація кваліфікованого електронного підпису в органах державної влади та місцевого самоврядування, збройних силах, правоохоронних органах та судовій системі.

Чисельні випадки порушення законодавства в сфері довірчих послуг вимушені звернути нашу увагу на проблеми пов'язані із компрометацію кваліфікованого електронного підпису в органах державної влади, органах місцевого самоврядування, збройних силах, правоохоронних органах, органах зі спеціальним статусом та судовій системі.

1. Особливості застосування нормативних актів в сфері електронних довірчих послуг в Україні.

Згідно з абз. 2 п. 2 ст. 17 Розділу IV Закону 2155-VIII органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності, державні реєстратори, нотаріуси та інші суб'єкти, уповноважені державою на здійснення функцій державного реєстратора, для засвідчення чинності відкритого ключа використовують лише кваліфікований сертифікат відкритого ключа.

Порядок використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності регламентується постановою Кабінету Міністрів України від 19 вересня 2018 р. № 749 [5], Законом України «Про державну службу», Законом України «Про запобігання корупції».

Постановою Кабінету Міністрів України від 19 вересня 2018 р. № 749 (далі – постанова КМУ № 749 від 17.09.2018) визначено, що підписувачем в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності є представник державної установи – працівник державної установи, що створює електронний підпис для реалізації повноважень, спрямованих на набуття, зміну чи припинення прав та/або обов'язків фізичної або юридичної особи відповідно до закону.

Абзацом 2 п. 2 постанови КМУ № 749 від 17.09.2018 встановлено, що кваліфікований сертифікат відкритого ключа підписувача – представника державної установи є кваліфікований сертифікат відкритого ключа, в якому додатково до ідентифікаційних даних фізичної особи, яка є працівником державної установи, зазначаються ідентифікаційні дані відповідної державної установи (найменування та ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України).

Абзацом 4 п.2 постанови КМУ № 749 від 17.09.2018 визначено, що Державні установи та їх працівники для засвідчення чинності відкритого ключа використовують лише кваліфіковані сертифікати відкритих ключів.

Безпосереднім користувачем та власником кваліфікованих електронних підписів є відповідна Державна установа, яка отримує на договірних засадах такі кваліфіковані електронні довірчі послуги.

Відповідно до п.6 постанови КМУ № 749 від 17.09.2018 організація використання кваліфікованих електронних довірчих послуг у державній установі забезпечується відповідальним підрозділом відповідно, що виконує відповідні функції, або працівник, визначений рішенням такої установи (її керівника), на який покладено певні функції.

Пунктом 5 постанови КМУ № 749 від 17.09.2018 встановлено, що вимоги щодо ведення обліку підписувачів – представників державної установи, обліку засобів кваліфікованого електронного підпису, що застосовуються підписувачами – представниками державної установи, зберігання та знищення їх особистих ключів, а також надання кваліфікованому надавачу електронних довірчих послуг (далі – кваліфікований надавач) інформації, необхідної для скасування, блокування або поновлення кваліфікованих сертифікатів відкритих ключів підписувачів – представників державної установи, визначаються рішенням державної установи (її керівника), якщо інше не встановлено законом.

Відповідальність за організацію використання, у тому числі отримання, кваліфікованих електронних довірчих послуг у державній установі несе її керівник, якщо інше не встановлено законом.

Відповідно до ст. 12 Закону 2155-VIII, користувачі електронних довірчих послуг зобов'язані: забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа; невідкладно повідомляти надавача електронних довірчих послуг про підозру або факт компрометації кваліфікованого електронного підпису; не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування сертифіката відкритого ключа.

Отже, на орган державної влади, орган місцевого самоврядування, підприємство, установу та організацію державної форми власності як власника створених в установі кваліфікованих електронних підписів працівників державної установи покладається обов'язок повідомляти про його компрометацію для унеможливлення вчинення незаконних дій з використанням кваліфікованого електронного ключа та застосування процедури його скасування, блокування та поновлення кваліфікованих сертифікатів, як того вимагає ст. 25 Закону 2155-VIII.

2. Різновиди компрометації кваліфікованих електронних підписів в органах державної влади та місцевого самоврядування.

Окрему категорію складають наступні види компрометації кваліфікованого електронного підпису, які відбуваються з низки розповсюджених порушень організаційного, управлінського та кадрового характеру:

− компрометація кваліфікованого електронного підпису представника державної установи на період відсторонення державного службовця від виконання посадових обов'язків у разі вчинення ним корупційного правопорушення у відповідності до норм ч. 6 ст. 72 Закону України «Про державну службу» та відповідно до норм ст. 30–34 та ч. 5 ст. 65 Закону України «Про запобігання корупції»;

− компрометація ключа кваліфікованого електронного підпису представника державної установи на період його відсторонення від виконання посадових обов'язків у разі вчинення ним кримінального правопорушення у відповідності до норм ст. 154–158 Кримінального процесуального кодексу України;

− компрометація кваліфікованого електронного підпису представника органу державної влади, органу місцевого самоврядування, підприємства, установи та організації державної форми власності на період відсторонення працівника від виконання посадових обов'язків у відповідності норм ст. 46 Кодексу законів про працю [6];

− компрометація ключа кваліфікованого електронного підпису представника державної установи на період відпустки та його непрацездатності підтвердженої листком непрацездатності або відповідними медичними довідками;

− у відповідності до ст. 358 Кримінального кодексу України компрометація ключа кваліфікованого електронного підпису представника органу державної влади, органу місцевого самоврядування, підприємства, установи та організації державної форми власності пов'язана із випадками підробки, зміни електронного документа або використання такого електронного документа як справжнього;

− компрометація кваліфікованого електронного підпису представника органу державної влади у випадках

застосування особистого ключа кваліфікованого підпису відповідно до норм ст. 361–363 Кримінального кодексу України у разі його застосування для несанкціонованого доступу та втручання в роботу інформаційно-комунікаційних систем;

– компрометація кваліфікованого електронного підпису представника органу державної влади, органу місцевого самоврядування, підприємства, установи та організації державної форми власності за настанням обставин непереборної сили в наслідок бойових дій, евакуації, епідемій, інших непередбачуваних обставин, що створюють умови несанкціонованого доступу невстановлених осіб до особистих ключів кваліфікованих електронних підписів.

2.1. Щодо компрометації кваліфікованих електронних підписів представників державної установи на період відсторонення від виконання посадових обов'язків.

Відсторонення представника державної установи на підставі норм законодавства визначених ч. 6 ст. 72 Закону України «Про державну службу», ст. 30–34 та ч. 5 ст. 65 Закону України «Про запобігання корупції», ст. 46 Кодексу законів про працю, ст. 154–158 Кримінального процесуального кодексу України оформлюється відповідним наказом органу державної влади, органу місцевого самоврядування, підприємства, установи та організації державної форми власності. Даний наказ також доводиться до підрозділу або представника установи, відповідального за організацію використання кваліфікованих електронних підписів цієї установи (її керівника).

Згідно з наказом по державній установі про відсторонення представника державної установи від виконання посадових обов'язків та на підставі п. 6 та п. 12 постанови КМУ № 749 від 17.09.2018 відповідальний підрозділ або представник установи, відповідальний за організацію використання кваліфікованих електронних підписів цієї установи забезпечує взаємодію з кваліфікованим надавачем з питань використання кваліфікованих електронних довірчих послуг та подає кваліфікованому надавачу заяву про блокування або поновлення кваліфікованого електронного підпису підписувача.

Також відповідальний підрозділ (працівник) може фізично, шляхом вилучення в представника державної установи, носія особистого ключа кваліфікованого електронного підпису, обмежити використання і зберігання кваліфікованого електронного підпису посадових осіб, які мають права та обов'язки здійснювати владні повноваження та вчиняти юридично значимі дії.

2.2. Щодо компрометації кваліфікованих електронних підписів представників державної установи на період його відпустки або непрацездатності.

Це найпоширеніший вид компрометації в державних установах.

Відпустки надаються згідно з ст. 2 Закону України про відпустки, а ст. 4, 13–20, 25 цього ж закону визначено види відпусток.

Перебування представника державної установи у передбаченій законодавством відпусті оформлюється відповідним наказом органу державної влади, органу місцевого самоврядування, підприємства, установи та організації державної форми власності. Даний наказ також доводиться до підрозділу або представника установи, відповідального за організацію використання кваліфікованих електронних підписів цієї установи (її керівника), який, в свою чергу зобов'язаний вжити заходів передбачених п. 6 та п. 12 постанови КМУ № 749 від 17.09.2018.

Поняття працездатності, непрацездатності, обмеженої працездатності, тимчасової непрацездатності детально викладено у відповідному роз'ясненні Міністерства юстиції України [7].

Епідемія COVID-19 має чисельні випадки, коли представники державних установ або органів місцевого самоврядування, перебуваючи в стані різкого погіршення здоров'я або незадовільного морально-психологічного стану в наслідок захворювання, не завжди своєчасно відкривають лікарняне або просто повідомляють доступними засобами зв'язку керівництво установи про хворобу та втрату працездатності. Це впливає на неможливість своєчасного реагування підрозділами установи на організаційні та управлінські процеси, пов'язані як із персоналом так із організацію використання кваліфікованих електронних підписів установи передбачених п. 6 та п. 12 постанови КМУ № 749 від 17.09.2018 та упередженням можливої компрометації особистих ключів кваліфікованого електронного підпису представників державної установи.

Щодо компрометації юридичні наслідки факту компрометації кваліфікованого електронного підпису.

1. Юридичні властивості кваліфікованого ключа електронного підпису.

Частиною 4 ст. 18 Розділу IV Закону 2155-VIII визначено, що кваліфікований електронний підпис має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису.

Відмінність від звичайного власноручного підпису, який накладається на паперові документи, кваліфікованого електронного підпису полягає виключно у їх природі існування та процесах застосування. Власноручний підпис зазвичай накладається на документ шляхом фізичної дії, яку вчиняє безпосередньо фізична особа за допомогою певних фізичних приладь для письма. Тобто це її ідентифікаційний атрибут, який фізична особа застосовує для фізичної фіксацій свого волевиявлення. Власноручний підпис має фізичну (матеріальну) природу і виготовляється із застосуванням фізичних (матеріальних) інструментів.

Природа кваліфікованого електронного підпису та особистого ключа кваліфікованого електронного підпису носить нематеріальний (електронний) характер, тобто створений за результатом криптографічного перетворення електронних даних, з якими пов'язаний цей електронний підпис або особистий ключ, з використанням засобу кваліфікованого електронного підпису та особистого ключа, однозначно пов'язаного з підписувачем, і який дає змогу здійснити електронну ідентифікацію підписувача та виявити порушення цілісності електронних даних, з якими пов'язаний цей електронний підпис.

Причому у якості електронного підпису, за згодою сторін, може буди використано будь-які електронні дані (символи, електронні фото, електронні аудіо- або відеофайли, тексти тощо). Однак цей різновид електронних підписів не забезпечує цілісність електронних даних шляхом застосування алгоритмів криптографічного перетворення електронних, на відміну від удосконаленого та кваліфікованого електронного підпису.

Відповідно до матеріальної та нематеріальної природи підписів вони набувають як спільні властивості, так і індивідуальні.

Матеріальний власноручний підпис в Українському законодавстві застосовується для оформлення різних видів правочинів, а також для документообігу та створення офіційних юридично значимих документів органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності тощо.

Під офіційним документом слід розуміти документи, що містять зафіксовану на будь-яких матеріальних носіях інформацію, яка підтверджує чи посвідчує певні події, явища або факти, які спричинили чи здатні спричинити наслідки правового характеру, чи може бути використана як документи – докази у правозастосовній діяльності, що складаються, видаються чи посвідчуються повноважними (компетентними) особами органів державної влади, місцевого самоврядування, об'єднань громадян, юридичних

осіб незалежно від форми власності та організаційно-правової форми, а також окремими громадянами, у тому числі самозайнятими особами, яким законом надано право у зв'язку з їх професійною чи службовою діяльністю складати, видавати чи посвідчувати певні види документів, що складені з дотриманням визначених законом форм та містять передбачені законом реквізити.

2. Недійсність правочину (нікчемність).

Особа, яка вчиняє правочин, повинна мати необхідний обсяг цивільної дієздатності; волевиявлення учасника правочину має бути вільним і відповідати його внутрішній волі; правочин має вчинятися у формі, встановленій законом; правочин має бути спрямований на реальне настання правових наслідків, що обумовлені ним.

Недійсність правочину (нікчемність) в наслідок підроблення підпису в договорі визначено ч. 3 ст. 203 та ч. 1 ст. 215 Цивільного кодексу України. Зокрема Верховний Суд України в постанові від 22.04.2015 у справі № 6-48цс15 визначив, що правочин, укладений від імені реальної особи, підписаний не нею, а іншою особою, без волевиявлення реальної особи є недійсним (нікчемним) на підставі ч. 3 ст. 203 та ч. 1ст. 215 Цивільного кодексу України [14].

3. Підробка електронних документів із застосуванням скомпрометованих кваліфікованих електронних підписів.

Уразі коли за допомогою скомпрометованого кваліфікованого електронного підпису створюється посадова особа органу державної влади або органу місцевого самоврядування вчиняє дії із електронними документами, а саме змінює їх зміст чи атрибути, або знищує електронний документ, або створює «фіктивний» електронний документ, або документ підписується особою, що не має встановлених законом службових повноважень по займаній посаді. В цьому випадку електронний документ стає недійсним (нікчемним) і втрачає статус юридично значимих документів органу державної влади, органу місцевого самоврядування, підприємствами, установами та організаціями державної форми власності тощо.

Кримінальний кодекс України має відповідні норми визначені статтею 358 щодо підроблення документів, печаток, штампів та бланків, збут чи використання підроблених документів, печаток, штампів, а також статтею 366 щодо службового підроблення шляхом складання, видачі службовою особою завідомо неправдивих офіційних документів, внесення до офіційних документів завідомо неправдивих відомостей, інше підроблення офіційних документів. Вказані вище норми стосуються як матеріального підпису так і його нематеріального аналогу – електронного підпису.

4. Вчинення різних протиправних дій в інформаційно-комунікаційних системах із застосуванням скомпрометованих кваліфікованих електронних підписів.

Щодо компрометації особистого ключа кваліфікованого електронного підпису представника державної установи з метою його подальшого використання для несанкціонованого доступу та втручання в роботу інформаційно-комунікаційних систем.

Диспозиції статей ст. 361–363 Кримінального кодексу України визначають, що особистий ключ кваліфікованого електронного підпису користувача, можливо класифікувати як об'єкт (предмет або знаряддя) злочину, як технічний засіб несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, без якого такий доступ неможливий і використання скомпрометованого кваліфікованого електронного підпису для доступу до інформаційно-комунікаційної системи з подальшим створенням, зміною, видаленням (знищенням) електронних документів комплексно кваліфікується нормами ст. 203 та 215 Цивільного кодексу України та ст. 358, 361–363 Кримінального кодексу України [8; 9; 10].

Висновки. Сьогодні триває масштабна цифровізація, яка характерна широким використанням кваліфікованого електронного підпису. Компрометація кваліфікованого електронного підпису набула масового негативного явища як в органах державної влади так і в бізнесі. Це є один із ризиків Теорії опору інноваціям (IRT), атако ж формування негативного іміджу впровадження цифрових технологій. Підвищення заходів управлінського впливу, координація організаційних заходів, інформування про можливість настання відповідальності, в тому числі кримінальної, внаслідок нанесення шкоди шляхом компрометації електронного підпису, сприятиме зростанню якості інформаційної гігієни та кібербезпеки. В дослідженнях наведено більш розширене визначення компрометації кваліфікованого електронного підпису, а також перелік юридичних наслідків компрометації для застосування під час професійної підготовки державних службовців та службовців органів місцевого самоврядування, та інших категорій працівників організацій всіх форм власності.

ЛІТЕРАТУРА

1. Про довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2155-19.
2. Костенко О. В. Компрометація особистого ключа електронного підпису (правовий аспект). *International Journal of Innovative Technologies in Economy.* April 2018. 3(15). С. 15–21.
3. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : затв. наказом № 22 ДСТСЗІ СБУ від 28.04.1999.
4. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації : наказ Адміністрації ДССЗЗІ України від 20.07.2007 № 141 (зареєстровано в Міністерстві юстиції України від 30.07.2007 за № 862/14129). URL: https://zakon.rada.gov.ua/laws/show/z0862-07#Text.
5. 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 від 19 вересня 2018 р. № 749. URL: https://zakon.rada.gov.ua/laws/show/749-2018-%D0%BF#Text.
6. Кодекс законів про працю України : *Затв. Законом № 322-VIII від 10.12.1971 ВВР*. URL: https://zakon.rada.gov.ua/laws/show/322-08#Text.
7. Втрата працездатності. Міністерство юстиції України. URL: https://minjust.gov.ua/m/str_23359
8. Кримінальне право України: Загальна частина : підручник / за ред. В. Я. Тація, В. І. Тютюгіна, В. І. Борисова – 6-е вид., перероб. і доп. – К. : «Право», Харків, 2020. – 584 с.
9. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку. Узагальнення опрацьовано суддею Верховного Суду України М.І. Грицівим та головним консультантом управління вивчення та узагальнення судової практики Верховного Суду України В. В. Антощуком.
10. Науково-практичний коментар Кримінального кодексу України. Станом на 20 травня 2020 року. / За заг. ред. Копотуна І. М. – Київ: Видавничий дім «Професіонал», 2020. – 864 с.
11. Pellegrini A., Bertacco V., Austin T. Fault-Based Attack of RSA Authentication. URL: https://web.archive.org/web/20170814063603/http://web.eecs.umich.edu/~valeria/research/publications/DATE10RSA.pdf.
12. Genkin D., Shamir A., Tromer E. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. URL: https://link.springer.com/chapter/10.1007/978-3-662-44371-2_25
13. Mike Just, Paul C. van Oorschot Addressing the Problem of Undetected Signature Key Compromise. URL: https://www.ndss-symposium.org/wp-content/uploads/2017/09/Addressing-the-Problem-of-Undetected-Signature-Key-Compromise-Mike-Just.pdf.

14. Постанові Верховного Суду України від 22.04.2015 у справі № 6-48цс15. URL: https://verdictum.ligazakon.net/document/43801777?utm_source=biz.ligazakon.net&utm_medium=news&utm_content=bizpress01

15. Костенко О.В. Ідентифікація IoT: витоки проблеми правого регулювання управління ідентифікаційними даними. *Фаховий науковий журнал «Juris Europensis Scientia»*. Чернівці. 2021. № 1. С. 77-83.DOI: https://doi.org/10.32837/chern.v0i1.177.

16. Костенко О.В. Управління ідентифікаційними даними: правове регулювання та класифікація. *Науковий журнал «Молодий вчений»*. 2021. № 3(91). С. 90-94. DOI: https://doi.org/10.32839/2304-5809/2021-3-91-21.