DOI: 10.18372/2410-7840.22.14658
УДК 004.56:342.9

ПРАВОВІ АСПЕКТИ ЩОДО ПОНЯТТЯ «КОМПРОМЕТАЦІЯ ОСОБИСТОГО КЛЮЧА ЕЛЕКТРОННОГО ПІДПИСУ»

Олександр Корнейко, Олексій Костенко

Статтю присвячено визначенню поняття «компрометація особистого ключа електронного підпису» в контексті правової науки. Наведено, що хоча в науково-технічній літературі проблематика щодо компрометації особистого ключа електронного підпису та її видів представлена достатньо повно, але в юридичній літературі відсутнє єдине тлумачення цієї дефініції та правових наслідків компрометації. Показано, чому урегулювання правової невизначеності дефініції «компрометація особистого ключа електронного підпису» та своєчасне реагування права на ризики, які виникають або зумовлені компрометацією особистого ключа електронного підпису, є актуальною проблемою. Наведені приклади щодо цієї правової проблеми в контексті відповідних судових рішень. Показано, як існуючі проблеми в правовій моделі суспільно-правових відносин, що регулюють використання електронного підпису, формують недовіру до законодавства в сфері електронного підпису та сумніви до надійності електронних підписів, їх особистих ключів, цілісності та достовірності електронних документів, що підписані ними. Наведені приклади явної і неявної компрометації особистого ключа електронного підпису та межі їх дії, а також правові наслідки компрометації. За результатами досліджень запропоновані відповідні визначення, які рекомендовано включити до існуючої редакції Закону України «Про електронні довірчі послуги».

Ключові слова: *електронний підпис, особистий ключ, компрометація.*

Вступ

На даний час так звана «цифровізація» (або за новішим сленгом «діджиталізація») є глобальною, загальносвітовою тенденцією. Сучасні інформаційні технології за рахунок широкого використання електронних даних у цифровій формі створюють нові можливості, що, в свою чергу, народжує нові суспільні відносини, які виникають між суб'єктами правовідносин під час: електронного обміну інформацією (Electronic Data Interchenge); електронного руху капіталу (Electronic Funds Transfer); електронної торгівлі (e-Trade); використання електронних грошей (e-cash); електронного маркетингу (e-market); електронного банкінгу (e-banking); електронної системи здоров'я (e-health) та в інших в сферах [1].

В сучасних інформаційних системах обмін інформацією здійснюється в формі цифрових даних, де надійність інформації під час обміну забезпечується завдяки застосуванню довірчих електронних послуг, а вимоги достовірності і цілісності інформації – завдяки застосування технології електронного підпису, коли відповідні електронні дані, сформовані за рахунок використання алгоритмів цифрового криптографічного захисту інформації, додаються до інших електронних даних (документу) і логічно з ними пов'язуються.

З метою правового врегулювання зазначених механізмів електронної торгівлі та застосування електронних підписів для забезпечення юридичної значимості електронних документів основні держави світу прийняли відповідні спеціальні закони у цій сфері. Так, Європейським парламентом та Радою у 1999 році прийнято Директиву «Про систему електронних підписів, що застосовується в межах Співтовариства», в США у 2000 році введено Закон «Про електронні підписи в глобальній і національній комерції», а у 2001 році Францією затверджено Декрет «Про електронний підпис» і Німеччиною – федеральний закон «Про цифрові підписи» [1].

Україна, гармонізуючи своє законодавство з міжнародним, у 2003 році також прийняла Закон «Про електронний цифровий підпис» (далі – Закон про ЕЦП). Але у 2016 році зазначену європейську Директиву було скасовано та на заміну їй прийшов Регламент ЄС 2014 року про електронну ідентифікацію, верифікацію та довірчі послуги (eIDAS). Тому Україна робить аналогічну рокіровку в профільному законодавстві й з 7 листопада 2018 року набрав чинність новий Закон України «Про електронні довірчі послуги», а Закон про ЕЦП втратив чинність [2].

В той же час більшість національних законів розроблювались як моделі загальних правил використання електронних підписів, а практичне застосування вказаних законодавчих актів виявили низку неврегульованих правових питань. Тому вітчизняні та зарубіжні науковці провели ряд наукових досліджень у сфері суспільних відносин, пов'язаних з використанням електронного підпису. Такими дослідженнями займались українські вчені Г. Козіел, А. Петрицький, В. Плескач, Л. Пономаренко, А. Шпірко, Л. Янчева, А. Локшин та ін., а серед іноземних вчених дану тему досліджували, наприклад, С. Масон, А. Тірі, М. Венбо, А. Петров, О. Беззубцев [1].

Однак ці дослідження у сфері адміністративного права фактично не зачепили проблеми, пов'язані з правовою невизначеністю дефініції «компрометація особистого ключа електронного підпису», як елемента понятійного апарату законодавства.

Більш детальним вивченням питань створення надійних механізмів визнання електронних підписів займались українські науковці І. Горбенко, О. Потій, О. Перевозчикова, С. Белов, Б. Погорелов, А. Мелащенко та ін., результати яких представлені, наприклад, в роботах [3-5]. Однак цими вченими проблема компрометації особистого ключа електронного підпису висвітлювалась виключно в технічному, а не в юридичному аспекті.

Таким чином, урегулювання проблеми правової невизначеності дефініції «компрометація особистого ключа електронного підпису» та своєчасне реагування права на ризики, які виникають або зумовлені компрометацією особистого ключа електронного підпису, є наразі актуальною проблематикою правової науки.

Метою дослідження є: на підставі аналізу профільної науково-технічної літератури та в контексті відповідних судових рішень дослідити правові проблеми та сформулювати пропозиції щодо формулювання дефініції «компрометація особистого ключа електронного підпису».

Виклад основного матеріалу дослідження. Необхідність створення нової дефініції «компрометація особистого ключа електронного підпису» зумовлена наявністю наступних причин [1].

По-перше, міжнародні законодавчі норми в галузі електронного підпису не мають чітких, загальноприйнятих визначень базового поняття «компрометація» стосовно електронного підпису. Термін «компрометація», в контексті «компрометація електронного підпису», застосовано у Типовому законі Комісії ООН з права міжнародної торгівлі (ЮНСІТРАЛ) «Про електронні підписи і Керівництво із прийняття рішень», прийнятого у Відні 5 липня 2001 року на 34-й сесії ЮНСІТРАЛ [6]. У ньому, в статті 57 поняття «ненадійний сертифікат» трактується як такий, особистий ключ якого «скомпрометовано» в наслідок втрати підписувачем контролю над ним. У США поняття «компрометація» визначено Національним інститутом стандартів і технологій (National Institute of Standards and Texchnology, NIST) як «*неавторизоване розкриття, модифікація, заміщення або використання конфіденційних даних (включаючи криптографічні ключові тексти та інші дані Центру Політики Безпеки (CSP) або неавторизоване розкриття, модифікація, заміщення або використання конфіденційних даних (наприклад, ключів, метаданих та іншої інформації, що стосується безпеки)*» [19].

По-друге, вітчизняне законодавство та нормативно-правові акти в сфері захисту інформації також по різному коментують дефініцію «компрометація».

Так, пунктом 26 статті 1 Закону України «Про електронні довірчі послуги» визначено, що «*компрометація особистого ключа – будь-яка подія, що призвела або може призвести до несанкціонованого доступу до особистого ключа*» [2].

Але в нормативно-правових актах сфери захисту інформації [7, 8], що розроблені Державною службою спеціального зв'язку та захисту інформації України (Держспецзв'язку), запроваджено декілька інших варіантів дефініції «компрометація».

Так, в НД ТЗІ 1.1-003-99 застосовано таке визначення «*компрометація (compromise) – це порушення політики безпеки; несанкціоноване ознайомлення*» [7]. Дане визначення спрямоване на врегулювання деструктивних подій в системі безпеки, пов'язаних із порушенням чітких правил використання електронних підписів, проте, воно не поширюється на відносини, що відбуваються із використанням особистого ключа по за межами визначеними політикою безпеки, а самі політики можуть суттєво різнитися [1]. Також, така дефініція не пояснює визначення «несанкціоноване ознайомлення».

Відповідним Положенням про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису визначено, що «*компрометація – 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*» [8]. На наш погляд, це найбільш вдале визначення поняття «компрометація», яке доцільно покласти в основу дефініції «компрометація особистого ключа електронного підпису» та закріпити на рівні законодавчого акту, що сприятиме чіткому застосуванню норм права [1].

По-третє, за останні роки збільшилось кількість правопорушень та злочинів, пов'язаних з електронними підписами, коли самі підписувачі створюють умови для компрометації особистого ключа електронних підписів й подальшого його незаконного використання.

Здебільшого такі злочини вчиняються в банківській сфері. Прикладом слугує низка кримінальних справ, фігуранти яких, будучи банківськими працівниками, нехтували правилами політик банківської безпеки, під різними приводами заволодівали особистими ключами електронних підписів своїх колег або підлеглих та організували схеми незаконного заволодіння коштами банківських клієнтів [9, 10].

Має місце також практика компрометації особистих ключів електронних підписів нотаріусів або реєстраторів під час вчинення ними правочинів. Так, непоодинокі випадки компрометації через неналежне зберігання та заволодіння особистим ключем нотаріуса або реєстратора, які призводять до незаконного відчуження майна та власності шляхом втручання в роботу Єдиного державного реєстру речових прав на нерухоме майно (ЄДРРПНМ) та Єдиного державного реєстру юридичних осіб та фізичних осіб-підприємців (ЄДРЮОФОП) [11].

Також, непоодинокі випадки заволодіння сторонніми особами особистих ключів електронних підписів керівників підприємств та головних бухгалтерів або отримання таких ключів в Акредитованих центрах сертифікації ключів за підробленими довіреностями з подальшим вчиненням фінансових злочинів [12].

По-четверте, існуючі норми законодавства в сфері електронного підпису не враховують різні види компрометації ключів електронного підпису. У зв'язку з цим, на основі аналізу наукових робіт та нормативних документів технічного характеру щодо електронного підпису, наприклад [4, 5, 13, 14], розглянемо можливі види та прояви компрометації особистого ключа електронного підпису.

Компрометація особистого ключа електронного підпису може бути явною та неявною [4, 5].

Явною компрометацією особистого ключа слід вважати втрату доступу до інформації особистого ключа, що гарантовано підтверджується наявними фактами порушень політики безпеки та несанкціонованого ознайомлення із ключовою інформацією [4, 5].

Явну компрометацію можливо розподілити на [4, 5]:

– компрометацію, що відбулася за участю або з волі підписувача;

– компрометація, яка здійснена третіми особами без відома підписувача.

Так, до явної компрометації особистого ключа, що відбулася за участю або за волею підписувача слід віднести наступні фактори [4, 5, 13, 14]:

– втрата ключових носіїв та втрата ключових носіїв із наступним їх знаходженням;

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

– свідома або шляхом зловживання довіри передача особистого ключа сторонній особі;

– порушення правил зберігання та знищення (після закінчення терміну дії) особистого ключа;

– зберігання особистого ключа у відкритому, незашифрованому вигляді, безпосередньо на жорсткому диску (HDD) комп'ютера користувача;

– неналежне зберігання пароля або PIN-коду до особистого ключа;

– викрадення особистого ключа в наслідок змови з особами, які мають право на його використання на законних підставах;

– порушення встановлених в організації правил використання і зберігання особистих ключів, розголошення мережевих паролів, паролів криптозахисту;

– компрометація особистого ключа, яка здійснена третіми особами без відома підписувала 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 особистого ключа в наслідок відповіді на запит, надісланий із ознаками шахрайства або підробки;

– виготовлення особистого ключа за підробленими документами.

На відміну від явної компрометації особистого ключа неявна компрометація базується на припущеннях або версіях подій, що створили або створюють умови компрометації особистого ключа електронного підпису з використанням сторонніми особами технічних засобів, програмного забезпечення тощо [1].

Так, до неявної компрометації можливо віднести [4, 5, 13, 14]:

– виникнення підозри 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 оброблюється інформація із застосуванням особистих ключів;

– звільнення співробітників, які мали доступ до ключової інформації;

– перехоплення спеціальними технічними засобами, спеціалізованим або шпигунським програмним забезпеченням інформації, яка циркулює в Internet або локальній мережі, в яких оброблюється інформація із застосуванням особистих ключів.

По-п'яте, неявна компрометація із застосуванням технічних методів та пристроїв несанкціонованого доступу до особистих ключів підписувачів на сьогодні більш обмежена у протиправних можливостях через доволі складний механізм криптозахисту даних, хоча в наукових публікаціях періодично демонструються можливості технічного, знеособленого доступу до ключів особистого електронного підпису [18].

По-шосте, проблеми пов'язані із складністю надання правової оцінки наслідків компрометації особистого ключа в період між реальним фактом компрометації та фактом її офіційного оголошення, із наступним блокуванням або скасуванням сертифікату особистого ключа. Саме протягом такого періоду існує ймовірність застосування скомпрометованого особистого ключа для вчинення дій, що мають юридичні наслідки [20].

По-сьоме, на сьогодні в законодавстві поняття компрометації особистого колюча електронного підпису фактично не має чіткого визначення та переліку подій або підстав, що дають можливість беззаперечно вважати їх компрометаційними, і, відповідно, базовими «маяками» для правознавців, які сьогодні оцінюють прецеденти порушення законодавства, пов'язані із використанням особистого ключа електронного цифрового підпису виключно в контексті статей 361-363 Кримінального кодексу України [15]. Диспозиції цих статей визначають, що особистий ключ підписувача, можливо класифікувати як 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 [16].

У той же час, дії або бездіяльність підписувача, які призвели до компрометації особистого ключа електронного підпису, як і поняття «компрометації особистого ключа електронного підпису» поки що не знайшли правової оцінки. Відсутність переліку базових ознак компрометації особистого ключа створює неоднозначність трактування правоохоронними органами, судами та адвокатурою ознак злочинів, що вчиняються із використанням електронного підпису, що, в свою чергу, створює умови для уникнення від покарання [17].

Отже, правова невизначеність у самих дефініціях «компрометація» та «компрометація особистого ключа електронного підпису», існуючі проблеми в правовій моделі суспільно-правових відносин, що регулюють сферу використання електронного підпису, формують в цілому недовіру до законодавства в сфері електронного підпису. Ця недовіра створює сумніви до надійності електронних підписів, цілісності електронних документів підписаних ними, достовірності правочинів вчинених нотаріусами та державними реєстраторами в електронному вигляді, незмінності інформації внесеної в ЄДРРПНМ та ЄДРЮОФОП, надійності угод та договорів, укладених в електронній формі тощо [1].

Зважаючи на викладене вище, авторами вважається за доцільне запровадити дефініцію «компрометація особистого ключа електронного підпису», та викласти її в наступній редакції: «*Компрометація особистого ключа електронного підпису – як будь-яка явна (не явна) подія, дія та/або бездіяльність (втрата, розголошення, крадіжка, несанкціоноване копіювання тощо) з даними особистого ключа та засобами криптографічного захисту інформації, що призвела або може призвести до несанкціонованого витоку особистого ключа, а також інформації, яка обробляється та передається за його допомогою.*

Явною компрометацією особистого ключа електронного підпису є втрата доступу до інформації особистого ключа, за участю або бездіяльності підписувача або третіх осіб без застосування технічних засобів.

Неявною компрометацією особистого ключа електронного підпису є втрата доступу до інформації особистого ключа із застосуванням будь-яких технічних засобів без участі підписувача».

Таке визначення, що містить загальне поняття компрометації та два деталізованих визначення явної та неявної компрометації, дозволить здійснювати більш якісну правову кваліфікацію суспільно небезпечних протиправних дій із використанням особистого ключа електронного підпису.

Вказане визначення дефініції «компрометація особистого ключа електронного підпису» у запропонованій вище редакції доцільно внести замість існуючого до пункту 26 статті 1 Розділу І існуючої редакції Закону України «Про електронні довірчі послуги» [2].

Значення суспільної небезпечності компрометації особистого ключа електронного підпису як матеріальної ознаки злочину полягає в тому, що вона, по-перше, є основним об'єктивним критерієм визнання діяння злочином; по-друге, дозволяє дати класифікацію злочинів за ступенем тяжкості; по-третє, визначає межу між злочином та іншими правопорушеннями; по-четверте, є однією з загальних засад індивідуалізації відповідальності і покарання [16].

Крім того, визначення «явна компрометація» сприятиме можливості надання юридичної оцінки вчинкам як володільця особистого ключа електронного підпису, так і третім особам, які ним заволоділи та несанкціоновано використовують. В той же час, використання поняття «неявна компрометація» дозволить детальніше класифікувати суспільно-небезпечні діяння, які скоюють стосовно особистого ключа підписувача або із його використанням в контексті статей 361-363 Кримінального кодексу України [15].

Висновки. Враховуючи проаналізовані підходи до визначення компрометації особистого ключа електронного підпису, її видів та характерних ознак, можливо зробити висновок, що відсутність повного законодавчого врегулювання такого суспільно небезпечного діяння як «компрометація особистого ключа електронного підпису» в сфері права впливає на стабільність інформаційних ресурсів держави та стан її кібербезпеки.

Отже, забезпечуючи чіткість законодавчої мови та визначеність правових норм, надана авторами нова законодавча дефініція «компрометація особистого ключа електронного підпису», яку доцільно включити до існуючої редакції Закону України «Про електронні довірчі послуги», сприятиме: правовому регулюванню суспільних відносин, пов'язаних з використанням електронного підпису; чіткій класифікації злочинів та правопорушень, вчинених із використанням особистого ключа електронного підпису; підвищить довіру до надійності електронних підписів та електронних документів підписаних ними, угод та договорів, укладених в електронній формі; стимулюватиме розвитку транскордонної електронної торгівлі та послуг.

ЛІТЕРАТУРА

[1]. О. Костенко, "Компрометація особистого ключа електронного підпису (правовий аспект)", *Інформація і право*, № 1(24), С. 72-80, 2018.

[2]. "Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII", *Відомості Верховної Ради України*, № 45, ст. 400, 2017.

[3]. Ю. Горбенко, І. Горбенко, *Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія*, Харк. нац. ун.-т радіоелектрон., ЗАТ Інт інформ. Технологій, Х. : Форт, 2010, 593 с.

[4]. І. Горбенко, Ю. Горбенко, *Прикладна криптологія. Теорія. Практика. Застосування : монографія*, Харк. нац. ун-т радіоелектрон., ЗАТ "Ін-т інформ. Технологій", Х. : Форт, 2012, 868 с.

[5]. А. Потий, Ю. Горбенко, А. Корнейко та ін., "EIDAS: Принципы предоставления доверительных электронных услуг и проблема интероперабельности", *Прикладная радиоэлектроника*, Т. 13, № 3, С. 252-260, 2014.

[6]. Типовой закон ЮНСИТРАЛ об электронных подписях. [Електронний ресурс]. Режим доступу: http://zakon0.rada.gov.ua/laws/show/995_937.

[7]. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99, наказ ДСТСЗІ СБУ від 28.04.1999 № 22. [Електронний ресурс]. Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/doccatalog/list?currDir=41640.

[8]. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису: наказ ДССЗЗІ України від 20.07.2007 № 141: зареєстровано в Міністерстві юстиції України 30.07.2007 за № 862/14129. [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0862-07.

[9]. Постанова Ленінського районного суду м. Кіровограда від 19 жовтня 2011 р. у справі № 1-463/11 [Електронний ресурс]. Режим доступу: http://www.reyestr.court.gov.ua/Review/20422029.

[10]. Розслідування 12016040730000533. [Електронний ресурс]. Режим доступу: http://www.gp.gov.ua/ua/erdr.html.

[11]. Ухвала Івано-Франківського міського суду Івано-Франківської області від 09 березня 2017 р. у справі № 344/3171/17. [Електронний ресурс]. Режим доступу: http://www.reyestr.court.gov.ua/Review/65214508.

[12]. Ухвала Печерського районного суду м. Києва від 14 березня 2017 р. у справі № 757/10916/16-к. [Електронний ресурс]. Режим доступу: http://www.reyestr.court.gov.ua/Review/56854252.

[13]. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи. [Електронний ресурс]. Режим доступу: www.dsyst.com/files/security-manual.doc.

[14]. Инструкция по обеспечению безопасности эксплуатации сертифицированных средств криптографической защиты информации. [Електронний ресурс]. Режим доступу: www.aksicom.ru/content/istr_skzi.pdf

[15]. Кримінальний кодекс України від 05.04.2001 № 2341-III, *Відомості Верховної Ради України*, № 25-26, ст. 131, 2001.

[16]. М. Бажанов, Ю. Баулін, В. Борисов та ін., *Кримінальне право України: Загальна частина: Підручник*, за ред. проф. М. Бажанова, В. Сташиса, В. Тація, 2е вид., перероб. і допов, К.: Юрінком Інтер, 2005, 480 с.

[17]. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних

машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку. [Електронний ресурс]. Режим доступу: http://www.scourt.gov.ua/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02/.

[18]. A. Pellegrini, V. Bertacco, T. Austin, *Fault-Based Attack of RSA Authentication*. [Electronic resource]. Onine access: https://web.eecs.umich.edu/~taustin/papers/DATE10-rsa.pdf.

[19]. *NIST SP 800-57 Part 3 Revision 1 Recommendation for Key Management*. [Electronic resource]. Onine access: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf.

[20]. M. Just, Paul C. Van Oorschot, *Addressing the Problem of Undetected Signature Key Compromise*. [Electronic resource]. Onine access: http://citeseerx.ist.psu.edu/viewdoc/download?doi =10.1.1.26.507&rep=rep1&type=pdf.

ПРАВОВЫЕ АСПЕКТЫ ОТНОСИТЕЛЬНО ПОНЯТИЯ «КОМПРОМЕТАЦИЯ ЛИЧНОГО КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ»

Статья посвящена определению понятия «компрометация личного ключа электронной подписи» в контексте правовой науки. Показано, что, хотя в научно-технической литературе проблематика по компрометации личного ключа электронной подписи и ее видов представлена достаточно полно, но в юридической литературе отсутствует единое толкование этой дефиниции и правовых последствий компрометации. Показано, почему урегулирование правовой неопределенности дефиниции «компрометация личного ключа электронной подписи» и своевременное реагирование права на риски, которые возникают или обусловленные компрометацией личного ключа электронной подписи, является актуальной проблемой. Приведены примеры этой правовой проблемы в контексте соответствующих судебных решений. Показано, как существующие проблемы в правовой модели общественно-правовых отношений, которые регулируют использование электронной подписи, формируют недоверие к законодательству в сфере электронного подписи и сомнения в надежности электронных подписей, их личных ключей, целостности и достоверности электронных документов, подписанных ними. Приведены примеры явной и неявной компрометации личного ключа электронной подписи и пределы их действия, а также правовые последствия компрометации. По результатам исследований предложены соответствующие определения, которые рекомендуется включить в существующую редакцию Закона Украины «Об электронных доверительных услугах».

Ключевые слова: электронная подпись, личный ключ, компрометация.

LEGAL ASPECTS OF THE DEFINITION «COMPROMISE OF THE PERSONAL KEY OF DIGITAL SIGNATURE»

The article is devoted to the definition of "compromise of the personal key of digital signature" in the context of law science. It is shown that although in the scientific and technical literature the problem of compromising the private key of digital signature and its types is presented quite fully, in the legal literature there is no single interpretation of this definition and the legal consequences of compromise. Examples of these definitions in various regulations of Ukraine and other countries are given. It is shown why the resolution of the legal uncertainty of the definition "compromise of digital signature private key" and timely response of the right to digital risks is an urgent problem of legal science. It is shown how the lack of a list of basic signs of personal key compromise in the legislation creates ambiguity in the interpretation by law enforcement agencies, courts and the bar of signs of crimes committed with the use of electronic signatures. It is shown how the existing problems cause distrust of the legislation in the field of electronic signatures, doubts about the reliability of electronic signatures and their private keys, the integrity and reliability of electronic documents signed by them. Examples of this legal problem in the context of relevant court decisions are given. Examples of explicit and implicit compromise of a private key of digital signature and their limits, as well as the legal consequences of compromise are given. Based on the results of the research, appropriate definitions are proposed, which are recommended to be included in the existing version of the Law of Ukraine "On electronic trust services". The authors conclude that this will contribute to: the legal regulation of public relations related to the use of electronic signatures; clear classification of crimes and offenses committed using an electronic signature personal key; increase confidence in the reliability of electronic signatures and electronic documents signed by them, agreements and contracts concluded in electronic form; will stimulate the development of cross-border e-commerce and services.

Keywords: digital signature, personal key, compromise.

Корнейко Олександр Васильович, кандидат технічних наук, професор, завідувач кафедри інформаційних технологій та кібербезпеки Національної академії внутрішніх справ, м. Київ.
E-mail: alex_korneiko@meta.ua.
Orcid ID: 0000-0002-1882-9680.

Корнейко Александр Васильевич, кандидат технических наук, профессор, заведующий кафедрой информационных технологий и кибербезопасности Национальной академии внутренних дел, г. Киев.

Korneiko Oleksandr, candidate of technical sciences, professor, head of the informatics technologies and cybersecurity academic department, National Academy of Internal Affairs, Kyiv, Ukraine.

Костенко Олексій Володимирович, аспірант Науково-дослідного інституту інформатики та права Національної академії правових наук України, м. Київ.
E-mail: antizuk@gmail.com.
Orcid ID: 0000-0002-2131-0281.

Костенко Алексей Владимирович, аспирант Научно-исследовательского института информатики и права Национальной академии правовых наук Украины, г. Киев.

Kostenko Oleksii, postgraduate student of the Research Institute of Informatics and Law, National Academy of Legal Sciences of Ukraine, Kyiv, Ukraine.