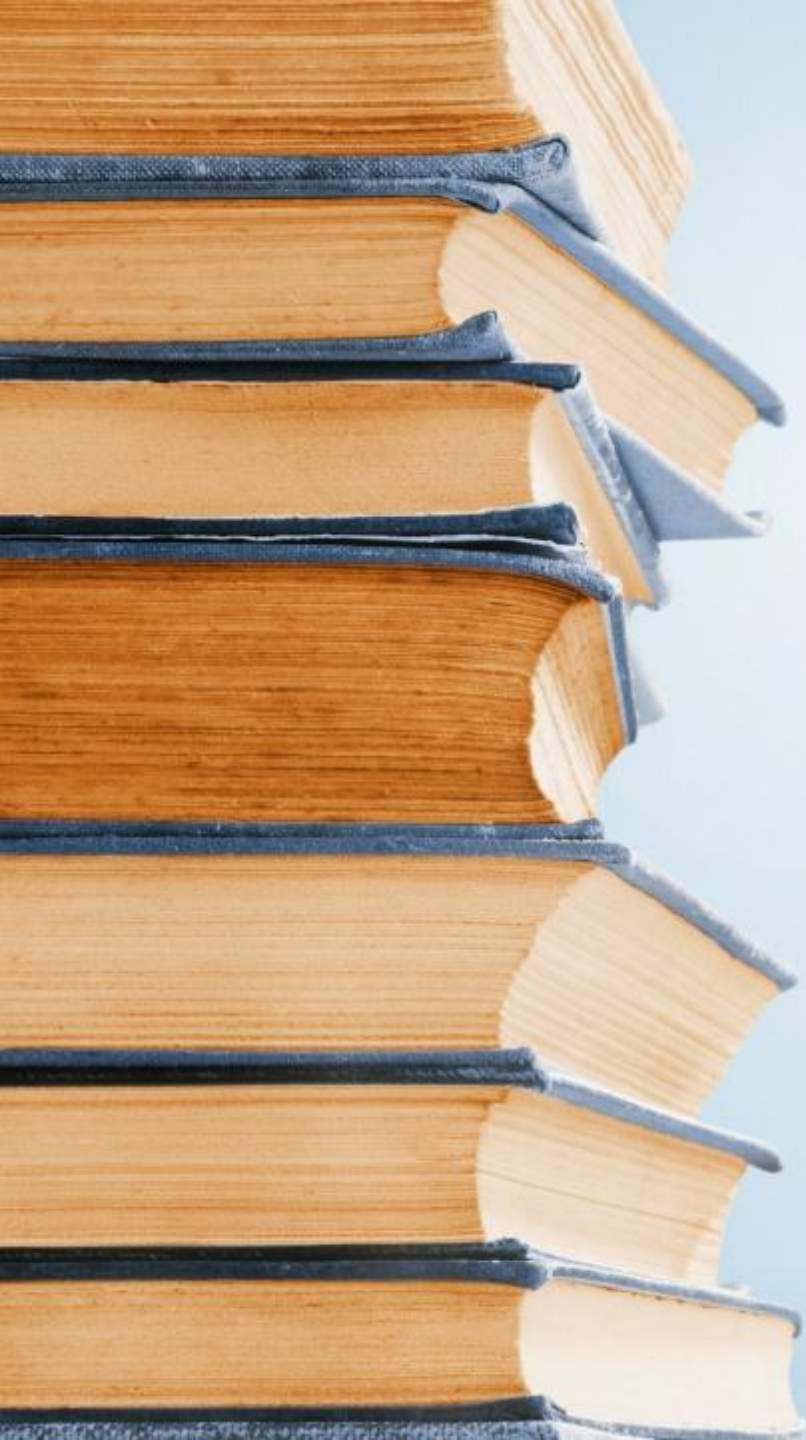




КОМПРОМЕТАЦІЯ ОСОБИСТОГО КЛЮЧА ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ (ПРАВОВИЙ АСПЕКТ)

Костенко О.В.

Український науково-дослідний інститут спеціальної
техніки та судових експертиз Служби безпеки України

правова невизначеність дефініції «Компрометація»

Проблема

несвоєчасне реагування права на ризики, які виникають або зумовлені компрометацією особистого ключа електронного цифрового підпису

правові наслідки компрометації особистого ключа електронного цифрового підпису

- Аналіз наукових джерел, публікацій іноземних країн та актів міжнародного права, що регулюють правовідносини в сфері електронного цифрового підпису, а також вітчизняної судової практики свідчать, про те, що увага приділяється виключно усуненню правових наслідків подій, що відбулися за фактом встановленої компрометації.
- За межами права залишається неоднозначність визначення самого поняття компрометації, правових наслідків та юридичних механізмів протидії цим наслідкам, які виникають на різних стадіях компрометації.

Компрометація ?



- Вперше термін «компрометація» в контексті «компрометація електронного підпису» застосовано у Типовому законі ЮНІСТРАЛ «Про електронні підписи і Керівництво із прийняття рішень», прийнятого у Відні 5 липня 2001 року на 34-й сесії ЮНІСТРАЛ.
- Статтею 57 Типового закону ЮНІСТРАЛ поняття «ненадійний сертифікат» трактується як такий, особистий ключ якого «скомпрометовано» в наслідок втрати підписувачем контролю над ним.
- Статтею 61 визначено, що в якості можливих факторів, які потрібно приймати до уваги при оцінці надійності постачальника сертифікованих послуг, розглядалися процедури анулювання сертифікатів на випадок коли криптографічні ключі можуть бути втрачені або «скомпрометовані».

- У 2015 році американським Національним інститутом стандартів і технологій (National Institute of Standards and Technology – NIST) надано визначення компрометації :
 - це 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)

А тим часом в Україні....

ЗУ «Про електронний
цифровий підпис», 2003 рік

Ст. 1

**Компрометація особистого
ключа – будь-яка подія
та\або дія, що призвела
або може призвести до
несанкціонованого
використання особистого
ключа**

ЗУ «Про довірчі послуги», 2017
рік

Ст. 26

Компрометація особистого
ключа – будь-яка подія
та\або дія, що призвела
або може призвести до
несанкціонованого
використання особистого
ключа

Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

НД ТЗІ 1.1.-003-99 «Термінологія в галузі захист інформації в комп'ютерних системах від несанкціонованого доступу»

компрометація (compromise) – це порушення політики безпеки; несанкціоноване ознайомлення

Державна служба спеціального зв'язку та захисту інформації України

Наказ від 20.07.2007 №141 «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису»

Компрометація - 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

Види компрометації

Явна компрометація

Неявна компрометація

ЯВНА КОМПРОМЕТАЦІЯ

відбулася за участю або за волею підписувача

- втрата ключових носіїв;
- втрата ключових носіїв із наступним їх знаходженням;
- втрата ключів (кодів) від сейфів у момент зберігання в них ключових носіїв;
- втрата ключів (кодів) від сейфів у момент зберігання в них ключових носіїв із наступним їх знаходженням;
- свідомо 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;
- зберігання особистого ключа безпосередньо на HDD ПЕОМ користувача;
- неналежне зберігання пароля або PIN-коду до особистого ключа;
- викрадення особистого ключа в наслідок змови із особами, які мають право на його використання на законних підставах;
- порушення встановлених в організації правил використання і зберігання особистих ключів;
- розголошення мереживних паролів, паролів криптозахисту;



ЯВНА КОМПРОМЕТАЦІЯ

відбулася за участю або за волею третіх осіб

- 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;
- компрометація особистого ключа, яка здійснена третіми особами без відома підписувача.



Неявна компрометація.

Неявна компрометація базується на припущеннях або версіях подій, що створили або створюють умови компрометації особистого ключа із використанням сторонніми особами технічних засобів, програмного забезпечення тощо.



Неявна компрометація

- виникнення підозри на витік інформації щодо ключових даних;
- випадки коли неможливо достовірно встановити що саме відбулося зі 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.

Судова практика



Так, громадянка М. перебуваючи на посаді начальника сектору супроводу касових операцій і розрахунків, була призначена відповідальною за роботу із засобами захисту електронної банківської інформації Кіровоградської обласної філії «Укрсоцбанку» та роботу з АРМ РгоРіх/BANK на правах операціоніста робочого місця.

Вказана посадова особа діючи по необережності, порушила правила захисту інформації, яка оброблюється в комп'ютерах, порядок використання, зберігання особистих ключів та дотримання технології обробки розрахункових документів в електронному вигляді. До неї з особистою вимогою звернулась громадянка Н., заступник керуючого Кіровоградською обласною філією АКБ «Укрсоцбанку».

Громадянка М., будучи не обізнаною про злочинні наміри громадянки Н., передала останній дискету з своїм секретним ключем електронного цифрового підпису і пароль, легковажно розраховуючи на не настання суспільно-небезпечних наслідків з боку громадянки Н., не повідомила про те, що сталося в установленому порядку до підрозділу банківської безпеки. Внаслідок цього заступник керуючого Кіровоградською обласною філією АКБ «Укрсоцбанк», громадянка Н., використовуючи передану їй дискету з особистим ключем електронного цифрового підпису і пароль для входу в програму «РгоРіх», за допомогою свого службового комп'ютера протиправно здійснила низку переказів значних грошових коштів в гривні та валюті на рахунок громадянина К. У результаті вказаних дій громадянка Н. умисно, зловживаючи своїм службовим становищем, заволоділа майном банку в значній сумі, а банку було завдано значної матеріальної шкоди.

Судова практика



- Так, до ПАТ «Державний ощадний банк» звернулася громадянка Д. щодо зняття коштів із її рахунку, яким вона не користувалася із 2009 року і підтвердила даний факт відсутністю записів у ощадній книжці. За результатами розгляду порушеної кримінальної справи встановлено, що посадові особи територіального відділення ПАТ «Державний ощадний банк», а саме завідувача відділенням Т. та контролер-касир А. розробили злочинну схему привласнення коштів громадян шляхом проведення видаткових операцій із використанням службових особистих електронних цифрових підписів та паролів співробітників банківської установи за рахунками фізичних осіб, по яким тривалий час не здійснювались операції. Посадові особи територіального відділення ПАТ «Державний ощадний банк», порушуючи низку розпорядчих документів щодо захисту інформації та банківської таємниці, фактично отримали доступ до цифрових підписів працівників відділення та їх паролів. Згідно отриманих пояснень на робочому столі контролера-касира А. був зошит з паролями для візування, яким могли користуватись інші працівники відділення. Вказані особи у приватному порядку з'ясовували дані вкладника (помер, відбуває тривале покарання, виїхав закордон, місцезнаходження невідоме), після чого ініціювали, вводили та візували в АБС «БАРС» так звані «власні» операції із зняття коштів з рахунків вкладників без перевірки правильності операцій. У результаті вказаних дій громадянка Т та громадянка А. умисно, зловживаючи своїм службовим становищем, заволоділи майном банку в значній сумі, а банку було завдано значної матеріальної шкоди

Судова практика



- Під час закордонної відпустки приватного нотаріусу Івано-Франківського міського нотаріального округу невстановленою особою із використанням ключів, що належать приватному нотаріусу, відбулося несанкціоноване втручання в роботу електронного реєстру «Приватний нотаріус» Мінюсту, зокрема, були використані ключі доступу з метою внесення неправдивих відомостей щодо реєстрації заяви та довіреності, бланки суворої звітності. За даним фактом порушено кримінальну справу за злочином ознаки якого передбачені ч. 1 [ст. 361 КК України](#)

Судова практика



- Так до АЦСК «М» звернулись особи із заявою на виготовлення ключів електронного цифрового підпису на ім'я директора та головного бухгалтера ТОВ «А», для чого надали довіреність та копії необхідних документів. АКСЦ «М» заявку розглянуто та в день звернення згенеровані відповідні електронні цифрові ключі. Згодом було з'ясовано, що ТОВ «А» не замовляло електронні цифрові підписи посадових осіб. Однак, за допомогою незаконно виготовлених електронних цифрових підписів невстановленими особами від імені ТОВ «А» в Єдиному реєстрі податкових накладних зареєстровано податкові накладні, якими було штучно сформовано податковий кредит ТОВ «Р» та ТОВ «П» на загальну суму понад 12,6 млн грн. за рахунок ТОВ «А», незважаючи на те, що ТОВ «А» фактично ніколи не мало господарських правовідносин із вказаними вище підприємствами. По захист своїх прав ТОВ «А» звернулося до суду та правоохоронних органів, наразі тривають слідчі дії.

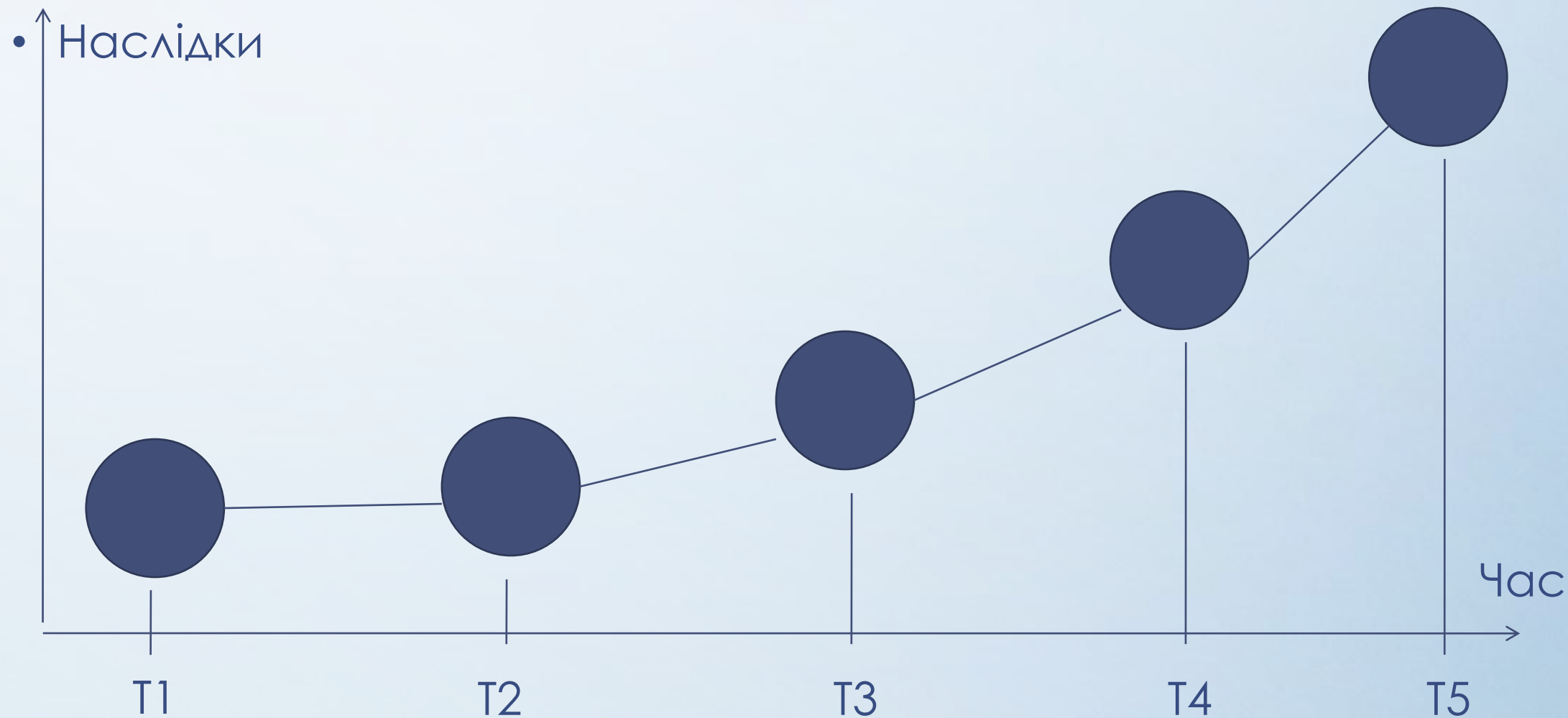
Неявна компрометація

- Група вчених з Японії, Швейцарії, Нідерландів та США застосували метод факторизації успішно вираховували дані зашифровані із допомогою криптографічного ключа стандарту RSA довжиною спочатку 768 біт, а згодом і довжиною 1024 біт.
- Відомий криптограф Аді Шамір (буква «S» у аббревіатурі RSA) розробив метод відтворення 4096-бітного RSA ключа шляхом акустичного криптоаналізу з низькою частотою дискредитації. Метод реалізується за допомогою звичайного мікрофону або мобільного телефону, які розміщуються на відстані 0,3-4 метри від комп'ютера на якому оброблюється інформація, та унікального програмного забезпечення високочастотних сигналів, які випромінюють комп'ютер під час роботи внаслідок вібрацій окремих компонентів та багатоядерних процесорів.

визначення в часі періоду компрометації

- Окрему зацікавленість для правової оцінки правових наслідків компрометації особистого ключа представляє визначення періоду в часі між реальним фактом компрометації та фактом її офіційного оголошення із наступним блокуванням або скасуванням сертифікату особистого ключа.

Наслідки і час



Період t_0 - t_1

- це час коли компрометація особистого ключа відбулася але підписувач не має підозри та фактів явної або не явної компрометації. Цей період найскладніше зафіксувати процесуально і правові наслідки, які створює цей період скомпрометований особистий ключ, мають статус офіційних та таких, що має низьку вірогідність визнання їх в подальшому недійсними, через недостатню доказову базу, яка зазвичай базується на припущеннях

Період t_1 - t_2

- характерний тим, що у підписувача, за результатом суб'єктивного аналізу певних фактів або подій, формується підозра щодо можливості компрометації особистого ключа. Правові наслідки, які створює у разі використання в цей період скомпрометований особистий ключ, більш передбачувані, оскільки припущення підозри можливо перевірити у доступний спосіб, в тому числі, в ході досудового розслідування, та зібрати необхідну доказову базу.

Період t_2 - t_3

- Характеризується необхідністю прийняти рішення підписувачем щодо оголошення компрометації особистого ключа.
- Може тривати від кількох хвилин до кількох діб. Це обумовлено наступними факторами: прийняттям рішення щодо компрометації користувачем, у разі якщо ЕЦП використовувалось для роботи з ресурсами, що не несуть юридичні ризики, потребує незначного часу. Натомість, прийняття рішення щодо компрометації особистого ключа, який постійно використовується для роботи в реєстрах або групи ключів, що забезпечують функціонування інформаційно-обчислювальних систем та мереж установи, потребує аналізу ситуації та розрахунку часу для заміни ключів та відновлення роботи систем. В органах державної влади або місцевого самоврядування прийняття рішення щодо оголошення компрометації особистих ключів може тривати декілька днів.

період t_3 - t_4

- Оголошення компрометації здійснюється у період t_3 - t_4 . Законодавство передбачає процедуру оголошення про компрометацію шляхом звернення до Акредитованого центру сертифікації ключів із заявою про компрометацію, яка передається будь-якими засобами комунікацій.

період t_4-t_5

- Останній період t_4-t_5 передбачено Законом України «Про довірчі послуги» і він не повинен перевищувати 2 години, протягом яких сертифікат ЕЦП блокується або скасовується Акредитованим центром сертифікації електронного цифрового підпису після отримання заяви/повідомлення підписувача про факт компрометації.

Проблеми

- Фактично в законодавстві поняття компрометації особистого ключа не має чіткого визначення та переліку подій або підстав, що дають можливість беззаперечно вважати їх компрометаційними, і, відповідно, базовими «маяками» для правознавців, які оцінюють прецеденти порушення законодавства, пов'язані із використанням особистого ключа електронного цифрового підпису в контексті статей 361-363 Кримінального кодексу України.
- 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 [21].
- В той же час дії або бездіяльність підписувача, які призвели до компрометації особистого ключа, як і поняття компрометації 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 ЕЦП, що, в свою чергу, створює умови для уникнення від покарання.

Ризики використання скомпрометованого особистого ключа електронного цифрового підпису

- Ризики, пов'язані з аутентифікацією (підтвердженням справжності) користувача. Особа, на якого вказує підпис під документом, може заявити про те, що підпис сфальсифікована і не належить даній особі.
- Ризики, пов'язані з відмовою від вмісту документа. Особа, на яку вказує підпис під документом, може заявити про те, що документ був змінений і не відповідає документу, підписаного даною особою.
- Ризики, пов'язані з юридичною значимістю електронного підпису. У разі судового розгляду одна зі сторін може заявити про те, що документ з електронним підписом не може породжувати юридично значимих наслідків або вважатися достатнім доказом в суді.
- Ризики, пов'язані з невідповідністю умов використання електронного підпису встановленому порядку. У разі використання електронного підпису в порядку, що не відповідає вимогам законодавства або угод між учасниками електронної взаємодії, юридична сила підписаних в даному випадку документів може бути поставлена під сумнів.
- Ризики, пов'язані з несанкціонованим доступом (використанням електронного підпису без відома власника). У разі компрометації ключа ЕЦП або несанкціонованого доступу до засобів ЕЦП може бути отриманий документ, який породжує юридично значимі наслідки, які виходять від імені користувача, ключ якого був скомпрометований.

Власник особистого ключа ЕЦП зобов'язаний

- Зберігати в таємниці ключ ЕП (особистий/закритий ключ).
- Не використовувати для електронного підпису та шифрування ключі, якщо підписувачу відомо, що ці ключі використовуються або використовувалися раніше.
- Негайно вимагати призупинення дії сертифіката особистого ключа ЕЦП при наявності підстав вважати, що таємниця ключа ЕЦП (особистого/закритого ключа) порушена (сталася компрометація ключа).
- Оновлювати сертифікат ключа ЕЦП відповідно до встановленого регламенту.



**Бережіть особистий ключ
електронного цифрового
підпису так, як бережете
власноручний підпис**



