УДК 004.56:342.9
DOI https://doi.org/10.32782/2524-0374/2025-3/186

ВИЗНАЧЕННЯ ДЕФІНІЦІЇ «КОМПРОМЕТАЦІЯ ОСОБИСТОГО КЛЮЧА ЕЛЕКТРОННОГО ПІДПИСУ» В КОНТЕКСТІ ПРАВОВОЇ НАУКИ

DEFINITION OF THE TERM “COMPROMISE OF A PRIVATE KEY OF AN ELECTRONIC SIGNATURE” IN THE CONTEXT OF LEGAL SCIENCE

Костенко О.В., доктор філософії в галузі права, доцент,
завідувач лабораторії теорії цифрової трансформації та права
Державна наукова установа «Інститут інформаційної безпеки і права Національної академії правових наук України»

Кудінов В.А., к.ф.-м.н., доцент, завідувач кафедри інформаційних технологій
Національна академія внутрішніх справ

Корнейко О.В., к.т.н., професор, професор кафедри інформаційних технологій
Національна академія внутрішніх справ

Актуальність даного дослідження обумовлена недостатньою розробленістю правового аспекту питання компрометації особистого ключа електронного підпису. Попри те, що технічні аспекти компрометації та її види досить широко висвітлені в науково-технічній літературі, юридична доктрина досі не виробила узгодженого визначення цього поняття та не окреслила правові наслідки таких випадків. Метою статті є дослідження зазначеного правового питання та формулювання пропозицій щодо визначення дефініції «компрометація особистого ключа електронного підпису» на основі аналізу спеціалізованої науково-технічної літератури та релевантної судової практики. У роботі обґрунтовано необхідність нормативного врегулювання дефініції «компрометація особистого ключа електронного підпису» та своєчасного реагування правової системи на ризики, що виникають у зв'язку з її настанням. Проаналізовано, як недоліки чинної правової моделі регулювання суспільно-правових відносин у сфері електронного підпису спричиняють недовіру до відповідного законодавства, ставлять під сумнів надійність електронних підписів, їхніх особистих ключів, а також цілісність і достовірність електронних документів, що ними підписані. Наведено приклади явної та неявної компрометації особистого ключа, визначено межі їх дії та охарактеризовано відповідні правові наслідки. Наукова новизна проведеного дослідження полягає у формулюванні авторського юридичного визначення поняття «компрометація особистого ключа електронного підпису», що спрямоване на забезпечення термінологічної чіткості та нормативної визначеності у відповідній сфері правового регулювання. Практичне значення отриманих результатів виявляється у можливості доповнення чинної редакції Закону України «Про електронні довірчі послуги» зазначеною дефініцією, що сприятиме удосконаленню правового механізму регулювання суспільних відносин, пов'язаних із застосуванням електронного підпису. Це, у свою чергу, посилить довіру до надійності електронних підписів, автентичності та цілісності електронних документів, а також легітимності правочинів, укладених в електронній формі. Запропоновані підходи також мають потенціал стимулювати розвиток транскордонної електронної комерції та цифрових послуг.

Ключові слова: електронний підпис, особистий ключ, компрометація.

The relevance of this study stems from the insufficient development of the legal framework addressing the compromise of a personal electronic signature key. While the technical aspects and classifications of key compromise are extensively covered in scientific and technical literature, legal doctrine has yet to establish a consistent definition of this concept or delineate its legal consequences. The purpose of the article is to study the indicated legal issue and formulate proposals for defining the definition of "compromise of a personal key of an electronic signature" based on an analysis of specialized scientific and technical literature and relevant case law. This paper substantiates the need for normative regulation of the term “compromise of a personal electronic signature key” and emphasizes the importance of timely legal responses to the risks arising from such incidents. The study analyzes how deficiencies in the current legal model governing social and legal relations in the field of electronic signatures undermine trust in the relevant legislation, cast doubt on the reliability of electronic signatures and their personal keys, and challenge the integrity and authenticity of electronically signed documents. Examples of both explicit and implicit key compromise are provided, with boundaries of their manifestation defined and corresponding legal implications characterized. The scientific novelty of the research lies in the formulation of an original legal definition of the concept “compromise of a personal electronic signature key,” aimed at ensuring terminological clarity and normative precision within the relevant legal domain. The practical significance of the findings is reflected in the potential to amend the current version of the Law of Ukraine “On Electronic Trust Services” by incorporating the proposed definition, thereby improving the legal mechanism for regulating social relations involving the use of electronic signatures. This, in turn, will enhance trust in the reliability of electronic signatures, the authenticity and integrity of electronic documents, and the legitimacy of transactions concluded in electronic form. The proposed approaches also hold promise for stimulating the development of cross-border electronic commerce and digital services.

Key words: electronic signature, private key, compromise.

Вступ. У сучасних інформаційних системах обмін даними здійснюється у цифровому форматі, де надійність переданої інформації забезпечується через використання електронних довірчих послуг, а вимоги до її достовірності та цілісності реалізуються шляхом застосування технології електронного підпису. Такий підпис формується за допомогою алгоритмів криптографічного захисту, що генерують відповідні електронні дані, які приєднуються до електронного документа та логічно з ним пов'язуються.

З метою нормативного регулювання механізмів застосування електронного підпису для надання юридичної сили електронним довірчим послугам, Україна, у процесі гармонізації національного законодавства з міжнародними стандартами, у 2017 році ухвалила Закон України «Про електронні довірчі послуги» [16]. Внаслідок цього попередній Закон України «Про електронний цифровий підпис» [16], чинний з 2004 року, був визнаний таким, що втратив силу.

Водночас більшість чинних нормативно-правових актів були розроблені на основі положень попереднього закону, що передбачав загальні правила використання електронного підпису. Практика застосування цих актів у межах нового правового регулювання виявила низку невирішених юридичних питань. Серед них особливої уваги потребує проблема правової невизначеності дефініції «компрометація особистого ключа», яка є складовою термінологічного апарату законодавства у сфері електронного підпису.

Таким чином, усунення правової невизначеності щодо поняття «компрометація особистого ключа електронного підпису» та забезпечення своєчасного реагування правової системи на ризики, що виникають у зв'язку з компрометацією, становить актуальну науково-правову проблему.

Відповідно, метою статті є дослідження зазначеного правового питання та формулювання пропозицій щодо визначення дефініції «компрометація особистого ключа електронного підпису» на основі аналізу спеціалізованої науково-технічної літератури та релевантної судової практики.

Огляд літератури Упродовж останніх років питання правового регулювання суспільних відносин, а також технічні аспекти, пов'язані із застосуванням електронного підпису, стали предметом дослідження низки вітчизняних науковців, зокрема С. Бєлова (2019), У. Ватаманюк-Зелінської (2020), Р. Новосада (2023), Я. Рижого (2023), А. Святошнюка (2023), В. Чешуна (2024), Ю. Яремчука (2024) та інших. Серед зарубіжних дослідників варто відзначити V. Sucasas (2023), який також звертався до цієї тематики.

Так, Р. Новосад (2023) аналізував загальні засади правового статусу електронного підпису в Україні. У. Ватаманюк-Зелінська (2020) зосередила увагу на перспективах та особливостях правового регулювання використання електронного підпису в державному секторі, тоді як А. Святошнюк (2023) досліджував специфіку застосування електронного цифрового підпису при укладенні цивільно-правових договорів у мережі Інтернет.

Окремий масив наукових праць присвячено нормативно-правовому регулюванню технології цифрового підпису, зокрема в контексті формування сигнатури на основі атрибутів підписувача. У цьому напрямі Я. Рижий (2023) розглядає класифікацію персональних атрибутів та їх роль у створенні цифрового підпису, а В. Чешун (2024) аналізує правові засади формування сигнатури на основі персональних даних підписувача, що забезпечує тісний зв'язок між підписом і особою автора, підвищуючи інформативність для верифікатора. Такий підхід сприяє розвитку систем електронного підпису, орієнтованих на індивідуалізацію та точну ідентифікацію підписувача. Аналогічні питання порушуються також у роботах V. Sucasas (2023).

Натомість проблема компрометації особистого ключа електронного підпису в українському науковому дискурсі розглядається переважно з технічної точки зору. Зокрема, С. Бєлов (2016) досліджує наслідки компрометації електронного підпису, І. Рефагі (2021) наводить приклади її реалізації, а І. Горбенко (2015) здійснює глибокий аналіз технічних аспектів компрометації ключів. Ці питання також висвітлюються у навчальних виданнях, серед яких варто згадати працю Ю. Яремчука (2024).

Водночас, на сьогодні спостерігається очевидна недостатність теоретичних досліджень, присвячених комплексному аналізу дефініції «компрометація особистого ключа електронного підпису» та її правових наслідків. Серед небагатьох робіт, що торкаються цієї проблематики, слід відзначити дослідження О. Костенка (2023), яке, однак, обмежується аналізом кваліфікованого електронного підпису.

Таким чином, попри наявність значного теоретичного доробку, питання чіткого юридичного визначення поняття «компрометація особистого ключа електронного підпису» та правових наслідків такої компрометації залишається відкритим і потребує подальшого наукового осмислення.

Матеріали та методи. Методологічну основу статті становлять загальнонаукові та спеціально-юридичні методи дослідження. Діалектичний метод використано для аналізу розвитку загальних суспільних правовідносин у сфері електронних довірчих послуг. Порівняльно-правовий метод надав можливість виявити особливості правовідносин саме із застосуванням електронних підписів. Метод правового моделювання використано для розроблення пропозицій щодо вдосконалення термінології та правового регулювання аспекти.

Результати й обговорення. Необхідність формулювання нової дефініції поняття «компрометація особистого ключа електронного підпису», на думку авторів, зумовлена низкою чинників, які обґрунтовують актуальність цього завдання.

По-перше, міжнародне нормативно-правове регулювання у сфері електронного підпису не містить уніфікованого, загальновизнаного визначення базового терміна «компрометація» у контексті електронного підпису. Зокрема, термін «компрометація» вживається у Типовому законі Комісії ООН з права міжнародної торгівлі (ЮНСІТРАЛ) «Про електронні підписи та Керівництві із прийняття рішень», ухваленому 5 липня 2001 року на 34-й сесії ЮНСІТРАЛ у Відні [17]. У статті 57 цього документа поняття «ненадійний сертифікат» трактується як такий, особистий ключ якого було скомпрометовано внаслідок втрати підписувачем контролю над ним. У правовій системі США термін «компрометація» визначається Національним інститутом стандартів і технологій (National Institute of Standards and Technology, NIST) «*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)*» [18].

По-друге, національне законодавство України та підзаконні нормативно-правові акти у сфері інформаційної безпеки також демонструють відсутність єдиного підходу до тлумачення поняття «компрометація».

Так, відповідно до пункту 26 статті 1 Закону України «Про електронні довірчі послуги», компрометація особистого ключа визначається як «*будь-яка подія, що призвела або може призвести до несанкціонованого доступу до особистого ключа*». У цьому ж Законі надано визначення поняття «особистий ключ», а також класифікацію електронних підписів, яка включає електронний підпис, удосконалений електронний підпис та кваліфікований електронний підпис.

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

Так, у нормативному документі НД ТЗІ 1.1-003-99 [19] термін «компрометація (compromise)» визначається як «*порушення політики безпеки; несанкціоноване ознайомлення*». Це визначення орієнтоване на регулювання інцидентів у сфері інформаційної безпеки, пов'язаних із порушенням встановлених правил використання електронного підпису. Водночас воно не охоплює правовідносини, що виникають у зв'язку з використанням особистого ключа поза межами визначеної політики безпеки, яка, до того ж, може суттєво варіюватися залежно від контексту. Крім того, у цьому визначенні не розкривається зміст поняття «несанкціоноване ознайомлення», що ускладнює його практичне застосування.

Натомість у «Положенні про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису» [20] компрометація трактується 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*». На думку авторів, саме це визначення є найбільш релевантним серед проаналі-

зованих і може бути покладене в основу формулювання дефініції «компрометація особистого ключа електронного підпису». Його нормативне закріплення на рівні законодавчого акту сприятиме підвищенню правової визначеності та ефективному застосуванню відповідних норм права.

По-третє, упродовж останніх років спостерігається зростання кількості правопорушень і злочинів, пов'язаних із використанням електронних підписів. Однією з ключових причин цього явища є створення самими підписувачами умов, що сприяють компрометації особистих ключів електронного підпису та їх подальшому неправомірному використанню.

Найбільша концентрація таких правопорушень фіксується у банківській сфері. Зокрема, у низці кримінальних проваджень встановлено, що окремі працівники банківських установ, порушуючи внутрішні політики інформаційної безпеки, під різними приводами отримували доступ до особистих ключів електронного підпису своїх колег або підлеглих, після чого організовували схеми незаконного заволодіння коштами клієнтів банку. Один із показових прикладів такого правопорушення розглянуто у судовому рішенні, ухваленому у 2011 році [21].

Поширеною є також практика компрометації особистих ключів електронного підпису нотаріусів та державних реєстраторів під час здійснення ними нотаріальних дій або реєстраційних процедур. Неналежне зберігання ключів або їх незаконне привласнення призводить до неправомірного відчуження майна через втручання в функціонування Єдиного державного реєстру речових прав на нерухоме майно та Єдиного державного реєстру юридичних осіб і фізичних осіб-підприємців [22].

Окрему загрозу становлять випадки заволодіння особистими ключами електронного підпису керівників підприємств та головних бухгалтерів сторонніми особами, зокрема шляхом отримання таких ключів в Акредитованих центрах сертифікації ключів на підставі підроблених довіреностей. Це створює передумови для вчинення фінансових злочинів, пов'язаних із незаконним використанням електронного підпису [23].

По-четверте, чинне законодавство у сфері електронного підпису не охоплює всі можливі види компрометації особистих ключів, що створює прогалини у правовому регулюванні відповідних ситуацій. З огляду на це, доцільним є проведення аналізу наукових джерел та технічних нормативних актів, присвячених електронному підпису, з метою класифікації типів та форм прояву компрометації особистого ключа.

У межах такого аналізу компрометацію особистого ключа електронного підпису доцільно поділяти на явну та неявну [3, 14].

Під явною компрометацією слід розуміти втрату контролю над інформацією, що становить особистий ключ, яка підтверджується достовірними фактами порушення політики безпеки та несанкціонованого ознайомлення з ключовими даними [3]. Явну компрометацію можливо розподілити на [3, 14]:

– 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 [3, 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 мереживних 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, яка підтверджується встановленими фактами порушення безпеки, неявна компрометація особистого ключа електронного підпису ґрунтується на припущеннях або гіпотетичних сценаріях, що свідчать про наявність або ймовірність створення умов для неправомірного доступу до особистого ключа. Такі умови можуть виникати внаслідок використання сторонніми особами технічних засобів, спеціалізованого програмного забезпечення чи інших інструментів, здатних порушити конфіденційність криптографічної інформації [5].

Так, до неявної компрометації можливо віднести [3, 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 обробляється 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 обробляється 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 [3, 5].

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 [4].

По-сьоме, чинне законодавство України не містить чіткого визначення поняття «компрометація особистого ключа електронного підпису», а також не передбачає вичерпного переліку подій або обставин, які можуть бути беззаперечно кваліфіковані як компрометаційні. Відсутність таких нормативних орієнтирів ускладнює правозастосування, зокрема для юристів, які змушені оцінювати порушення законодавства, пов'язані з використанням особистого ключа електронного цифрового підпису, переважно в межах диспозицій статей 361–363 Кримінального кодексу України [15].

Згідно з положеннями зазначених статей [6], особистий ключ підписувача може розглядатися як предмет або знаряддя злочину, тобто як технічний засіб, що використовується для несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку.

Водночас дії чи бездіяльність підписувача, які спричинили компрометацію особистого ключа, як і саме поняття «компрометація особистого ключа електронного підпису», наразі не отримали належної правової кваліфікації. Відсутність нормативно закріплених ознак компрометації створює неоднозначність у правозастосуванні, що ускладнює роботу правоохоронних органів, судів та адвокатів при кваліфікації злочинів, пов'язаних із використанням електронного підпису, і, як наслідок, може сприяти уникненню відповідальності за такі правопорушення [11].

Таким чином, відсутність правової визначеності у дефініціях «компрометація» та «компрометація особистого ключа електронного підпису», а також наявні структурні проблеми в нормативній моделі регулювання суспільно-правових відносин у сфері застосування електронного підпису, зумовлюють загальну недовіру до чинного законодавства, що регламентує відповідну сферу. Наслідком цього є виникнення сумнівів щодо надійності електронних підписів, цілісності електронних документів, автентичності правочинів, вчинених нотаріусами та державними реєстраторами в електронному форматі, а також правової стабільності договорів та угод, укладених із використанням електронного підпису.

У зв'язку з викладеним, автори вважають за доцільне нормативно закріпити дефініцію «компрометація особистого ключа електронного підпису» та пропонують її формулювання в такій 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».

Запропоноване визначення, що охоплює загальне поняття компрометації та містить деталізовані класифікації її явної і неявної форм, створює підґрунтя для більш точного правового аналізу суспільно небезпечних протиправних дій, пов'язаних із використанням особистого ключа електронного підпису.

З огляду на це, доцільним є нормативне закріплення дефініції «компрометація особистого ключа електронного підпису» у запропонованій авторській редакції шляхом внесення відповідних змін до пункту 26 статті 1 Розділу I чинної редакції Закону України «Про електронні довірчі послуги».

Суспільна небезпечність компрометації особистого ключа електронного підпису як матеріальної ознаки злочину полягає, по-перше, у її ролі як об'єктивного критерію для визнання діяння злочинним; по-друге, у можливості класифікації злочинів за ступенем їх тяжкості; по-третє, у визначенні межі між злочином і правопорушенням; по-четверте, у її значенні як одного з принципів індивідуалізації юридичної відповідальності та покарання [6].

Крім того, нормативне закріплення поняття «явна компрометація» сприятиме наданню правової оцінки діям як власника особистого ключа електронного підпису, так і третіх осіб, які незаконно заволоділи ним та здійснюють несанкціоноване використання. Водночас застосування терміна «неявна компрометація» дозволить більш диференційовано класифікувати суспільно небезпечні діяння, що вчиняються щодо особистого ключа підписувача або з його використанням, зокрема в контексті правозастосування положень статей 361–363 Кримінального кодексу України.

Висновки. Запровадження запропонованого авторами визначення, яке охоплює загальне поняття компрометації, а також містить окремі дефініції явної та неявної компрометації, сприятиме більш точній правовій кваліфікації суспільно небезпечних діянь, пов'язаних із неправомірним використанням особистого ключа електронного підпису.

У зв'язку з цим доцільним видається внесення запропонованої авторської редакції дефініції «компрометація особистого ключа електронного підпису» до пункту 26 статті 1 Розділу I чинної редакції Закону України «Про електронні довірчі послуги» замість існуючого формулювання.

Суспільна небезпечність компрометації особистого ключа електронного підпису як матеріальної ознаки складу злочину полягає, по-перше, у її значенні як об'єктивного критерію для визнання діяння злочинним; по-друге, у можливості класифікації злочинів за ступенем їх тяжкості; по-третє, у визначенні межі між злочином і правопорушенням; і, по-четверте, у забезпеченні принципу індивідуалізації юридичної відповідальності та покарання [6].

Крім того, закріплення поняття «явна компрометація» дозволить здійснювати правову оцінку як діям власника особистого ключа, так і третіх осіб, які незаконно заволоділи цим ключем і використовують його без відповідного дозволу. Водночас використання терміна «неявна компрометація» забезпечить можливість більш диференційованого підходу до класифікації суспільно небезпечних діянь, що вчиняються щодо особистого ключа підписувача або з його використанням, зокрема в межах застосування статей 361–363 Кримінального кодексу України.

ЛІТЕРАТУРА:

1. Бєлов С.В., Мартиненко С.В. Моделі побудови національної інфраструктури центрів сертифікації ключів та їх ризики. URL: http://www.itsway.kiev.ua/pdf/Model-CA_Risks.pdf

2. Ватаманюк-Зелінська У. З., Сушко В. С. Перспективи використання електронного цифрового підпису в державних структурах, Ефективна економіка, № 7. URL: http://www.economy.nayka.com.ua/?op=1&z=8043.

3. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування : монографія / І.Д. Горбенко, Ю.І. Горбенко ; Харк. нац. ун-т радіоелектрон., ЗАТ "Ін-т інформ. технологій". Х. : Форт, 2015. 868 с.

4. Mike Just, Paul C. van Oorschot Addressing the Problem of Undetected Signature Key Compromise. URL: http://citeseerx.ist.psu.edu/viewdoc/ download?doi=10.1.1.26.507&rep=rep1&type=pdf.

5. Костенко О. В., Прокопович-Ткаченко Д. І., Флоров С. В. Юридичні ризики компрометації кваліфкованого електронного підпису // *Юридичний науковий електронний журнал*. 2023. № 11. с. 373-379.

6. А. А. Васильєв, Є. О. Гладкова, О. О. Житний та ін.Кримінальне право України. Загальна частина : підручник. Харків. нац. ун-т внутр. справ. Харків, 2020. 428 с.

7. Новосад Р. В. Правовий статус електронного підпису в Україні: від ідеї до реалізації, *Право та державне управління.* 2023. № 3. С. 112–116.

8. Рефагі Ірина (2021). Колос на цифрових ногах: як підробляють електронні підписи і як це загрожує діджиталізації. URL: https://focus.ua/uk/technologies/487417-kak-poddelyvayut-elektronnye-podpisi-i-chem-eto-grozit-didzhitalizacii

9. Рижий Я. О. Класифікація атрибутів особи і формування цифрового підпису на їх основі. *Актуальні проблеми комп'ютерних наук АПКН-2023:* збірник наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції. Хмельницький. С. 252–256.

10. Святошнюк А. Л. Щодо особливостей використання електронного цифрового підпису при укладенні цивільно-правових договорів у мережі інтернет, *Вісник Одеського національного університету.* Серія: Правознавство, 2023, том 25, Випуск 2 (37), pp. 21–24.

11. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку : Верховний Суд України. URL: http://www.scourt.gov.ua/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02/

12. Sucasas V., Mantas G., Papaioannou M., Rodriguez J. Attribute-Based Pseudonymity for Privacy-Preserving Authentication in Cloud Services, IEEE Transactions on Cloud Computing, 2023, vol.11, № 1, pp. 168-184.

13. Віктор Чешун, Юрій Кльоц, Віра Тітова, Наталія Петляк. Нормативно-правове регулювання технології цифрового підпису на основі особових атрибутів. Problems of Scientific, Technical and Legal Support for Cybersecurity in the Modern World. Monograph. Edited by Serhii Semenov, Mateusz Muchacki. Krakow, 2024. PP. 263-272.

14. Яремчук Ю. Є.? Салієва О. В., Бондаренко І. О. Основи криптографічного захисту інформації : електронний навчальний посібник комбінованого (локального та мережного) використання/ Вінниця : ВНТУ, 2024. 139 с.

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

16. Про електронний цифровий підпис: Закон України від 22.05.2003 № 852-IV // *Відомості Верховної Ради України*, 2003, № 36, ст.276.

17. UNCITRAL Model Law on Electronic Signatures (2001). URL: http://www.uncitral.org/ pdf/english/texts/electcom/ ml-elecsig-e.pdf.

18. NIST SP 800-57 Part 3 Revision 1 Recommendation for Key Management // National Institute of Standards and Texchnology, January 2015. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf.

19. 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. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/doccatalog/list?currDir=41640.

20. 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. URL: http://zakon2.rada.gov.ua/laws/show/z0862-07

21. Постанова Ленінського районного суду м. Кіровограда від 19 жовтня 2011 р. у справі № 1-463/11 // Єдиний державний реєстр судових рішень. URL: http://www.reyestr.court.gov.ua/Review/20422029

22. Ухвала Івано-Франківського міського суду Івано-Франківської області від 09 березня 2017 р. у справі № 344/3171/17 // Єдиний державний реєстр судових рішень. URL: http://www.reyestr.court.gov.ua/ Review/65214508

23. Ухвала Печерського районного суду м. Києва від 14 березня 2017 р. у справі № 757/10916/16-к // Єдиний державний реєстр судових рішень. URL: http