УДК 340.5

КОСТЕНКО О.В., головний науковий співробітник Інституту спеціальної техніки та судових експертиз Служби безпеки України

КОМПРОМЕТАЦІЯ ОСОБИСТОГО КЛЮЧА ЕЛЕКТРОННОГО ПІДПИСУ: ПРАВОВИЙ АСПЕКТ

Анотація. *Статтю присвячено дослідженню поняття компрометації особистого ключа електронного підпису, правовим аспектам компрометації в контексті теорії права. У роботі наведено поняття явної і неявної компрометації та межі їх дії, а також правові наслідки компрометації.*

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

Summary. *The article is devoted to the study of the concept of compromising the personal key of digital signature, the legal aspects of compromise in the context of the theory of law. The paper presents the concept of explicit and implicit compromise and the limits of their actions, as well as the legal consequences of compromise.*

Keywords: *compromise, personal key, signer, digital signature.*

Аннотация. *Статья посвящается исследованию понятия компрометации личного ключа электронной подписи, правовым аспектам компрометации в контексте теории права. В работе представлены понятия явной и не явной компрометации, их границы, а так же правовые последствия компрометации.*

Ключевые слова: *компрометация, личный ключ, подписчик, электронная подпись.*

Постановка проблеми. Значущим фактором сьогодення є стрімкий розвиток політичних, економічних, наукових, бізнесових, торгівельних, інформаційних відносин які безпосередньо впливають не тільки на міжнародний стан, а й на відповідні процеси у конкретних країнах, а також на здійснення прав, задоволення інтересів і потреб їх громадян та державних інституцій. Однією з основних вимог при реалізації цих відносин є швидкий обмін інформацією, відображеною в цифровому вигляді, забезпечення її актуальності, надійності, цілісності, оперативності, ідентичності, достовірності і повноти.

Потужні інформаційні комп’ютерні технології створюють нові можливості за рахунок використання цифрової інформації (даних), що, в свою чергу, створює нові суспільні відносини, які виникають між суб’єктами правовідносин під час: електронного обміну інформацією (Electronic Data Interchange); 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. Обмін інформацією здійснюється в процесі електронних транзакцій у формі електронних (цифрових) документів. Надійність інформації під час обміну забезпечується завдяки застосуванню довірчих електронних послуг, а вимоги достовірності і цілісності інформації – завдяки застосуванню алгоритмів цифрового криптографічного захисту із використанням технології електронного підпису. Однак, широке застосування цієї технології водночас виявило й правові проблеми, пов’язані із використанням особистого ключа електронного підпису. Однією із таких проблем є правова невизначеність дефініції “компрометація” особистого ключа електронного підпису.

Якнайшвидше урегулювання проблеми правової невизначеності дефініції “компрометація” та своєчасне реагування права на ризики, які виникають або зумовлені компрометацією особистого ключа електронного підпису, є наразі актуальною проблемою.

Результати аналізу наукових публікацій. Питанням правового регулювання суспільних відносин, пов’язаних з використанням електронного підпису займались такі вітчизняні вчені: Козіел Г., Петрицький А., Плескач В., Пономаренко Л., Шпірко А., Янчева Л., Локшин А. та ін. Серед іноземних вчених дану тему досліджували: Масон С., Тірі А., Венбо М., Петров А., Беззубцев О. За останні роки питання створення надійних механізмів визнання електронних підписів порушували такі науковці: Перевозчикова О.Л., Бєлов С.В., Горбенко І.Д., Потій О.В., Погорелов Б.А., Мелащенко А.О. Проблема компрометації в контексті компрометації особистого ключа електронного підпису в Україні висвітлювалась переважно в технічному аспекті. Так, у статті Бєлова С.В. “Моделі побудови національної інфраструктури центрів сертифікації ключів та їх ризики” висвітлюються виключно наслідки компрометації електронного підпису [1], а в публікації Погорелова Б.А. “Щодо визначення основних криптографічних понять” наголошено на нейтралізації загроз компрометації для системи управління електронними ключами [2].

Разом з тим, на даний час недостатньо теоретичних праць та досліджень в комплексі питань, які визначають дефініцію “компрометація” особистого ключа електронного підпису.

Метою статті є визначення правових проблем, пов’язаних із визначенням дефініції “компрометація”, як елемента понятійного апарату в чинному законодавстві, а також пропозиції щодо формулювання дефініції “компрометація особистого ключа”.

Виклад основного матеріалу. Перш ніж перейти до дослідження дефініції “компрометація особистого ключа” розглянемо історію виникнення самого терміну “компрометація” в правовій моделі суспільно-правових відносин, що регулюють сферу використання підпису.

Розвиток телекомунікаційних технологій сприяв виникненню механізмів обміну між користувачами документами в електронній формі, які мають юридичну значимість. Потреба в використанні та обміні такими документами була настільки високою, що багато країн майже одночасно прийняли спеціальні закони, що регулювали основи електронної торгівлі та застосування електронних підписів. Так, Європейським Парламентом та Радою 13 грудня 1999 року прийнято Директиву “Про систему електронних підписів, що застосовується в межах Співтовариства”, у США введено Закон “Про електронні підписи в глобальній і національній комерції”, Францією затверджено Декрет “Про електронний підпис”, Німеччиною прийнято Федеральний закон “Про цифрові підписи”.

Однак на той час ні в України, ні у більшості країн не було практичного досвіду побудови систем електронних підписів як в організаційному, так і в правовому аспекті. Багато національних законів розроблялись як моделі загальних правил використання електронних підписів. Практичне застосування вказаних законодавчих актів виявило низку неврегульованих нормами права суспільних відносин, пов’язаних з використанням електронного підпису, в тому числі, з відсутністю чіткої дефініції поняття “компрометація особистого ключа”.

Слід зауважити, що необхідність створення нової дефініції “компрометація особистого ключа” зумовлена наявністю таких причин.

По-перше, міжнародні законодавчі норми в галузі електронного підпису не мають чітких, загальноприйнятих визначень поняття “компрометації”. Термін “компрометація”, в контексті “компрометація електронного підпису”, застосовано у Типовому законі

ЮНСІТРАЛ “Про електронні підписи і керівництво із прийняття рішень” [3], прийнятого у Відні 5 липня 2001 року на 34-й сесії ЮНСІТРАЛ, статтею 57 якого 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 Technology – NIST) як “неавторизоване розкриття, модифікація, заміщення або використання конфіденційних даних (включаючи криптографічні ключові тексти та інші дані Центру політики безпеки (CSP)” [4] або “неавторизоване розкриття, модифікація, заміщення або використання конфіденційних даних (наприклад, ключів, метаданих та іншої інформації, що стосується безпеки)” [5; 6].

По-друге, вітчизняне законодавство також по-різному трактує дефініцію “компрометація”. Так, пунктом 26 статті 1 Закону України “Про електронні довірчі послуги” визначено, що “компрометація особистого ключа – будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа” [7]. Однак, таке ж саме тлумачення містив і попередній Закон України “Про електронний цифровий підпис”. На жаль, таке визначення з одного боку не надає визначення які саме об’єкти або суб’єкти правових відносин вчиняють вказані вище дії та які саме дії/події призводять до несанкціонованого використання особистого ключа, а з іншого боку невизначеність дефініції створює підстави для довільного трактування вказаної норми закону.

В той же час, українські технічні спеціалісти в галузі захисту інформації запровадили кілька варіантів визначення “компрометація”, як технічного терміну. Так, 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” (compromise) – як порушення політики безпеки; несанкціоноване ознайомлення” [8]. Дане визначення 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”.

Крім того, наказом Державної служби спеціального зв’язку та захисту інформації України “Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису” від 20.07.07 р. № 141 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 [9]. Без сумніву, це найбільш вдале визначення “компрометації”, яке доцільно покласти в основу дефініції “компрометація особистого ключа” та закріпити на рівні законодавчого акта, що сприятиме чіткому застосуванню норм права.

По-третє, в українському законодавстві склалася ситуація, коли відсутність дефініції “компрометація особистого ключа” в суспільних відносинах, які регулюють сферу використання електронних ключів, позбавила право ясності та конкретики, ускладнивши процес його застосування, що зменшило довіру до електронних

документів та правочинів, які вчинили за допомогою електронних підписів, про що свідчить судова практика.

За останні роки збільшилася кількість правопорушень та злочинів, пов’язаних саме із компрометацією та незаконним використанням особистих ключів електронних підписів. Переважна більшість злочинів із використанням особистого ключа електронного підпису скоєні внаслідок явної компрометації особистого ключа самим підписувачем. Саме підписувачі створюють умови для компрометації особистого ключа й подальшого його незаконного використання. Здебільшого такі злочини здійснюються в банківській сфері, а також в галузі нотаріату та реєстрації юридичних осіб. Прикладом є низка кримінальних справ, фігуранти яких, будучи банківськими працівниками, нехтували правилами політик банківської безпеки, під різними приводами заволодівали особистими ключами цифрових підписів своїх колег або підлеглих та організували схеми незаконного заволодіння коштами клієнтів банків [10; 11]. Має місце практика компрометації особистого ключа нотаріуса або реєстратора під час вчинення 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 та Єдиного державного реєстру юридичних осіб та фізичних осіб-підприємців [13]. Також мають місце випадки заволодіння сторонніми особами особистими ключами керівників підприємств та головних бухгалтерів або отримання таких ключів в Акредитованих центрах сертифікації ключів за підробленими довіреностями з подальшим вчиненням фінансових злочинів [14].

По-четверте, специфічні проблеми надання послуг в галузі електронного підпису, пов’язані із компрометацією особистого ключа, полягають у достатньо складній структурі та видах компрометації.

У зв’язку із невизначеністю дефініції пропонується поділяти “компрометацію особистого ключа” на явну та неявну компрометацію.

Розглянемо вказані види компрометації.

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.

В свою чергу, явну компрометацію можливо розподілити на:

− 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:

− втрата (викрадення) ключових носіїв, 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 особистого ключа сторонній особі;

− порушення встановлених в організації правил використання і зберігання особистих ключів, розголошення мережних паролів, паролів криптозахисту, правил зберігання та знищення (після закінчення терміну дії) особистого ключа, а також вимог зберігання пароля або PIN-коду до особистого ключа;

− зберігання особистого ключа у відкритому, незашифрованому вигляді, безпосередньо на HDD ПЕОМ користувача;

− компрометація особистого ключа, яка здійснена третіми 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 особистого ключа внаслідок відповіді на запит, надісланий із ознаками шахрайства або підробки;

− виготовлення особистого ключа за підробленими документами [15; 16].

На відміну від явної компрометації особистого ключа, 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. До неявної компрометації можливо віднести:

− 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;

− перехоплення спеціальними технічними засобами, спеціалізованим або шпигунським програмним забезпеченням інформації, яка циркулює в Інтернет або локальній мережі, в яких оброблюється інформація із застосуванням особистих ключів [16; 17].

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. Світове наукове товариство періодично демонструє можливості технічного, знеособленого доступу до ключів особистого електронного підпису. Так, група вчених з Японії, Швейцарії, Нідерландів та США, успішно здійснили технічний доступ до даних, зашифрованих за допомогою криптографічного ключа [18]. Відомий криптограф Аді Шамір розробив метод технічного доступу та відтворення особистого ключа шляхом акустичного криптоаналізу без явного фізичного втручання в телекомунікаційні мережі та системи [19].

По-шосте, проблеми пов’язані із складністю надання правознавцями оцінки правових 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.

Розглянемо перебіг подій у часі, який умовно поділимо на п’ять періодів від початку компрометації особистого ключа до усунення наслідків його компрометації.

Перший період – це час коли компрометація особистого ключа відбулася але підписувач не має підозри та фактів явної або неявної 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 [20].

Другий період характерний тим, що у підписувача, за результатом суб’єктивного аналізу певних фактів або подій, формується підозра щодо можливості компрометації особистого ключа.

Наступний період характеризується необхідністю прийняти рішення підписувачем щодо оголошення компрометації особистого ключа. Третій період може тривати від кількох хвилин до кількох діб. Це обумовлено наступними факторами: прийняттям рішення щодо компрометації користувачем, у разі якщо електронний підпис використовувався для роботи з ресурсами, що не несуть юридичних ризиків та 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.

Оголошення компрометації здійснюється під час четвертого періоду. Законодавство передбачає процедуру оголошення про компрометацію шляхом звернення до Акредитованого центру сертифікації ключів із заявою про компрометацію, яка передається будь-якими технічними засобами комунікацій. Останній період передбачено Законом України “Про довірчі послуги” і він не повинен перевищувати 2 години, протягом яких сертифікат ЕЦП блокується або скасовується [7].

Аналізуючи етапи компрометації від реального факту компрометації та факту офіційного блокування або скасування сертифікату особистого ключа електронного підпису, можемо стверджувати, що найбільшому ризику піддаються дії із особистим ключем, які здійснюються в перший період, оскільки можливість збору доказової бази щодо вчинення суспільно небезпечного діяння із використанням скомпрометованого особистого ключа має низьку вірогідність.

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. 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 електронного підпису, як і поняття “компрометації особистого ключа”, поки що не знайшли правової оцінки. Відсутність переліку базових ознак компрометації особистого ключа електронного підпису створює неоднозначність трактування правоохоронними органами, судами та адвокатурою ознак злочинів, що вчинені із використанням електронного підпису, що, в свою чергу, створює умови для уникнення від покарання.

Отже, дефініція “компрометація” в нині діючому законодавстві – це фактично розпливчатий термін, для якого можуть виникати пограничні випадки, у яких може бути незрозумілим чи допустиме використання терміну, чи ні. Тому слід розширити встановлену практику використання дефініції “компрометація”, щоб зробити термін

менш розпливчастим та більш інформативним, врахувати поняття явної та неявної компрометації, що сприятиме більш якісному застосуванню норм права.

Без сумніву, існуючі проблеми в правовій моделі суспільно-правових відносин, що регулюють сферу використання електронного підпису, формують в цілому недовіру до законодавства в сфері електронного підпису, пов’язану саме із невизначеністю дефініції “компрометація”, створюють сумнів щодо надійності електронних підписів, цілісності електронних документів, підписаних ними, достовірності правочинів, вчинених нотаріусами та державними реєстраторами в електронному вигляді, незмінності інформації, внесеної в Єдиний державний реєстр речових прав на нерухоме майно та Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців, надійності угод та договорів, укладених в електронній формі тощо.

Зважаючи на наявну неврегульовану нормами права проблему суспільних відносин, пов’язану з використанням електронного підпису, вважається за доцільне запровадити дефініцію “компрометація особистого ключа електронного підпису” та викласти її в наступній редакції:

Компрометація особистого ключа електронного підпису – будь-яка явна або неявна подія та/або дія (втрата, розголошення, крадіжка, несанкціоноване копіювання тощо) з даними особистого ключа електронного підпису та засобами криптографічного захисту інформації, що призвела або може призвести до несанкціонованого розголошення, зміни, знищення, блокування, перехоплення, копіювання та використання особистого ключа електронного підпису, 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 бездіяльністю підписувача або третіх осіб без застосування технічних засобів.

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

Дане визначення містить загальну норму компрометації та два деталізованих визначення явної та неявної компрометації. Такий підхід дозволить здійснювати більш якісну кваліфікацію суспільно небезпечних протиправних дій із використанням особистого ключа електронного підпису.

Варто зазначити, що злочин, як і будь-яке інше правопорушення, є вчинком людини. Але на відміну від інших вчинків людини злочин за своєю соціальною сутністю є посяганням на ті відносини, що склалися в суспільстві, відображають його найбільш важливі інтереси, внаслідок чого охороняються законом. Компрометацію особистого ключа електронного підпису слід розглядати саме як свідомий вольовий вчинок людини, який виражений у конкретній дії або бездіяльності. Суспільна небезпечність компрометації особистого ключа електронного підпису, як матеріальна ознака злочину полягає в тому, що діяння чи бездіяльність заподіює шкоду відносинам, які охороняються законом, або містить у собі реальну можливість заподіяння такої шкоди. Це – об’єктивна властивість злочину, реальне порушення відносин, що склалися в суспільстві в сфері електронного підпису. 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 [22].

Крім того, визначення “явна компрометація” сприятиме можливості надання юридичної оцінки вчинкам як підписувача, власника особистого ключа, 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, які регулюють суспільні відносини у сфері інформаційної діяльності, в тому числі і електронного підпису, та окреслюють особливий вид злочинів, пов’язаних із незаконним використанням сучасних інформаційних технологій і засобів комп’ютерної техніки. Компрометацію особистого ключа електронного підпису слід відносити до зазначених в законі наслідків вчинення злочинів, передбачених ст. 361-363 Кримінального кодексу України – витоку, втрати, підроблення, блокування інформації, спотворення процесу її обробки або порушення встановленого порядку її маршрутизації [23].

Пропонуємо дефініцію “компрометація особистого ключа” у запропонованій редакції внести до пункту 26 статті 1 Розділу І Закону України “Про електронні довірчі послуги”.

Висновки.

Враховуючи проаналізовані підходи до визначення компрометації особистого ключа, її види та характерні ознаки, можливо зробити висновок, що відсутність законодавчого врегулювання такого суспільно небезпечного діяння як “компрометація особистого ключа” в сфері права впливає на стабільність інформаційних ресурсів держави та їх безпеку.

Отже, забезпечуючи чіткість законодавчої мови та визначеність правових норм нова законодавча дефініція “компрометація особистого ключа електронного підпису” сприятиме правовому регулюванню суспільних відносин, пов’язаних з використанням електронного цифрового підпису, чіткій класифікації злочинів та правопорушень, вчинених із використанням особистого ключа електронного підпису, а також підвищить довіру до надійності електронних документів підписаних ними, електронних сервісів, угод та договорів, укладених в електронній формі із використанням електронного підпису, стимулюватиме розвиток транскордонної електронної торгівлі та послуг.

Використана література

1. Бєлов С.В., Мартиненко С.В. Моделі побудови національної інфраструктури центрів сертифікації ключів та їх ризики. – Режим доступу : http://www.itsway.kiev.ua/pdf/Model-CA_ Risks.pdf

2. Погорелов Б.А., Черемушкин А.В., Чечета С.И. Об определении основных криптографических понятий : материалы конференции [“Математика и безопасность информационных технологий”], (г. Москва, МаБИТ-03, 23-24 октября 2003 г.). – М. : МГУ, 2003.

3. Типовой закон ЮНСИТРАЛ об электронных подписях. – Режим доступу : http://zakon 0.rada.gov.ua/laws/show/995_937

4. FIPS PUB 140-2. Security Requirements for Cryptographic Modules // Federal Information Processing Standards Publication 140-2, U.S. Department of Commerce, 05/2001.

5. Recommendation for Key Management. Special Publication 800-57, Part 1 Rev. 3, NIST, 05/2014.

6. NIST SP 800-130. A Framework for Designing Cryptographic Key Management Systems. – Режим доступу : http://nvlpubs.nist.gov/nistpubs/SpecialPublications/ NIST.SP.800-130.pdf

7. Про довірчі послуги : Закон України від 05.10.17 р. № 2155-VIII. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2155-19

8. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу : Наказ ДСТСЗІ СБУ від 28.04.99 р. № 22. – Режим доступу : http://www.dsszzi.gov.ua/dsszzi/control/uk/doccatalog/list?currDir=41640

9. 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 20.07.07 р. № 141. – (Зареєстрований Міністерством юстиції України від 30.07.07 р. № 862/14129). – Режим доступу : http://zakon2.rada.gov.ua/laws/show/z0862-07

10. Постанова Ленінського районного суду м. Кіровограда від 19.10.11 р. у справі № 1-463/11. – (Єдиний державний реєстр судових рішень). – Режим доступу : http://www.reyestr.court.gov.ua/Review/20422029

11. Розслідування 12016040730000533. – (Єдиний державний реєстр судових рішень). – Режим доступу : http://www.gp.gov.ua/ua/erdr.html

12. Ухвала Івано-Франківського міського суду Івано-Франківської області від 09.03.17 р. у справі № 344/3171/17. – (Єдиний державний реєстр судових рішень). – Режим доступу : http://www.reyestr.court.gov.ua/Review/65214508

13. Ухвала Печерського районного суду м. Києва від 14.03.17 р. у справі № 757/10916/16-к. – (Єдиний державний реєстр судових рішень). – Режим доступу : http://www.reyestr.court.gov.ua/Review/56854252

14. Kleinjung T., Aoki K., Franke J., Lenstra A.K., Thome E., Bos J.W., Gaudry P., Kruppa A., Montgomery P.L., Osvik D.A., H. te Riele, Timofeev A., Zimmermann P. Factorization of a 768-bit RSA modulus, version 1.4, February 18, 2010. – Режим доступу : https://eprint.iacr.org/2010/006.pdf

15. Инструкция по работе со средствами криптографической защиты информации, сертификатами ключей подписи, открытыми и закрытыми ключами электронной подписи. : Приложение № 17 к постановлению администрации Хабаровского муниципального района от 14.04.17 р. № 808. – Режим доступу : khabrayon.ru/sites/default/files/2016/05/808_14.04.2017_p 17.rtf

16. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи. – Режим доступу : www.dsyst.com/files/security-manual.doc

17. Инструкция по обеспечению безопасности эксплуатации сертифицированных средств криптографической защиты информации (СКЗИ). – Режим доступу : www.aksicom.ru/content /istr_skzi.pdf.

18. Pellegrini A., Bertacco V., Austin T. Fault-Based Attack of RSA Authentication. – Режим доступу : https://web.eecs.umich.edu/~taustin/papers/DATE10-rsa.pdf

19. Genkin D., Shamir A., Tromer E. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. – Режим доступу: http://www.tau.ac.il/~tromer/papers/acoustic-20131218.pdf

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

21. Кримінальний кодекс України : Закон України від 05.04.01 р. № 2341-III // Відомості Верховної Ради України (ВВР). – 2001. – № 25-26. – Ст. 131.

22. Кримінальне право України : загальна частина : підручник / [М.І. Бажанов, Ю.В. Баулін, В.І. Борисов та ін.] ; за ред. проф. М.І. Бажанова, В.В. Сташиса, В.Я. Тація. – [2 е вид., перероб. і допов.]. – К. : Юрінком Інтер, 2005. – 480 с.

23. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), автоматизованих систем та комп’ютерних мереж і мереж електрозв’язку. – Режим доступу : http://www.scourt.gov.ua/clients/vsu/vsu.nsf/(documents) /AFB1E90622E4446FC2257B7 C00499C02

~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~