9. Малиновський В.Я. Оптимізація функцій органів виконавчої влади України: теоретико-методологічні засади: дис... канд. політ. наук: 23.00.02 / Українська Академія держ. управління при Президентові України. – К., 2002. – 213 с.

10. Основы социального управления: [учебное пособие] / А.Г. Гладышев, В.Н. Иванов, В.И. Патрушев и др.; под ред. В.Н. Иванова. – М. : Высш. шк., 2001. – 271 с.

11. Про оптимізацію системи центральних органів виконавчої влади: Постанова Кабінету Міністрів України від 10 вер. 2014 р. № 442 // Урядовий кур'єр. – 2014 – № 169.

12. Розпорядження Кабінету Міністрів України «Деякі питання реформування державного управління України» від 24.06.2016 року № 474-р закріплено Стратегію реформування державного управління України на 2016–2020 роки. [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/474-2016-%D1%80/card4#History.

13. Сучасний словник іншомовних слів / За ред. О. Семотюк. – Х.: Ранок, 2007. – 467 с.

УДК 342.9

ГАВЛОВСЬКИЙ І.А.

АДМІНІСТРАТИВНО-ПРАВОВА ПРИРОДА ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

У статті з'ясовано адміністративно-правову природу електронного цифрового підпису в Україні. Він базується на науковій природі математичних категорій криптографії та криптоперетворення. Завдяки об'єктивній юридичній регламентації через норми адміністративного права забезпечує адміністративно-правовий та організаційно-правовий захист особистих ключів підписувачів від несанкціонованого використання, підвищує ефективність управлінської діяльності органів публічної влади та зручність користування приватними особами. Він прирівнюється до власноручного підпису (печатки) і не може заперечуватися виключно на підставі того, що він має електронну форму.

Ключові слова: *адміністративно-правова природа, адміністративно-правовий захист, електронна форма, електронний цифровий підпис, криптографія, норми адміністративного права, особисті ключі, підписувач.*

В статье выясняется административно-правовая природа электронной цифровой подписи в Украине. Научная основа её лежит в плоскости математических категорий криптографии и криптопреобразования. Благодаря объективной юридической регламентации через нормы административного права она обеспечивает административно-правовую и организационно-правовую защиту личных ключей подписчиков от несанкционированного использования, повышает эффективность управленческой деятельности органов публичной власти и удобство для пользователей. Она приравнивается к собственноручной подписи физического лица и печати юридического лица и не может оспариваться только на том основании, что имеет электронную форму.

Ключевые слова: *административно-правовая защита, административно-правовая природа, криптография, личные ключи, нормы административного права, электронная форма, электронная цифровая подпись.*

The article clarifies the administrative and legal nature of electronic digital signature in Ukraine. It based on the scientific nature of the mathematical categories of cryptography and crypto transformation. Due to objective legal regulation through the norms of administrative law provides the administrative-legal and organizational-right protection

© ГАВЛОВСЬКИЙ І.А. – здобувач (Науково-дослідний інститут публічного права)

of personal keys of signers from unauthorized use increases the efficiency of management activities of public authorities and the convenience of using private individuals. It is equivalent of a handwritten signature (stamp) and cannot be denied solely on the grounds, that it has an electronic form.

Key words: *administrative and legal protection, administrative nature, cryptography, electron shape, electronic digital signature, norms of administrative law, personal keys, signer.*

Вступ. В умовах ускладнення суспільних відносин поступово виникає якісно нова ситуація, коли накопичення постійно повторюваного одиничного суспільного досвіду приводить до виникнення нової якості, яка є більш складною за наявні раніше, одночасно більш простою для користувачів. В останній час вагомим кроком у розвитку світового суспільства є практичне використання різноманітних «крипто»-технологій, які (через те, що стають найважливішими для великої кількості осіб) починають регулюватися нормами права, зокрема нормами адміністративного права.

Серед криптологічних технологій найбільшого практичного застосування отримав електронний цифровий підпис, що зумовлює нові вимоги до безпеки особистих даних і зручності їх використання.

Проте, незважаючи на захищеність використання такого підпису нині існує велика небезпека з боку хакерських атак, тобто кіберзлочинності, яка на сьогодні заполонила майже всі країни. З розвитком та методами кіберзлочинності розвиваються і шляхи подолання цих проблем. Це зроблено для запобігання володіння чужим ключем, адже, якщо зловмисник заволодіє чужим ключем, він може потенційно від імені справжнього власника здійснювати неправомірні дії, наприклад: проводити певні грошові транзакції, змінювати записи в базах даних тощо.

У такому разі актуальним є виявлення та опис внутрішніх засад цього феномена, який практично вже використовується фізичними та юридичними особами, що підвищують ефективність своєї управлінської праці за допомогою захищених криптологічними засобами захисту і такими, що постійно модернізуються, використовуючи нові технології.

Огляд останніх досліджень. До проблеми адміністративно-правових відносин із використання електронного цифрового підпису зверталися вчені- юристи Ю. Атаманова, Н. Бааджи, І. Верес, В. Галунько, А. Гетьман, А. Дегтярьов, М. Дутов, Р. Еннан, О. Кирилюк, С. Короєд, В. Курило, В. Мілаш, С. Лур'є та ін. Проте безпосередньо до аналізованої нами проблематики вони зверталися лише під час аналізу інших більш загальних, спеціальних чи суміжних викликів.

Виклад основних положень. Електронний цифровий підпис нині є найбільш сучасним та безпечним типом електронного підпису. Він застосовується згідно з вимогами чинного законодавства і використовується у найрізноманітніших сферах українського суспільства – від електронного протоколу, що складає Національна поліція України, до використання його в банківській сфері. Електронний цифровий підпис дав змогу замінити звичайний підпис, захистивши його від злочинних посягань та використання в недобросовісних цілях для отримання певної вигоди. Міжнародна практика використання засобів електронного цифрового підпису свідчить про поширене у розвинених країнах вжиття нормативних та технічних заходів щодо захисту особистих ключів від несанкціонованого використання. Найнадійнішим варіантом такого захисту є захищений носій особистих ключів. Він має вбудовані апаратно-програмні засоби, що забезпечують захист даних від несанкціонованого доступу, зокрема, від ознайомлення із значенням параметрів особистих ключів та їх копіювання [1].

Наукова природа електронного цифрового підпису базується на категоріях криптографії та криптоперетворення. Криптографія – це практика і вивчення методів безпечного спілкування в присутності третіх осіб (так званих противників). У більш загальному понятті йдеться про побудову та аналіз протоколів, які дозволяють подолати вплив противників і які пов'язані з різними аспектами в області інформаційної безпеки, таких як конфіденційність даних, цілісність даних, аутентифікації і безвідмовності. Сучасна криптографія перетинає дисципліни математики, інформатики та електротехніки. Застосування криптографії включає таке: банківські карти, комп'ютерні паролі й електронну комерцію [2]. Криптоперетворення – це сукупність операцій шифрування та дешифрування даних [3]. А. Дегтярьов класифікує криптографічний генезис на етапи: перший етап – етап донаукової криптології (до 1949 р.); другий етап – етап наукової криптології із секретними ключами (з 1949 р. по сімдесяті роки); третій етап – етап наукової

криптології із використанням ЕОМ (із сімдесятих і дотепер). Аналізуючи наукову природу електронного цифрового підпису, слід описати алгоритми шифру, які використовуються у цифровому підписі. Алгоритми шифрування поділяють на класичні та сучасні, нас цікавлять сучасний алгоритм шифрування. Сучасні, своєю чергою, поділяються на симетричні (заміна) та асиметричні (перестановка) [2].

Симетричне шифрування потокового шифру кожного символу відкритого тексту зашифрується незалежно від інших. Головною проблемою створення потокового шифру є створення послідовності, що шифрує. Під час використання потокових шифрів вони можуть вироблятися як на передавальному, так і на прийомному кінцях лінії зв'язку. За симетричного шифрування блокових шифрів відкритий текст розбивається на блоки фіксованої довжини й зазнає шифрування. При чому кожний блок зашифровується своїм шифром, але алгоритм перемішування залишається однаковим для всіх блоків. На цьому принципі побудована велика кількість шифрів, включаючи американський стандарт DES [2].

Чинний Закон України «Про електронний цифровий підпис» дає визначення електронного цифрового підпису – це вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа [4].

Асиметричними криптоалгоритмами вважається криптосистема з відкритим ключем. Для шифрування повідомлення використовується відкритий ключ, а за дешифрування – закритий. Тобто, знаючи ключ шифрування і зашифрований текст, неможливо відновити вихідне повідомлення. У разі порушення конфіденційності робочої станції зловмисник довідається тільки «закритий» ключ: це дає йому змогу читати всі повідомлення, що приходять абонентові К., але не дає змогу видавати себе за нього під час відправлення листів. В асиметричних системах кількість наявних ключів пов'язана з кількістю абонентів лінійно [2].

В Україні електронний цифровий підпис використовується у різноманітних сферах життєдіяльності, а саме: у банківській сфері, прикордонній службі, органах виконавчої влади (поліції) тощо. Розвинуті технологічні пристрої дають змогу незаконним шляхом підробити письмовий підпис, тому на заміну письмовому підпису доречно використовувати саме електронний цифровий підпис, який дає змогу з великою ймовірністю виключити можливість незаконного підроблення документа та будь-які незаконні дії. Підписувач, який володіє особистим ключем та ставить свій підпис на програмний засіб, програмно-апаратний або апаратний пристрій, призначений для генерації ключів, накладення або перевірки електронного цифрового підпису повністю захищає себе як суб'єкт, який перебуває у правовому колі, від недобросовісних втручань.

Однак, як показують матеріали Єдиного державного реєстру судових рішень, за останні 2 роки електронний цифровий підпис був об'єктом адміністративно-правового спору більше 30 тисяч разів [5]. При цьому найбільш часто предметом позову було доведення чи спростування виключності достатності електронного цифрового підпису директора та печатки юридичної особи як юридичного факту, що не підлягає сумніву. При цьому треба зазначити, що, користуючись казуїстичними невідповідностями у чинному законодавстві, адміністративний суд, як правило, не підтверджує достовірності юридичного факту. Від такого стану речей потерпають банківські установи та бюджет України, а приватні фізичні та юридичні особи змушені у взаємодії з органами публічної влади часто дублювати електронний цифровий підпис із паперовим його варіантом. Тим самим вітчизняне суспільство поступово і не безболісно пристосувалось до новітніх технологій.

Оновлення нормативно-правової бази України щодо створення спеціальних юридичних норм сприятиме ефективному впровадженню та функціонуванню електронного документообігу та електронного цифрового підпису. Для регулювання правовідносин у сфері інформаційних технологій Верховна Рада України ухвалила певну кількість законів: «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис», «Про обов'язковий примірник документів», «Про Національну програму інформатизації», «Про телекомунікації», «Про Національну систему конфіденційного зв'язку», «Про захист інформації в інформаційно-телекомунікаційних системах».

Проте основним законом, яким регулюються адміністративно-правові відносини між колами осіб, є Закон України «Про електронний цифровий підпис». Цей Закон визначає певні адміністративно-правові аспекти. Правовий статус електронного цифрового підпису визначається

тим, що електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо: електронний цифровий підпис підтверджено із використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису; під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису; особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті. Основне юридичне призначення електронного цифрового підпису – це забезпечення діяльності фізичних та юридичних осіб, яка здійснюється із використанням електронних документів. Електронний цифровий підпис використовується лише фізичними та юридичними особами – суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі. Хоч електронний цифровий підпис має специфічний вигляд, його використання не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі. Має таку ж юридичну силу, як і письмовий підпис [4].

Застосування електронного цифрового підпису в електронному документообігу через те, що визначає правовий статус не лише електронного цифрового підпису, але й електронних документів у цілому, обов'язковим реквізитом яких є ЕЦП, який прирівнюється до власноручного підпису (печатки) тільки у разі виконання всіх трьох умов. Дві з трьох умов вимагають використання посиленого сертифіката, який є українським ноу-хау і не визначений міжнародним та Європейським законодавством, якими визначається удосконалений електронний підпис та кваліфікований сертифікат, які є міжнародними умовами визнання цифрового підпису еквівалентним власноручному та вимоги до яких дещо інші, а також не відображені у стандартах «X.5091» [6; 7].

При цьому треба зазначити, що законодавство ЄС на відміну від українського під електронним підписом розуміє не тільки ідентифікацію автора, а і достовірність/цілісність самих підписаних даних. Термін ЕЦП закону України є більш слабким, ніж визначення «удосконалений електронний підпис» Директиви ЄС, який визнається еквівалентним власноручному, оскільки для ЕЦП відсутня ключова вимога щодо забезпечення можливості автору підпису тримати під своїм повним контролем засіб створення підпису. Крім того, обов'язкові вимоги до «безпечного механізму створення підпису» Директиви ЄС відрізняються від вимоги до «надійного засобу електронного цифрового підпису» за законом України як об'єкта, що має сертифікат відповідності виключно українського походження [8].

Електронний цифровий підпис має свою законодавчу базу, в якій прописуються захисні механізми, які з більшою можливістю виключають ймовірність злочинних посягань. Цифрові підписи використовують цифровий ідентифікатор на основі сертифіката, виданого акредитованим органом сертифікації або постачальником довірчого сервісу, тому під час цифрового підписування документа підписувач однозначно прив'язує підпис до себе. Цифровий підпис створений, захищений та забезпечений найвищими рівнями безпеки. При цьому підписувач у вигляді суб'єкта має повне право: вимагати скасування, блокування або поновлення свого сертифіката ключа; оскаржити дії чи бездіяльність центру сертифікації ключів у судовому порядку. Скасування, блокування та поновлення посильного сертифіката ключа має здійснювати Акредитований центр сертифікації ключів у разі закінчення строку чинності сертифіката ключа після подання заяви власника ключа або його уповноваженого представника, припинення діяльності юридичної особи – власника ключа, смерті фізичної особи – власника ключа або оголошення його померлим за рішенням суду, визнання власника ключа недієздатним за рішенням суду, надання власником ключа недостовірних даних, компрометації особистого ключа. Скасування і блокування посиленого сертифіката ключа набирає чинності лише з моменту внесення до реєстру чинних, скасованих і блокованих посилених сертифікатів із зазначенням дати та часу здійснення цієї операції. Центральний засвідчувальний орган, засвідчувальний центр, акредитований центр сертифікації ключів негайно повідомляють про скасування або блокування посиленого сертифіката ключа його власника. Підписувач зобов'язаний: зберігати особистий ключ у таємниці, надавати центру сертифікації ключі до даних згідно з вимогами законодавства [4].

Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму. Допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму. Електронний документ не може бути застосовано як оригінал: документа, який відповідно до законодавства може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів; в інших випадках, передбачених законом [9].

У процесі розроблення, виробництва та експлуатації засобів криптографічного захисту інформації (КЗІ) беруть участь і взаємодіють між собою: замовники; розробники; виробники; організації, що експлуатують засоби КЗІ; організації, що проводять сертифікаційні випробування (експертні роботи); постачальники ключових документів. В інструкції із забезпечення безпеки експлуатації засобів криптографічного захисту інформації (КЗІ) вказуються: права та обов'язки осіб, відповідальних за забезпечення безпеки експлуатації засобу КЗІ; права та обов'язки користувачів засобів КЗІ; порядок забезпечення безпеки засобу КЗІ під час його встановлення, експлуатації, виведення з експлуатації, ремонту, знищення, а також у разі порушення функціонування інформаційно-телекомунікаційної системи; порядок обліку засобів КЗІ; питання проведення тестування засобів КЗІ та їх резервування в системі; дії персоналу в умовах надзвичайних ситуацій, стихійного лиха та підозри компрометації ключів; порядок проведення контролю за станом забезпечення безпеки засобів КЗІ; порядок допуску в приміщення, у яких установлені засоби КЗІ; порядок знищення засобів КЗІ. В інструкції щодо порядку генерації ключових даних і поводження (облік, зберігання, знищення) з ключовими документами вказуються: опис ключової системи та ключових документів; термін дії ключових даних, ключових документів; порядок генерації ключових даних, їх запису на носії ключової інформації; порядок обліку, зберігання носіїв ключової інформації та їх знищення; особливості повторного використання носіїв ключової інформації; особливості використання ключових даних за призначенням та їх знищення [10].

З 2014 року в країнах-учасницях ЄС використовується розширений електронний підпис «eIDAS», він відповідає кільком вимогам, зокрема: підписувач має бути однозначно ідентифікований та пов'язаний з підписом; підписувач мусить мати єдиний контроль над своїм ключем, який використовувався для створення електронного підпису; підписувач має бути здатний визначити, чи було змінено супровідні дані після підписання повідомлення; у тому разі, якщо супровідні дані були змінені, підпис має бути визначний недійсним [11].

Усе вищевикладене дає можливість сформулювати такі висновки щодо адміністративно-правової природи електронного цифрового підпису в Україні:

1) наукова природа електронного цифрового підпису базується на категоріях криптографії та криптоперетворення, які дають змогу подолати вплив противників і які пов'язані з різними аспектами в галузі інформаційної безпеки, таких як конфіденційність даних, цілісність даних, аутентифікації і безвідмовності;

2) електронний цифровий підпис вимагає правового (зокрема, адміністративно-правового) та технічного (організаційно-правого) захисту особистих ключів від несанкціонованого використання;

3) законодавством України визначено, що електронний цифровий підпис – це вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його юридичну цілісність та ідентифікувати підписувача;

4) в Україні для звичайних потреб (не для спеціальних державних служб) використовується зворотний асиметричний криптоалгоритм, коли підписувач володіє особистим закритим ключем та ставить свій підпис на програмний засіб, а перевіряється адресатом за допомогою відкритого ключа;

5) норми адміністративного права, які визначають юридичну природу електронного цифрового підпису зосереджені в таких основних європейських та вітчизняних джерелах: 1) міжнародно-правові джерела: Конвенція ООН про використання електронних повідомлень у міжнародних договорах (2005); Регламент ЄС від 23.07.2014 «Про електронну ідентифікацію та довірчі служби для електронних операцій на внутрішньому ринку»; 2) вітчизняні джерела: а) закони: «Про електронний цифровий підпис» (спеціальний); «Про електронні документи та електронний документообіг»; «Про обов'язковий примірник документів»; «Про Національну програму інформатизації»; «Про телекомунікації»; «Про Національну систему конфіденційного зв'язку»; «Про захист інформації в інформаційно-телекомунікаційних системах»; б) підзаконні нормативно-правові акти: Наказ Адміністрація державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 «Про затвердження «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації»;

6) основне юридичне призначення електронного цифрового підпису – це забезпечення діяльності фізичних та юридичних осіб, що здійснюється із використанням електронних документів;

7) застосування електронного цифрового підпису в електронному документообігу визначає правовий статус не лише електронного цифрового підпису, але й електронних документів у цілому, обов'язковим реквізитом яких є ЕЦП, який прирівнюється до власноручного підпису (печатки) тільки у випадку виконання всіх трьох умов.

8) допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму;

9) у цілому в Україні використовується розширений електронний підпис «eIDAS» ЄС, згідно з яким підписувач: має бути однозначно ідентифікований та пов'язаний з підписом; мати єдиний контроль над своїм ключем, має бути здатний визначити, чи було змінено супровідні дані після підписання повідомлення; у тому разі, якщо супровідні дані були змінені, підпис визнається недійсним.

Отже, адміністративно-правова природа електронного цифрового підпису в Україні полягає у тому, що він, базуючись на науковій природі математичних категорій криптографії та криптоперетворення, завдяки об'єктивній юридичній регламентації через норми адміністративного права забезпечує адміністративно-правовий та організаційно-правовий захист особистих ключів підписувачів від несанкціонованого використання (через використання закритого ключа), підвищує ефективність управлінської діяльності органів публічної влади та зручність користування приватними особами, прирівнюється до власноручного підпису (печатки) і не може заперечуватися виключно на підставі того, що він має електронну форму.

Список використаних джерел:

1. Лур'є С. Безпечність використання електронного цифрового підпису. / INVESTGAZETA. – 2016. [Електронний ресурс]. – Режим доступу : https://investgazeta.ua/blogs/bezpechnist-vikoristannya-elektronnogo-tsifrovogo-pidpisu.

2. Дегтярьов А. Методи сучасної криптографії. Криптографія: загальні визначення, класифікація, асиметричні та симетричні криптоалгоритми, їх порівняння. [Електронний ресурс]. – Режим доступу : https://dehtyarov09.wordpress.com/2014/03/16/криптографія-загальні-визначення-кл-2/.

3. Криптоперетворення. Академік. [Електронний ресурс]. – Режим доступу : https: //ukrainian_explanatory. academic.ru/74669/%D0%BA%D1%80%D0%B8%D0%BF%D1.

4. Про електронний цифровий підпис: Закон України від 22.05.2003 № 852-IV. // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 276.

5. Єдиний державний реєстр судових рішень. 2016. [Електронний ресурс]. – Режим доступу : http://reyestr.court.gov.ua/Page/1778.

6. Про систему електронних підписів, що застосовується в межах Співтовариства. Затверджена Директивою ЄС Європейського парламенту та Ради від 13.12.1999. // Верховна Рада України. [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/994_240.

7. Конвенция Организации Объединенных Наций об использовании электронных сообщений в международных договорах от 23.11.2005.// Верховна Рада України. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/995_e71.

8. Науково-практичний коментар до Закону України «Про електронний цифровий підпис. 2009. [Електронний ресурс]. – Режим доступу : http://cesaris.itsway.kiev.ua/public/Downloads/Science-practic %20 comment% 20for%20 Law%20about%20Electr%20Signature.pdf.

9. Про Національну систему конфіденційного зв'язку: Закон від 10.01.2002 № 2919-III. // Відомості Верховної Ради України. – 2002. – № 15. – Ст. 103.

10. Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації. Затверджено Наказом Адміністрація державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141. [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/z0862-07.

11. Dawn M. Advanced Electronic Signatures for eIDAS. Cryptomathic. – Retrieved 7 June 2016.

12. Верес І. Правове регулювання електронних підписів. / Підприємство, господарство і право. – 2016. – № 3.

14. Дутов М. Правове забезпечення розвитку електронної комерції: автореф. дис... канд. юрид. наук: 12.00.04. – Донецьк, 2003. – 17 с.

15. Кирилюк О. Договори, що укладаються з використанням електронних засобів зв'язку : автореф. дис. … канд. юрид. наук : спец. 12.00.03. – Київ, 2015. – 19 с.

16. Про затвердження Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації. Наказ від 12.06.2007 № 114. // Офіційний вісник України, № 50, стор. 99, стаття 2038, код акта 40341/2007

17. Про захист інформації в інформаційно-телекомунікаційних системах. Закон від 05.07.1994 № 80/94-ВР. // Відомості Верховної Ради України. –1994. – № 31. – Ст. 286.

18. Про Національну програму інформатизації: Закон України від 04.02.1998 № 74/98-ВР. // Відомості Верховної Ради України. – 1998. – № 27. – Ст. 181.

19. Про Національну систему конфіденційного зв'язку. Закон від 10.01.2002 № 2919-III. // Відомості Верховної Ради України. – 2002. – № 15. –Ст. 103.

20. Про обов'язковий примірник документів: Закон України від 09.04.1999 № 595-XIV. // Відомості Верховної Ради України від 11.06.1999. –№ 22. – Ст. 199.

21. Про систему електронних підписів, що застосовується в межах Співтовариства. Директива 1999/93/ЄС Європейського парламенту та Ради. 1999. // Офіційний журнал L 013, 19/01/2000 с.0012-0020.

22. Про телекомунікації: Закон від 18.11.2003 № 1280-IV. // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.

24. eIDAS Regulation (Regulation (EU) №°910/2014). European Commission. 2014. [Електронний ресурс]. – Режим доступу : https://ec.europa.eu/futurium/en/eidas-observatory/blogs.

25. What are digital signatures? Transform business processes with electronic and digital signatures. 2016. Mode access: https://acrobat.adobe.com/us/en/sign/capabilities/digital-signatures-faq.html.

УДК 342.9

ДАВИДОВА Н.В.

ВИЗНАЧЕННЯ ПОНЯТТЯ ПРОПАГАНДИ БЕЗПЕКИ ДОРОЖНЬОГО РУХУ НА СУЧАСНОМУ ЕТАПІ

Стаття присвячена проблематиці поняття пропаганди безпеки дорожнього руху. Проаналізовано літературу з дослідження поняття пропаганди безпеки дорожнього руху. Сформульовано авторське визначення поняття «пропаганда безпеки дорожнього руху». Вказано на відсутність у законодавстві України визначення пропаганди безпеки дорожнього руху.

Ключові слова: *безпека дорожнього руху, пропаганда, профілактика, попередження дорожньо-транспортних пригод, пропаганда безпеки дорожнього руху.*

Статья посвящена проблематике понятия пропаганды безопасности дорожного движения. Осуществляется анализ литературы по исследованию понятия пропаганды безопасности дорожного движения. Формулируется авторское определение понятия «пропаганда безопасности дорожного движения». Указывается на отсутствие в законодательстве Украины определения пропаганды безопасности дорожного движения.

Ключевые слова: *безопасность дорожного движения, пропаганда, профилактика, предупреждение дорожно-транспортных происшествий, пропаганда безопасности дорожного движения.*

© ДАВИДОВА Н.В. – завідувач навчально-методичної лабораторії криміналістики при кафедрі адміністративного і кримінального права (Дніпровський національний університет імені Олеся Гончара)