УДК 342.373.5.016:30

Оксана Сірант
Інститут права імені Володимира Великого МАУП
здобувач кафедри адміністративного права
Myroslava_55@mail.ru

ЦИФРОВІ ДОКАЗИ, УТВОРЕНІ ІЗ ЗАСТОСУВАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРОВАДЖЕННІ У СПРАВАХ ПРО АДМІНІСТРАТИВНІ ПРАВОПОРУШЕННЯ

Розглянуто теоретичні аспекти дослідження цифрових доказів, утворених із застосуванням інформаційно-комунікаційних технологій у провадженні у справах про адміністративні правопорушення з позиції динамічних інформаційних систем із застосуванням синергетичного підходу і інформаційної генотипології інформаційних систем з погляду на аналогічні дослідження в Європейському Союзі. Проаналізовано правопорушення, передбачені Кодексом України про адміністративні правопорушення, де інформація, утворена із застосуванням інформаційно-комунікаційних технологій, може бути безпосереднім об'єктом правопорушення.

Ключові слова: інформація; доказ; інформаційно-комунікаційні технології; справа про адміністративне правопорушення; цифрові докази.

Оксана Сирант

ЦИФРОВЫЕ ДОКАЗАТЕЛЬСТВА ОБРАЗОВАНЫ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОИЗВОДСТВЕ ПО ДЕЛАМ ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ

В статье рассматривается теоретические аспекты исследования цифровых доказательств образованных с применением информационно-коммуникационных технологий в производстве по делам об административных правонарушениях с позиции динамических информационных систем с применением синергетического подхода и информационной генотипологии информационных систем с точки зрения аналогичные исследования в Европейском Союзе. Анализируются правонарушения предусмотренные Кодексом Украины об административных правонарушениях где информация образована с применением информационно-коммуникационных технологий может быть непосредственным объектом правонарушения.

Ключевые слова: информация; доказательство; информационно-коммуникационные технологии; дело об административном правонарушении; цифровые доказательства.

Oksana Sirant
Law Institute of Vladimir the Great
Interregional Academy of Personnel Management
Researcher of the Department of Administrative Law

DIGITAL EVIDENCE IS ESTABLISHED FOR THE APPLICATION OF INFORMATION TECHNOLOGIES IN MANUFACTURE ON AFFAIRS ABOUT ADMINISTRATIVE OFFENCES

In the article the theoretical aspects of the study of digital evidence generated using information and communication technologies in the proceedings in cases of administrative offenses from the perspective of dynamic information system using a synergistic approach henotypolohiyi information and information systems in view of similar studies in the European Union. Analyzes the offense the Code of Ukraine on Administrative Offences where information is created using information and communication technologies can be the target of the offense.

Key words: information; evidence; information and communication technologies; case on administrative offense; digital evidence.

Постановка проблеми. Сучасний етап розвитку суспільства характеризується зростанням ролі інформаційного середовища, що представляє сукупність інформації, інформаційної інфраструктури, суб'єктів, які збирають, формують, розповсюджують, використовують інформацію та систему регулювання суспільних відносин. Інформаційна сфера, будучи системо утворювальним чинником життя суспільства, активно впливає на стан політичної, економічної, оборонної та інших складових безпеки України. Одними з засобів, що забезпечує нормальне функціонування інформаційної сфери, є адміністративно-юрисдикційні засоби. Методи та підходи до аналізу адміністративно-юрисдикційних засобів взаємозв'язані зі стрімкими темпами змін в інформаційних технологіях, з трансформаціями соціальних відношень, з реформуванням соціальних інститутів.

Аналіз дослідження проблеми. Проблематику дослідження доказів в адміністративному праві в контексті впровадження інформаційно-комунікаційних технологій розглядали вчені: О. Андрійко, В. Біленко, Н. Бортник, І. Голосніченко, Є. Додін, С. Єсімов, Г. Жозеф, Р. Калюжний, Т. Коломоєць, В. Колпаков, В. Ортинський, О. Остапенко, А. Селіванов та ін. У цей час у юридичній науці мало комплексних досліджень цифрових доказів утворені із застосуванням інформаційних технологій у провадженні у справах про адміністративні правопорушення.

Метою статті є аналіз цифрових доказів утворених із застосуванням інформаційних технологій у провадженні у справах про адміністративні правопорушення.

Виклад основного матеріалу. Більшість процесів, що відбуваються у суспільстві, є нелінійними і потребують спеціальних підходів і нової методології до аналізу та дослідження складних юридичних проблем. Використання синергетичного підходу не суперечить класичним методам та підходам до аналізу юридичних процесів, водночас є суттєвим доповненням, що значно розширює методологічний апарат правознавства. Застосування синергетичного підходу в дослідженнях юридичних аспектів інформаційної сфери отримує власну специфіку за рахунок характерних властивостей і особливостей інформаційно-технологічних і комунікаційних систем, пов'язаних з їхньою структурною складністю.

Інформація утворена із застосуванням інформаційно-комунікаційних технологій як доказ у справі про адміністративне правопорушення є однією з різновидів інформації, якій властиві ознаки загального поняття інформації. Але водночас необхідно враховувати специфічні особливості,

притаманні цьому виду інформації, які визначають її як окрему доказову категорію. Наше бачення цієї проблеми основується на доказах щодо інформації, що їх навів Є. Додін у навчальному посібнику "Доказательства в административно-юрисдикционной деятельности органов внутренних дел" [1, с. 32].

Інформаційні зв'язки є основою всіх соціальних взаємодій, під час дослідження яких доцільно використовувати інформаційний, системний і організаційний підходи так, як системне або організаційне явище основане на інформаційних взаємодіях. Вивчаючи основні форми та види інформаційних взаємодій, можливо визначити інформаційний простір юридичної системи.

Інформаційний підхід щодо інформації, яка утворена із застосуванням інформаційно-комунікаційних технологій дає можливість визначити належність інформації: фізичній чи юридичній особі, або створеній програмним забезпеченням.

Системний підхід щодо інформації утвореної із застосуванням інформаційно-комунікаційних технологій, як доказ у справах про адміністративне правопорушення, дає можливість визначити: середовище існування інформації (файл); метод перетворення інформації з електронного виду на доступну для сприйняття форму, на підставі чого суддя або посадова особа, яка розглядає матеріали може визначити значення для справи.

Інформація може вважатися доказом, якщо вона має значення для справи та дає можливість встановити наявність або відсутність обставин, що підлягають доказуванню [2, с. 96].

Організаційний підхід щодо інформації, утвореної із застосуванням інформаційно-комунікаційних технологій як доказ у справах про адміністративне правопорушення дає можливість встановити допустимість, тобто відповідність законним вимогам щодо отримання.

Інформація, утворена із застосуванням інформаційно-комунікаційних технологій як доказ у справах про адміністративне правопорушення, представляє фактичні дані, відображені у формі, доступній для сприйняття людиною, що мають значення для справи та отримана у законний спосіб і представлена у вигляді файла [3, с. 314].

Інформація утворена із застосуванням інформаційно-комунікаційних технологій може бути безпосереднім об'єктом правопорушення (ст. 51-2 "Порушення прав на об'єкт права інтелектуальної власності"; ст. 188-7 "Невиконання законних вимог національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації"; ст. 188-31 "Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України"; ст. 188-39 "Порушення законодавства у сфері захисту персональних даних" КУпАП) і доказом у проваджені у справі про адміністративне правопорушення.

Як зазначають В. Разумов, В. Сізіков, автори монографії "Основы теории динамических информационных систем", для кожної категорії в динамічних інформаційних системах можливе її дешифрування у самостійну динамічну інформаційну систему, слідом за цим необхідний облік проявів у ній феномена рішення зворотних завдань як одного з актів процесу інформаційного функціонування динамічних інформаційних систем [4, с. 33].

Тому необхідно розмежувати об'єкти у сфері інформаційно-комунікаційних технологій за функціональним призначенням, які в подальшому можуть отримати статус цифрового доказу у провадженні у справах про адміністративні правопорушення:

– програмні продукти (операційні системи та програмні комплекси), які під час діагностики стану мають несанкціоновані зміни у наслідок пошкодження, видалення й інших технологічних втручань, не передбачених системою опрацювання інформації або втручання шкідливих програм і процесів [5, с. 315];

– інформація, яку створює комп'ютер автоматично під час роботи користувача, і існує в певний файловій системі комп'ютера (файлах історії, тимчасових файлах тощо). У зв'язку з розвитком форензіки (комп'ютерної криміналістики) ця інформація є найпоширенішою серед цифрових доказів (технологічно складно внести зміни без втручання в програмний комплекс. Це виявляється SimCOSAR – програмним комплексом дискретно-подійного імітаційного моделювання систем моніторингу) [6, с. 132–133];

– інформація, яка цілеспрямовано стерта користувачем персонального комп'ютера або програмним засобом, комп'ютерним технологічним засобом;

– інформація, що перебуває на знімних носіях (планшетах, знімних жорстких дисках, оптичних дисках, картах флеш-пам'яті, смартфонах тощо);

– інформація, що розміщена в локальних комп'ютерних мережах (корпоративних, операторів мобільного зв'язку, операторів локальних і глобальних навігаційно-моніторингових систем) [7].

Для найефективнішого дослідження цифрових доказів за допомогою теорії інформації доцільно класифікувати інформаційні повідомлення, які покладено в інформаційну основу доказів, на: фактичні (об'єктивні, аргументовані факти), емоційні (суб'єктивне відношення до наявних фактів), конкретні (наявні факти в цей момент), абстрактні (факти, які не існують).

Інформаційна структура цифрових доказів становить сукупність елементів, яка бере участь в інформаційних взаємодіях усієї системи (на інформаційному та технічному рівнях). Під інформаційною структурою розуміють сукупність системних елементів, що визначають зовнішню та внутрішню інформаційну взаємодію. Цифрові докази є нематеріальними об'єктами.

Інформаційну структуру цифрових доказів доцільно подати у вигляді типової моделі, яка містить системні елементи, що: генерують інформацію; розподіляють інформацію; зберігають інформацію; передають інформацію.

Указана модель відображена у теорії інформаційних технологій. Узагальнюючи дослідження українських і закордонних вчених, класифікація цифрових доказів може здійснюватися за підставами:

– відповідно до походження – зберігаються на знімних носіях у цифровій формі, зберігаються у електронно-обчислювальному комплексі;

– відповідно до інтелектуального походження – на створені людиною і створені програмним комплексом;

– відповідно до форми надання – в цифровій формі на електронному носію (флеш-картах, жорстких дисках тощо), на екрані монітора [8, с. 64–65; 67–68].

Законодавство України в низці нормативно-правових актів регулює правовідносини в цій сфері. У КУпАП передбачено адміністративну відповідальність за порушення прав на об'єкт права інтелектуальної власності (ст. 51-2), невиконання законних вимог Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації (ст. 188-7); невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України (ст. 188-31); порушення законодавства у сфері захисту персональних даних (ст. ст. 188-39).

У ст. 188-39 КУпАП передбачено настання відповідних правових наслідків у разі порушення порядку збирання, зберігання, використання та поширення інформації про персональні дані. Вказане охоплює неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про оброблення персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей, невиконання законних вимог Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних, недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних [9, с. 206]. Персональні дані перебувають під захистом Закону України від 01.06.2010 № 2297-VI "Про захист персональних даних", де визначено поняття персональних даних як інформації, що належить до певної або на підставі якої визначається фізична особа (ініціали, дата та місце народження, адреса проживання, займана посада і професія тощо). Ця інформація має особливі властивості, забезпечує ідентифікацію конкретної особи та відноситься до категорії конфіденційної інформації доступ до якої обмежено законом. Винятком можуть слугувати: загальнодоступні персональні дані; дані, надані за згодою власника; знеособлені персональні дані для статистичних чи інших наукових цілей тощо. Захист персональних даних, крім зазначеного вище Закону, визначено в ст. 32 Конституції України, яка встановлює конституційну заборону на відповідний обіг персональних даних без згоди власника. Обмеження можуть бути тільки на підставі рішення суду або в інших передбачених законом випадках.

Об'єктами протиправних посягань можуть стати персональні дані, що містяться у локальних комп'ютерних мережах, у персональному комп'ютері користувача, в комп'ютерних базах даних і іншої інформації про громадян, що міститься в мережі Інтернет. Подібними правопорушеннями можуть бути незаконне копіювання, поширення, опублікування інформації про персональні дані, захищені законом, незаконне використання інформації про персональні дані, яка міститься в комп'ютерних системах або мережах, призначених для зберігання, обміну, поширення інформації з метою отримання прибутку.

Указаним правопорушенням властива власна доказового база, яка з урахуванням специфіки правопорушення складається з цифрових доказів.

Результати досліджень у межах спільної програми Ради Європи та Європейського Союзу "Зміцнення інформаційного суспільства в Україні" [10], у галузі соціальних інформаційних процесів щодо персональних даних не відображають повною мірою інформаційну структуру цієї проблеми, розглянуто тільки соціальну складову, не враховуючи технічний вимір інформації. Відсутність точної теоретичної та емпіричної інтерпретації цифрових доказів не дає можливості узагальнити результати та застосувати їх у інших сферах.

У цьому разі доцільно відмітити ще декілька проблем. По-перше, відсутність єдиного напряму і єдиних завдань; по-друге, наявні дослідження недостатньо охоплюють технічну складову інформації; по-третє, практично не використовуються закони теорії інформації, без яких використання цифрових доказів під час дослідження захисту персональних даних мало ефективне.

У контексті головного напряму предмета інформаційної генотипології як розділу теорії динамічних інформаційних систем, присвяченого дослідженню процедур регулювання, що основуються на принципі саморозвитку, ефективність правового захисту персональних даних залежить від ефективності адміністративно-юрисдикційної практики. Це потребує вивчення поведінки процесу інформаційного функціонування динамічної інформаційної системи, якою є нормативно-правове регулювання захисту персональних даних, за різних обмежень на визначення доказів. Базовим прикладом для формування відповідних завдань є проблема розвитку, у цьому разі, цифрових доказів. [4, с. 166].

Отже, елементи механізму правого регулювання адміністративної відповідальності за порушення законодавства у зазначеній сфері, так або інакше, між собою взаємозв'язані і утворюють певну систему, де кожний з елементів, зокрема процесуальне регулювання цифрових доказів, має своє значення.

Існують інші види правопорушень у сфері інформаційно-комунікаційних технологій. Статтею 188-31 "Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України" КУпАП передбачена адміністративна відповідальність за порушення правил захисту інформації, яка містить у собі безліч складів у цій галузі, спрямованих на захист інформації, які поділяються на:

– невиконання вимог щодо усунення порушень законодавства про криптографічний і технічний захист державних інформаційних ресурсів;

– невиконання вимог щодо усунення порушень законодавства про інформацію з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– порушення законодавства у сфері надання послуг електронного цифрового підпису.

Дані правовідносини регулюються нормативно-правовими актами України, адаптованими до вимог Європейського Союзу, Законами України: від 21.01.1994 р. № 3855-XII "Про державну таємницю", від 22.05.2003 р. № 852-IV "Про електронний цифровий підпис", від 02.10.1992 р. № 2657-XII "Про інформацію"; іншими нормативно-правовим актами: Переліком відомостей, що не становлять комерційної таємниці, Зводом відомостей віднесених до державної таємниці, Переліком відомостей, що становлять службову інформацію в системі МВС України і інші.

Розглянуті вище склади доцільно зарахувати до правопорушень сфери інформаційно-комунікаційних технологій, вчинення яких підлягає відповідному доведенню з використанням нових видів доказів – цифрових [7].

У сфері інформаційно-комунікаційних технологій інформація, яка є її складовою, повинна бути належно захищена, що є головним завданням Національної комісії, що здійснює державне регулювання у сфері зв'язку і інформатизації та Державної служби спеціального зв'язку та захисту інформації України [11; 12, с. 84–85]. На це спрямовані норми статей 188-7, 188-31 КУпАП, які передбачають настання адміністративної відповідальності за незаконну діяльність у сфері зв'язку, інформатизації, телекомунікацій, захисту інформації. Ці правовідносини регулюються Законом України "Про інформацію", в якому встановлені вимоги щодо захисту інформації та передбачається відповідальність за правопорушення нормативних вимог.

Захист інформації з обмеженим доступом, яка може бути об'єктом правопорушення в сфері інформаційно-комінікаційних технологій, забезпечується ст. 212-5 "Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію" КУпАП, яка передбачає адміністративну відповідальність за розголошення службової інформації (з обмеженим доступом). Вказана норма Закону поширюється на категорії інформації, яка є конфіденційною, крім інформації, що належить до державної таємниці. До зазначеної інформації зараховують відомості, що стосуються таємниці слідства і судочинства; службової таємниці; професійної (лікарська, нотаріальна, адвокатська) комерційної таємниці тощо [13, с. 136].

Стаття 212-2 "Порушення законодавства про державну таємницю" КУпАП передбачає відповідальність за:

– безпідставне засекречування інформації;

– надання грифа секретності матеріальним носіям конфіденційної або іншої таємної інформації, яка не становить державної таємниці, або ненадання грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставне скасування чи зниження грифа секретності матеріальних носіїв секретної інформації;

– невиконання норм і вимог криптографічного та технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення її конфіденційності, цілісності і доступності.

Стаття 212-6 "Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем" КУпАП передбачає адміністративну відповідальність за здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах, зокрема стосовно інформаційних систем, призначених для зберігання та оброблення інформації з обмеженим доступом, незаконне копіювання інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі, незаконне розповсюдження інформації або незаконний збут інформації, яка зберігається в інформаційних системах, у паперовій чи електронній формі.

КУпАП містить норми, що регулюють відповідальність у сфері інформаційно-комунікаційних технологій. Відповідно до теорії динамічних інформаційних систем наявність чітко визначеного складу правопорушення дає змогу визначитися з вибором типів інформації і одночасно тримати на обліку весь сектор визначених значень (у нашому випадку елементів складу правопорушення), що є найважливішим для практики ідентифікації. Водночас відсутність положення щодо використання феномена інваріантності значення (у нашому випадку цифрового доказу) у блоці ідентифікації вносить труднощі в організацію регулювання [4, с. 177]. Прикладами правопорушень, під час доведення яких можна використати цифрові докази, є:

– незаконне копіювання, поширення або опублікування неліцензійного програмного забезпечення без повідомлення про це правовласника, розробника;

– продаж або здавання в прокат неліцензійного програмного забезпечення;

– незаконне використання комп'ютерних програм, комп'ютерних відеоігор з метою отримання доходу у випадках, коли ці екземпляри є контрафактними або містять неправдиву інформацію про їх правовласників тощо [6].

Законне використання та поширення програмного забезпечення, програмних продуктів і комплексів передбачає наявність ліцензійних угод з правовласниками. Здебільшого угода містить,

окрім обмежень, право на отримання оновлень, додавань, що їх розробляє виробник для покращення початкового програмного продукту. Користувач на підставі ліцензії має право встановлювати, використовувати, отримувати доступ, відображати та запускати одну копію програмного продукту на одному персональному комп'ютері, яким може бути робоча станція, термінал, планшет і смартфон, що підтримують 3G, UMTS, HSPDA-технології, або інший пристрій (наприклад, розумний годинник (англ. Smartwatch).

Висновки. Системологія доказів, утворених із застосуванням інформаційно-комунікаційних технологій, представлена у офіційно прийнятих наукових концепціях більшості країн ЄС як сукупність наукових знань, які складають зміст загальної системології права та теорій адміністративного й інформаційного права, що містить наукові поняття та функціонально-логічну декомпозицію об'єкта та предмета, базову концепцію системи фундаментальних принципів; об'єктивні, суб'єктивні та формальні джерела;. Система доказів, утворених із застосуванням інформаційно-комунікаційних технологій у законодавстві України, представлена як цілісне складне утворення, яке швидко розвивається та охоплює основні багатоаспектно взаємнопов'язані інститути різних галузей права, предметні інформаційні відношення, на розвиток яких суттєво впливає науковий рівень теорії та системології інформаційного права.

СПИСОК ЛІТЕРАТУРИ

1. Додин Е. В. Доказательства в административно-юрисдикционной деятельности органов внутренних дел : учеб. пособ. / Е. В. Додин. – К. : НИ и РИО Киев. высш. школы МВД, 1985. – 100 с. 2. Казачук І. В. Використання у доказуванні електронних джерел фактичних даних в адміністративно-деліктному процесі / І. В. Казачук // Європейські перспективи. – 2014. – № 6. – С. 93–97. 3. Мурадов В. В. Електронні докази: криміналістичний аспект використання / В. В. Мурадов // Порівняльне правознавство. – 2013. – № 3–2. – С. 313–315. 4. Разумов В. И. Основы теории динамических информационных систем : монография / В. И. Разумов, В. П. Сизиков / Вступ. ст. А. А. Романюха. – Омск : Изд-воОмГУ, 2005. – 214 с. 5. J. Raymond Greene. Encyclopedia of Police Science / Jack Raymond Greene. – Vol. 2 ; 3rd ed. – London : Taylor Francis Ltd, United Kingdom, 2014. – 1678 p. 6. Земсков И. ASimcosar: программный комплекс моделирования процесса мониторинга состояния информационного поля Интернет / И. А. Земсков // Журнал Математические структуры и моделирование. – 2013. – Вып. 1 (11). – С. 128–157. 7. Mali P. Electronic Evidence & Cyber Law / PrashantMali // CSI Communications, September 2012. – P. 30–31 [Електронний ресурс]. – Режим доступу: http://www.csi-india.org/c/document_library/get_file?uuid=d817e5eb-ca5a-40c2-b8aa-d6302c26443a&groupId=10157. 8. Sommer P. Digital Evidence, Digital Investigationsand E-Disclosure: A Guide to Forensic Readiness for Organizations, Security Advisersand Lawyers / Peter Sommer. – [3rd ad.]. – [Mar. 2012]. – 115 p. [Електронний ресурс]. – Режим доступу: https://cryptome.org/2014/03/digital-investigations.pdf. 9. Єсімов С. С. Захист персональних даних у контексті розвитку динамічних інформаційних систем / С. С. Єсімов // Наук. вісник Львів. держ. ун-ту внутр. справ. Серія юридична. – 2013. – Вип. 3. – С. 198–208. 10. Захист персональних даних: Правове регулювання та практичні аспекти : наук.-практ. посіб. / М. В. Бем, І. М. Городиський, Г. Саттон, О. М. Родіоненко. – К. : К.І.С., 2015. – 220 с. 11. Річний звіт за 2015 рік Національної комісії, що здійснює державне регулювання у сфері зв'язку і інформатизації. Офіційний веб-портал НКРЗІ. 29 березня 2016 року. [Електронний ресурс]. – Режим доступу: http://nkrzi.gov.ua/images/upload/142/6128/ZVIT_NCCI_2015.pdf. 12. Галинська К. Ю. Застосування заходів адміністративного запобігання порушень інформаційного правопорядку в Україні / К. Ю. Галинська // Правова інформатика. – 2014. – № 1(41). – С. 81–87. 13. Хитра О. Л. Визначення адміністративно-правової відповідальності осіб за порушення законодавства про інформацію / О. Л. Хитра // Юрид.наук. електронний журнал. – 2015. – № 3. – С.135–138.

REFERENCES

1. Dodyn E. V. ***Dokazatel'stva v admynystratyvno-yurysdyktsyonnoy deyatel'nosty orhanov vnutrennykh del*** [The evidence in the administrative and jurisdictional activity of law enforcement bodies: Textbook. Collec.]. Kiev, NIand RIO, MVD, 1985, 100 p. 2. Kazachuk I. V. ***Vykorystannya u dokazuvanni elektronnykh dzherel faktychnykh danykh v administratyvno-deliktnomu protsesi*** [Vikoristannya in dokazuvanni Jerel E-factuality danih in administrativno-deliktnomu protsesi]. A Europeanperspective, Vol. 6, 2014, pp. 93–97. 3. Muradov V.V ***Elektronni dokazy: kryminalistychnyy aspekt vykorystannya*** [Electronicevidence: a forensicaspect]. Comparativelaw, Vol. 3–2, 2013, pp. 313–315. 4. Razumov V. Y. ***Osnovy teorii dinamicheskikh informatsionnykh sistem: monografiya*** [Fundamentals of the theory of dynamic information systems: monograph]. Omsk: PublishinghouseOmSU, 2005, 214 p. 5. ***J. Raymond Greene Encyclopedia of Police Science:*** vol. 2; 3rd ed. / Jack Raymond Greene. – London : Taylor Francis Ltd, United Kingdom, 2014. – 1678 p. 6. Zemskov Y. A ***Simcosar: programmnyi kompleks modelirovaniya protsessa monitoringa sostoyaniya informatsionnogo polya Internet*** [Simcosar: simulation software package for monitoring the state of the information field of the Internet process]. JournalofMathematicalstructuresandmodeling, Vol. 1 (11), 2013, pp. 128–157. 7. Mali P. ***ElectronicEvidence&CyberLaw*** / PrashantMali // CSI Communications, September 2012, pp. 30–31. Availadleat: http://www.csi-india.org/c/document_library/get_file?uuid=d817e5eb-ca5a-40c2-b8aa-d6302c26443a&groupId=10157. 8. Sommer P. ***Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers*** / Peter Sommer, 115 p. Availadleat: https://cryptome.org/2014/03/digital-investigations.pdf. 9. Yesimov S. S. ***Zakhyst personal'nykh danykh u konteksti rozvytku dynamichnykh informatsiynykh system*** [Protection of personal data in the context of dynamic information systems]. Herald of National University “Lviv Polytechnic”.Series.Legal science, 2013, Vol. 3, pp. 198–208. 10. Zakhyst personal'nykh danykh: Pravove rehulyuvannya ta praktychni aspekty : nauk.-prakt. posib. [Personal data protection: legal regulation and practical aspects: nauk. and practical. guidances.]. Bem M. V., Horodys'kyy I. M., Satton H., Rodionenko O. M. Kiev, K.I.C. Publ., 2015, 220 p. 11. Richnyy zvit za 2015 rik Natsional'noyi komisiyi, shcho zdiysnyuye derzhavne rehulyuvannya u sferi zv’yazku i informatyzatsiyi. Ofitsiynyy veb-portal NKRZI. 29 bereznya 2016 roku. [Annual Report 2015 of the National Commission for State Regulation of Communications and Informatization. Official Web Portal NCRC. March 29, 2016.]. Availadleat: http://nkrzi.gov.ua/images/upload/142/6128/ZVIT_NCCI_2015.pdf. 13. Halyns'ka K. Yu. ***Zastosuvannya zakhodiv administratyvnoho zapobihannya porushen' informatsiynoho pravoporyadku v Ukrayini*** [The use of administrative measures to prevent violations of information law in Ukraine]. LegalInformatics, 2014, Vol. 1 (41), pp. 81–87. 13. Khytra O. L. ***Vyznachennya administratyvno-pravovoyi vidpovidal'nosti osib za porushennya zakonodavstva pro informatsiyu*** [The definition of administrative and legal responsibility in case of violation of legislation on information]. Legal. Sciences. electronic journal, *2015*, Vol. 3, pp. 135–138.

Дата надходження: 26.12.2016 р.