

ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УДК 343.452; 343.353.12

**ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ
ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ**

Коваленко Є. В.,

кандидат юридичних наук,
завідувач спеціальної кафедри № 3
Інституту підготовки юридичних кадрів
для Служби безпеки України
Національного юридичного університету
імені Ярослава Мудрого,
м. Харків

Анотація: у статті розглянуто питання щодо визначення сутності інформації з обмеженим доступом як елемента інформаційної безпеки держави. Аналізуються форми та види такої інформації залежно від нормативно-правових актів, що їх регламентують, належності до відповідного об'єкту кримінально-правової охорони та їх належності до конфіденційної або таємної інформації. Зроблено висновок, що саме суспільна (громадська, загальна) небезпека завжди була і об'єктивно залишається ключовою ознакою встановлення підстав кримінальної відповідальності у разі вчинення несанкціонованого доступу до інформації з обмеженим доступом як елемента інформаційної безпеки держави.

Ключові слова: інформація з обмеженим доступом; конфіденційна інформація; таємна інформація; інформаційна безпека держави.

Аннотация: в статье рассмотрены вопросы определения сущности информации с ограниченным доступом как элемента информационной безопасности государства. Проанализированы формы и виды такой информации в зависимости от нормативно правовых актов, которые их регламентируют, принадлежности к соответствующему объекту уголовно-правовой охраны и их отнесения к конфиденциальной или тайной информации. Сделан вывод, что именно общественная (социальная, общая) опасность всегда была и объективно остается ключевым признаком установления оснований уголовной ответственности в случае совершения несанкционированного доступа к информации с ограниченным доступом как элемента информационной безопасности государства.

Ключевые слова: информация с ограниченным доступом; конфиденциальная информация; тайная информация; информационная безопасность государства.

Annotation: in the article the questions of determination of essence of information are examined with the limited access as an element of informative safety of the state. Forms and types of such information are analysed depending on normatively legal acts which they are regulated, belongings to the proper object of penal guard and their attributing to confidential or secret information. Drawn a conclusion, that exactly a public (social, general) danger always was and objectively remains the key sign of establishment of grounds of criminal responsibility in the case of feasant of unauthorized division to information with the limited access as an element of informative safety of the state.

Key words: information with the limited access; confidential information; private information; informative safety of the state.

В умовах розвитку інформаційного суспільства, вдосконалення сучасних інформаційних технологій, збільшення частки надання державних послуг в електронному вигляді, повсюдному запровадженню електронного документообігу, з одного боку підвищуються обсяги інформації, щодо якої обмежується доступ, з іншого – збільшується ймовірність ризиків, пов'язаних з існуванням загроз несанкціонованого доступу до такого роду інформації. Захист інформаційних ресурсів від несанкціонованого доступу, знімання інформації засобами технічних розвідок, забезпечення безпеки інформаційних і телекомунікаційних систем також є одним з основних національних інтересів в інформаційній сфері [6, с. 99]. Для забезпечення безпеки інформації необхідно вирішити завдання забезпечення конфіденційності, цілісності та доступності, що неможливо без належної кримінально-правової охорони інформації з обмеженим доступом.

Як зазначає Н. А. Савінова, збільшення значення для соціуму інформації, знань, інформаційно-комунікаційних технологій і комунікації, усвідомлення значення спілкування, у т.ч. з точки зору можливості ураження свідомості, не може не вплинути на перегляд підходів правової і кримінально-правової політики та загальної оцінки їх не лише як до цінностей, а і як до засобів створення системи цінностей [23, с. 172]. На сьогодні у галузі інформаційних відносин можна виділити декілька основних проблем забезпечення охорони інформації з обмеженим доступом, що пов'язані з недоліками правового врегулювання співвідношення прав та обов'язків учасників інформаційних відносин у питаннях захисту інформації з обмеженим доступом. Наразі законодавством не досить чітко визначений порядок набуття прав на інформацію, особливо створену за допомогою електронно-обчислювальної техніки (комп'ютерів), а також права громадянина розпоряджатися інформацією про себе.

Потребують більш чіткого визначення і питання щодо виду та обсягу інформації з обмеженим доступом як конфіденційної для службового користування, комерційно-конфіденційної або конфіденційно-професійної інформації (лікарської, адвокатської, банківської таємниці тощо) є інформацією з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації; визначення процедури визнання відповідних відомостей такою інформацією та зняття необґрунтованих обмежень щодо доступу до неї, а також чітке визначення підстав відповідальності суб'єктів інформаційних відносин у питаннях використання такої інформації та забезпечення її охорони. На думку окремих науковців, державно-правове регулювання інформаційних правовідносин має поширюватися виключно на інформацію з обмеженим доступом, яка пов'язана з відомостями, що становить державну або іншу передбачену законом таємницю, є конфіденційною інформацією, становить державний інформаційний ресурс або є інформацією про особу (її персональні дані) [22, с. 9–10].

Водночас, визначення в законі про кримінальну відповідальність такого предмету злочину як інформація з обмеженим доступом не є новелою кримінального законодавства. Питанням кримінально-правової охорони інформації з обмеженим доступом завжди приділялося багато уваги. Але такого роду інформація є неоднорідною за своїм змістом, соціальним значенням та правовим режимом. Так, відповідно до інформаційного листа Вищого Господарського Суду України від 28 березня 2007 року № 01-8/184 [13], інформація з обмеженим доступом за своїм правовим режимом поділяється на таємну і конфіденційну.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі, а тому доступ до неї здійснюється відповідно до законів про цю інформацію. До кола таємної інформації відносяться, зокрема: відомості в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (ч. 2 ст. 4 Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» [14]), секретна інформація та відомості військового характеру, що визнаються державною таємницею згідно Закону України «Про державну таємницю» [12]; інформація, що визнається банківською таємницею (ст. 1076 Цивільного кодексу України [27] (далі – ЦК України), статті 60–62 Закону України «Про банки і банківську діяльність» [9]; відомості, що становлять лікарську таємницю (ст. 40 Закону України «Основи законодавства України про охорону здоров'я» [7]), таємниці усиновлення (удочеріння) (ст. 226 Сімейного кодексу України [24]), адвокатську таємницю (ст. 22 Закону України «Про адвокатуру та адвокатську діяльність» [8]), таємницю вчинюваних нотаріальних дій (ст. 8 Закону України «Про нотаріат» [17]), таємницю голосування (ч. 4 ст. 67 Закону України «Про вибори народних депутатів України» [10]), таємницю листування (ст. 31 Конституції України [2]), професійної таємниці (ст. 31 Закону України «Про фінансові послуги та державне регулювання ринків фінансових послуг» [21], ст. 16 Закону України «Про Рахункову палату» [19], п. 25 ст. 8 Закону України «Про державне регулювання ринку цінних паперів в Україні» [11]).

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. Особи, які володіють конфіденційною інформацією, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту. До кола конфіденційної інформації у сфері господарювання (підприємницької діяльності) відноситься інформація про нові рішення і технічні знання (ст. 862 ЦК України [27]), комерційна таємниця (статті 505–508 ЦК України), «ноу-хау» (ст. 1 Закону України «Про інвестиційну діяльність» [15]). Також законодавство визначає і інші види конфіденційної інформації, а саме: конфіденційну інформацію про особу (ст. 32 Конституції України [2]), відомості, які потерпілий чи його близькі родичі бажують зберегти в таємниці (ст. 189 Кримінального кодексу України [3] (далі – КК України) та конфіденційну інформацію, яка є власністю держави (абз. 14 ч. 2 ст. 47 Закону України «Про інформацію» [16]), інформацію в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (ч. 2 ст. 4 Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» [14]).

У разі незаконного розголошення таємної інформації або незаконного поширення чи незаконного використання конфіденційної інформації третіми особами вчинене розглядається як правопорушення, а винні особи підлягають юридичній відповідальності відповідно до рівня та ступеню суспільної небезпеки (шкідливості) вчиненого [26, с. 208]. Так, кримінальне законодавство України передбачає наявність складу злочину та встановлює підстави кримінальної відповідальності за протиправні дії щодо державної таємниці (статті 114, 328 та 329 КК України), лікарської таємниці (ст. 145 КК України), таємниці голосування (ст. 159 КК України), таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції (ст. 163 КК України), таємниці усиновлення (удочеріння) (ст. 168 КК України), конфіденційної інформації про особу (ст. 182 КК України), погрози розголошення відомостей, які потерпілий чи його близькі родичі бажують зберегти в таємниці – як способу вчинення вимагання (ст. 189 КК України), комерційної або банківської таємниці (статті 231 та 232 КК України), інсайдерської інформації (ст. 232-1 КК України), інформації про діяльність емітента (ст. 232-2 КК України), інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України), професійної таємниці захисника чи представника особи (ст. 397 КК України), відомостей військового характеру, що становлять державну таємницю (ст. 422 КК України), службової інформації, зібраної у процесі оперативного-розшукової, контррозвідувальної діяльності, у сфері оборони країни (ст. 330 КК України).

Але не зважаючи на те, що у всіх зазначених випадках наведена інформація з обмеженим доступом є або предметом посягання, або предметом злочину, або безпосередньо пов'язана із посяганням на інші права, свободи та інтереси особи, законодавство чітко диференціює кримінальну відповідальність залежно від суб'єктивного ставлення (суб'єктивної інкримінації), тобто залежно від того, на який саме об'єкт здійснюється посягання винною особою. У разі вчинення діяння на шкоду суверенітетові, територіальній цілісності, недоторканності,

обороздатності, державній, економічній чи інформаційній безпеці України, поєднане із передачею або збиранням відомостей, що становлять державну таємницю, скоєне розглядається як злочин проти основ національної безпеки України (розділ I Особливої частини КК України). В інших випадках, розголошення відомостей, що становлять державну таємницю, розглядається як злочин у сфері охорони державної таємниці (розділ XIV Особливої частини КК України) або злочин проти встановленого порядку несення військової служби (розділ XIX Особливої частини КК України).

Таким чином, диференціація кримінальної відповідальності залежить не від змісту та особливостей певної інформації з обмеженим доступом, з певними властивостями якої закон про кримінальну відповідальність пов'язує наявність у діяч особи ознак конкретного складу злочину, а від характеристики конкретних правовідносин (об'єкту злочину) на які безпосередньо здійснюються посягання.

Вказане обумовлено тим, що предмет злочину як самостійна ознака злочину завжди існує поряд з об'єктом. Наведене у повному обсязі знайшло своє відображення в теорії кримінального права України, адже будь-які правовідносини можливі лише з приводу спільного, єдиного для них предмета, який завжди входить до кола людських потреб, а ця обставина саме і зумовлює виникнення і функціонування самих відносин (природні об'єкти, різні товари чи предмети, що мають ознаки товару) [25, с. 83]. Саме об'єкт і предмет у своїй сукупності утворюють самостійний елемент складу конкретного злочину. Вказаний підхід є основоположним, тобто таким, на якому побудована вся галузь кримінального права, окремі її інститути, правотворча і правозастосовна діяльність у нашій державі. У зв'язку з цим, В. Я. Тацій наголошує, що у багатьох випадках законодавець указує в кримінальному законі тільки на певний вид предметів, визначаючи тим самим, що будь-який із предметів цього виду має однакове значення для кримінальної відповідальності [25, с. 93].

На сьогодні в законі України про кримінальну відповідальність інформація з обмеженим доступом визначена предметом злочину, передбаченого ст. 361-2 КК України «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації». Проте вказаний вид інформації виступає також і як предмет інших (самостійних) злочинів і збут або поширення такої інформації передбачено статтями 145, 168, 231, 232, 328 КК України та іншими нормами за умови відсутності ознак злочинів проти основ національної безпеки України (Розділ I Особливої частини КК України). Але якщо така інформація, що зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації несанкціоновано здобувається або розповсюджується – вчинене утворює ідеальну сукупність злочинів і повинно кваліфікуватися за ст. 361-2 КК України і відповідною статтею КК, що встановлює відповідальність за збут чи розповсюдження конкретного виду інформації з обмеженим доступом (таємниці) [4, с. 774].

При цьому, інформація з обмеженим доступом як предмет злочину, передбаченого ст. 361-2 КК України, має зберігатися в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах. Інформація, що зберігається в мережах електров'язку, до предмета цього злочину не належить. Ознакою комп'ютерної інформації з обмеженим доступом є також те, що вона повинна бути створена та захищена відповідно до вимог чинного законодавства. При цьому, в кожному випадку для з'ясування наявності цієї ознаки необхідно звертатися до положень відповідних законів чи підзаконних нормативно-правових актів, в яких регламентується порядок створення і захисту такої інформації.

Водночас, при визначенні інформації з обмеженим доступом, як елементу інформаційної безпеки держави, виникають певні труднощі правового характеру, що пов'язані із визначенням верховенства як окремих нормативно-правових актів, так і об'єктів кримінально-правової охорони. Відповідно до ст. 3 Конституції України, людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються найвищою соціальною цінністю нашої держави. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави, яка відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави. Разом з тим, регламентуючи загрози національній безпеці нашої держави, ст. 1 Закону України «Про основи національної безпеки України» [18] визначає їх як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України (тобто держави в цілому). Про прерогативу саме державних інтересів над інтересами особистості свідчить і побудова системи Особливої частини КК України, Розділ I якої містить коло посягань саме проти основ національної безпеки України, включаючи й інформаційну безпеку як складову частину національної безпеки. На певний привілей національних інтересів над інтересами людини вказує і законотворча та правозастосовна практика діяльності органів державної влади нашої країни.

Так, Указом Президента України від 15 травня 2017 року № 133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)"» [20] в Україні було запроваджено заборону Інтернет-провайдерам надання послуг з доступу до ресурсів сервісів ТОВ «Мэйл.РУ ГРУП», ТОВ «Вконтакте», ТОВ «Яндекс», АТ «Лабораторія Касперського», ТОВ «Доктор Веб», ТОВ «ІС». Як зазначив у своєму позові про визнання частково незаконним Указу Президента № 133/2017 щодо блокування російських інтернет-ресурсів М. Євстифеев (і на що звертають увагу окремі громадські об'єднання як в Україні, так й за її межами), таке рішення порушує принципи верховенства права та становлять обмеження в реалізації положень ст. 10 Конвенції про захист прав людини і основоположних свобод [1] (далі – Конвенція) щодо свободи вираження поглядів, яке включає свободу одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів. Водночас, залучення Вищим Адміністративним судом України як третьої сторони судового розгляду Служби безпеки України, свідчить про наявність саме інтересів національної інформаційної безпеки, а відмова у задоволенні позову – про верховенство інтересів національної безпеки України над правами і свободами,

визначеними у розділі I вищенаведеної Конвенції. Крім того, представники ЄС та Північноатлантичного альянсу (НАТО) погодилися з позицією України, що рішення про блокування російських сайтів є питанням безпеки, а не свободи слова [5].

Позиція, що базується на принципі верховенства прав і свобод людини і громадянина (так звана «людиноцентриська» доктрина [28, с. 375–376]) є цілком зрозумілою і начебто такою, що прямо зазначена як в Конституції України, так і в основоположних міжнародно-правових актах з цього питання. Водночас, прихильники такої доктрини ігнорують можливість обмеження прав людини і громадянина, якщо цього вимагають суспільні інтереси або інтереси держави. Так, п. с) ч. 2 ст. 2 Конвенції не розглядає позбавлення життя як таке, що вчинене на порушення цієї статті (порушення прав і основоположних свобод), якщо воно є наслідком виключно необхідного застосування сили державою для придушення заворушення або повстання. Частина 2 ст. 8 Конвенції закріплює, що органи державної влади можуть втручатися у здійснення права на повагу до свого приватного і сімейного життя, якщо це є необхідним в інтересах національної та громадської безпеки чи економічного добробуту країни. Свобода сповідувати свою релігію або переконання підлягає обмеженням, що є необхідними в інтересах громадської безпеки, для охорони публічного порядку (ч. 2 ст. 9 Конвенції), а право на свободу мирних зібрань і свободу об'єднання з іншими особами підлягає обмеженням в інтересах національної або громадської безпеки, для запобігання заворушенням чи злочинам (ч. 2 ст. 11 Конвенції).

Вказаний перелік можна було б продовжити і щодо обмеження інших прав і свобод людини і громадянина, але наявність таких виключень засвідчує, що так звана «людиноцентриська» позиція або визначення прав і свобод людини і громадянина найвищою цінністю, ніж інтереси держави, за своїм змістом не тільки є утопією, а й суперечить принципам основоположних міжнародно-правових актів з цього питання. Саме суспільна (громадська, загальна) небезпека завжди була і об'єктивно залишається ключовою ознакою як злочину, так і неупередженою (об'єктивно існуючою) підставою криміналізації будь-якої шкідливої поведінки. Зазначене повною мірою стосується і захисту інформації з обмеженим доступом як одного з елементів інформаційної безпеки нашої держави.

ЛІТЕРАТУРА

1. Конвенція про захист прав людини і основоположних свобод: Рада Європи; Конвенція, Міжнародний документ від 4 листопада 1950 р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/995_004
2. Конституція України: Закон України від 28 червня 1996 р. // [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/254к/96-вр>
3. Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-ІІ [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/2341-14>
4. Кримінальний кодекс України. Науково-практичний коментар : у 2 т. / за заг. ред. В. Я. Тація, В. П. Пшонки, В. І. Борисова, В. І. Тютюгіна. – 5-те вид. допов. – Х. : Право, 2013. Т. 2 : Особлива частина / Ю. В. Баулін, В. І. Борисов, В. І. Тютюгін та ін. – 2013. – 1040 с.
5. НАТО: блокування сайтів – питання безпеки, а не свободи слова [Електронний ресурс]. – Режим доступу : <http://www.bbc.com/ukrainian/news-39948904>
6. Науково-методичне забезпечення створення та функціонування системи інформаційної безпеки держави / С. Я. Довбня, В. І. Кривцун, І. О. Четверіков та ін. // 36. наук. праць. – К. : ВІКНУ, 2014. – Вип. № 47. – С. 98–108.
7. Основи законодавства України про охорону здоров'я: Закон України від 19 листоп. 1992 р. № 2801-ХІІ [Електронний ресурс]. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/2801-12>
8. Про адвокатуру та адвокатську діяльність: Закон України від 5 липня 2012 р. № 5076-VІ [Електронний ресурс]. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/5076-17>
9. Про банки і банківську діяльність: Закон України від 7 грудня 2000 р. № 2121-ІІІ [Електронний ресурс]. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/2121-14>
10. Про вибори народних депутатів України: Закон України від 17 листопада 2011 р. № 4061-VІ [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/4061-17>
11. Про державне регулювання ринку цінних паперів в Україні: Закон України від 30 жовтня 1996 р. № 448/96-ВР [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/448/96-вр>
12. Про державну таємницю: Закон України від 21 січня 1994 р. № 3855-ХІІ [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/3855-12>
13. Про деякі питання практики застосування господарськими судами законодавства про інформацію: інформаційний лист Вишого Господарського суду України від 28 березня 2007 р. № 01-8/184 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/v_184600-07
14. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. № 80/94-ВР [Електронний ресурс]. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/80/94-вр>
15. Про інвестиційну діяльність: Закон України від 18 вересня 1991 р. № 1560-ХІІ [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/1560-12>
16. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-ХІІ [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/2657-12>
17. Про нотаріат: Закон України від 2 вересня 1993 р. № 3425-ХІІ [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/3425-12>
18. Про основи національної безпеки України: Закон від 19 червня 2003 р. № 964-ІV [Електронний ресурс]. – Режим доступу : <http://zakon5.rada.gov.ua/laws/show/964-15>
19. Про Рахункову палату: Закон України від 2 лип. 2015 р. № 576-VІІІ [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/576-19>
20. Про рішення Ради національної безпеки і оборони України від 15.05.2017 № 133/2017 «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України від 15 травня 2017 р. № 133/2017 [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/133/2017>
21. Про фінансові послуги та державне регулювання ринків фінансових послуг: Закон України від 12 липня 2001 р. № 2664-ІІІ [Електронний ресурс]. – Режим доступу : <http://zakon5.rada.gov.ua/laws/show/2664-14>

22. Прокоф'єв М. Проблеми захисту інформації в Україні / М. Прокоф'єв, В. Хорошко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2015. – Вип. № 2 (30). – С. 9–14.
23. Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти: монографія / Н. А. Савінова. – К. : ТОВ «ДКС», 2011. – 342 с.
24. Сімейний кодекс України: Закон України від 10 січня 2002 р. № 2947-III [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/2947-14>
25. Тацій В. Я. Об'єкт і предмет злочину в кримінальному праві : монографія / В. Я. Тацій. – Х. : Право, 2016. – 256 с.
26. Харченко В. Б. Проблеми кримінально-правової охорони комерційної таємниці як виду інформації з обмеженим доступом / В. Б. Харченко // Наук. вісн. Дніпропетр. держ. ун-ту внутр. справ. – 2008. – № 4. – С. 204–214.
27. Цивільний кодекс України: Закон України від 16 січня 2003 р. № 435-IV [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/435-15>
28. Шаблістий В. В. Безпековий вимір кримінального права України: людиноцентричне дослідження : монографія / В. В. Шаблістий. – Дніпропетровськ : Дніпроп. держ. ун-т внутр. справ ; Ліра ЛТД, 2015. – 420 с.