стандартів, уніфікованих систем класифікації та кодування інформації; рівень забезпечення комплексного захисту державних інформаційних ресурсів із використанням сучасних засобів і методів захисту інформації від несанкціонованого доступу, пошкодження, спотворення, руйнування і блокування.

Список використаних джерел:

1. United Nations E-government Survey 2014. E-Government for the Future We Want. United Nations, New York, 2014 [Електронний ресурс]. – Режим доступу : http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf.
2. Радченко И.А. Открытые данные: определение, основные принципы и механизмы роботы с открытыми данными / И.А. Радченко [Электронный ресурс]. – Режим доступа : http://www.slideshare.net/iradche/2-open-dataintroduction03.
3. United Nations E-government Survey 2014. E-Government for the Future We Want. United Nations. New York, 2014 [Електронний ресурс]. – Режим доступу : http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-gov_Complete_Survey-2014.pdf.
4. Стаття 10-1 Закону України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/main/2939-17.
5. Афанасьєв К. Державні управлінські послуги в механізмі адміністративного регулювання / К. Афанасьєв // Вісник Луганського державного університету внутрішніх справ. – 2006. – № 3. – С. 88.
6. Сучасний стан, проблеми.
7. Клименко І.В. Електронні послуги : [навчальний посібник] / І.В. Клименко. – К., 2014. – 100 с.
8. Концепція галузевої програми інформатизації судів загальної юрисдикції та інших установ судової системи [Електронний ресурс]. – Режим доступу : court.gov.ua/userfiles/concept.pdf.
9. Про Концепцію вдосконалення судівництва для утвердження справедливого суду в Україні відповідно до європейських стандартів : Указ Президента України від 10.05.2006 № 361/2006 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/361/2006/.
10. Самборська О. Послуга щодо отримання від суду процесуальних документів у електронному вигляді, а також СМС-повісток поступово набирає популярності серед учасників процесу / О. Самборська [Електронний ресурс]. – Режим доступу : http://zib.com.ua/ua/40018elektronniy_sudotrimannya_smspovistok_stae_vse_bilsh_popul.html/.

ПУНДА О. О.,
кандидат юридичних наук, доцент, докторант
(Університет державної фіскальної служби України)

УДК 342.45

АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ЗАСТОСУВАННЯ ЗАСОБІВ БІОМЕТРИЧНОГО КОНТРОЛЮ

Стаття присвячена питанням адміністративно-правового регулювання застосування засобів біометричного контролю. Наголошено на необхідності вирішення проблеми ідентифікації особистості шляхом використання технічних засобів – без її відома, дистанційно або у місці, де громадянин не зобов'язаний представляти себе. Зазначено, що використання будь-яких біометричних засобів контролю перебування особи у певному місці повинно дублюватися іншими засобами контролю. Окреслено необхідність розробки нормативного регулювання процедури доступу особи, членів її сім'ї та близьких родичів, а також представників правоохоронних органів або медичних установ до біометричної інформації.

Ключові слова: *біометрія, контроль присутності, дистанційно, електронне маркування, приватне життя.*

Статья посвящена вопросам административно-правового регулирования применения средств биометрического контроля. Подчеркнута необходимость решения проблемы идентификации личности путем использования технических средств – без ее ведома, дистанционно или в месте, где гражданин не обязан представлять себя. Отмечено, что использование любых биометрических средств контроля пребывания лица в определенном месте должно дублироваться другими средствами контроля. Акцентировано на необходимости разработки нормативного регулирования процедуры доступа лица, членов его семьи и близких родственников, а также представителей правоохранительных органов и медицинских учреждений к биометрической информации.

Ключевые слова: *биометрия, контроль присутствия, дистанционно, электронные маркеры, частная жизнь.*

The article is devoted to issues of administrative and legal regulation of application's means of biometric controls. It was marked the necessity of solving the problem of identification of individual through use of technical means – without her knowledge, remotely, or in a place where a citizen is not obliged to represent himself. It was indicated that the use of any biometric means of control of person's residence in a particular place should be duplicated by other means of control. It was outlined the necessity of development the procedure for access of the person, person's family members and close relatives and representatives of law enforcement bodies or medical institutions to biometric information.

Key words: *biometrics, control of presence, remotely, electronic labeling, private life.*

Вступ. Сучасний вектор розвитку цивілізації демонструє наближення інформаційної ери. Людство робить чергові кроки до переходу від цивілізації техногенної (індустріальної) до постіндустріальної. Науково-технічний прогрес насичує побут та виробництво новими зразками техніки, яка створює нові можливості та загострює «старі» проблеми. Постіндустріальний простір є сферою панування інформаційних технологій та науково-технічних засобів збору, накопичення, фіксації, переробки та збереження інформаційних ресурсів. А вони, ці ресурси, насамперед стосуються окремої людини та всього того, що створює її індивідуальність на рівні від антропологічних або генетичних показників до сфери характеристики типів її вищої нервової діяльності. Створення біометричних баз даних про особу сприяє також і процесу світової глобалізації.

Активне запровадження новацій у біометричній сфері ідентифікації громадян викликає занепокоєння науковців у різноманітних суспільних наукових галузях. Разом із тим, сучасні дослідники приділяють мало уваги проблемам правового регулювання біометричного контролю та його впливу на процес реалізації особистих прав громадян. Окремі аспекти є предметом аналізу науковців із кримінально-процесуальної та криміналістичної сфери. Серед таких необхідно згадати прізвища П.В. Берназа, Л.І. Белянської, М.В. Гуцалюка, І.М. Глебова, В.В. Свентного, А.М. Лисенко.

Проте численні аспекти співвідношення суспільних та приватних інтересів у контексті провадження заходів біометричного контролю залишаються ще недостатньо дослідженими.

Постановка завдання. Широке запровадження подібних технологій впливає на реалізацію таких прав, як право на свободу пересування, право на особисте життя та його таємницю. Зазначене зумовлює необхідність розробки принципів, які б визначали межі запровадження біометричного контролю в умовах громадянського суспільства.

Результати дослідження. Біометрія – сукупність методів математичного опрацювання даних, одержаних під час вимірювання тіла або окремих органів організму. За допомогою біометрії, в основі якої лежить теорія імовірностей, дається точна характеристика значення ознаки, яка вивчається, встановлюється вірогідність подібності або відмінності цієї ознаки.

Перші спроби автоматичної апаратної ідентифікації людини за властивими їй унікальними біологічними та поведінковими параметрами можна віднести до середини XX ст., коли з'явилися прикладні розробки з автоматичної ідентифікації голосу. Першою компанією, яка запропонувала власні біометричні системи контролю доступу, була Recognition Systems Inc (США). Проте лише у дев'яності роки XX ст. загальний рівень розвитку обчислювальної техніки дав змогу використовувати біометричні параметри для ідентифікації у режимі реального часу.

Сьогодні біометричні технології використовують у сфері контролю фізичного доступу та доступу до інформації. Біометричні системи широко використовуються у приватній, корпоративній, державній та наддержавній сферах. Практично біометрія поширена у системі доступу до комп'ютерної мережі, біометричних документах, які посвідчують акти цивільного стану, у сферах електронної торгівлі, банках, роздрібній торгівлі, контролі фізичного доступу та реєстрації робочого часу, іденти-

фікації осіб, які розшукуються, у громадських місцях або на транспорті, у доступі до індивідуальних засобів (мобільних телефонів або ноутбуків).

За методами використання біометричних засобів перше місце посідає програма проектів біометричних закордонних паспортів та віз. Сьогодні подібні програми запроваджуються у США, Канаді, країнах Євросоюзу, Японії, Сінгапурі. Подібні системи ідентифікації можна використовувати і для забезпечення контролю пересування, наприклад, сезонних працівників або з метою контролю за міграційними процесами. Не менш масштабним є потенціал використання біотехнології у внутрішньому документі багатоцільового призначення. Він може поєднувати у собі документ, який посвідчує особу, картку, яка підтверджує право на участь у виборах, карту соціального страхування (універсальний цивільний документ).

Так, до прикладу, з 2006 р. громадянам Російської Федерації відповідні служби оформляють закордоні паспорти нового зразка. Вони містять інформацію про їх власників на електронних носіях (чіпах). Опис нового паспорту було затверджено постановою Уряду Російської Федерації від 18 листопада 2005 р. У Росії, як і в інших країнах, робота у напрямі паспортизації провадиться вже давно. Вона активізувалася у 2003 р., коли держави-учасники ООН підписали Нью-Орлеанську угоду, яка проголосила, що основною умовою ідентифікації особи у закордонних паспортах та візах повинна бути біометрія. Практично всі розвинуті країни запровадили заходи щодо розробки національних програм електронної паспортизації.

Спеціалісти більшості країн зійшлися на думці, що обличчя є основною біометричною ознакою людини. Розробку міжнародного стандарту на формат даних, що містяться у електронних паспортах, ведуть Міжнародна організація цивільної авіації та Міжнародна організація по стандартизації. Мета їх роботи – досягнути технологічної сумісності та взаємного зчитування паспортно-візових документів різних країн [1, с. 18].

У всьому світі проблема забезпечення надійної ідентифікації особи набула особливої актуальності після подій 11 вересня 2001 р. Зокрема, згідно з Резолюцією Ради безпеки ООН № 1373 від 28 вересня 2001 р. всі держави повинні вжити заходів для попередження підробки та незаконного використання ідентифікаційних документів та пересування терористів шляхом ефективного прикордонного контролю проїзних документів та контролю за наданням документів, що посвідчують особу.

Національні реєстри населення існують у багатьох країнах світу: у Швеції – з 1947 р., в Ісландії – з 1953, у Данії – з 1968, у Франції – з 1971, в Іспанії – з 1976, в Бельгії – з 1983, у Греції – з 1986, у Болгарії – з 1999. У Росії в грудні 2003 р. введено в експлуатацію першу чергу автоматизованої системи «Державний реєстр населення». Координацію робіт в Україні у цьому напрямі покладено на Міжвідомчу комісію, склад якої затверджено Постановою Кабінету Міністрів від 18 червня 2004 р. № 789 [2].

Є поширеним використання засобів біометричної ідентифікації у фінансовій сфері, зокрема у платіжних пластикових картках для дистанційного підтвердження особи клієнта банку та регламентування ними дій брокерів.

Крім того, на окрему увагу заслуговує і такий напрям, як використання ідентифікуючих засобів у процесі електронної торгівлі та використання грошей. Поєднання біометрії та платіжної системи привела до появи нового виду торговельної мережі – біометричних інформаційних кіосків.

Проте зрозуміло, що найбільшого значення біометричні засоби ідентифікації мають у сфері забезпечення контролю фізичного доступу або доступу до інформації (віртуального доступу) на державному і корпоративному рівнях. У побудованій за подібною схемою біометричній системі може бути регламентовано пріоритетний список допуску певних категорій працівників на об'єкт (або до певної інформації), час або інші параметри. Корпоративні системи контролю доступу до інформації дають змогу позбавитися ненадійних систем захисту, що будувалися на паролях, та значно спрощують роботу мережевих адміністраторів.

Широкою сферою використання методів біометричного контролю є галузь безпеки на транспорті, правоохоронні системи обліку (наприклад, біометрична реєстрація в закладах пенітенціарної системи, створення баз даних біометричних зразків злочинців), використання як посвідчення особи або «посмертного» ідентифікатора військових, співробітників спецслужб, рятувальників, медичних та соціальних працівників, які працюють у зонах воєнних дій або стихійного лиха.

Таку роль відіграє RF10 – мітка, яку запроваджує міністерство оборони США. Цей мініатюрний пристрій вживлюється під шкіру, не заважає та не вимагає додаткової підзарядки. Такий пристрій буде містити всю необхідну інформацію про військовослужбовця: ім'я, групу крові, адресу проживання. Електронний датчик повинен замінити металевий жетон, на який нанесені особисті дані бійця. У найближчий час набуде поширення і використання біометричних технологій у проектах медичного страхування та обліку медичної інформації, а також у системі, яка отримала назву«інтелектуальний будинок».

Так, медичні заклади США активно використовують сканування відбитків папілярних узорів для попередження превентивних маніпуляцій з картками медичного страхування. Біометричні дані є як частиною історії хвороби пацієнта, що перешкоджає зловмиснику скористатися такою документацією для отримання страхового відшкодування. Стандартна медична картка не має фотографії, а тому у практиці є поширеними випадки використання картки членами однієї родини. Крім того, ефективним є використання біометричного контролю за персоналом, який має доступ до медичних препаратів або наркотичних речовин. У будь-якому разі швидка ідентифікація пацієнта надає додаткових можливостей для повноцінного лікування та проведення медичних маніпуляцій.

Проте є зрозумілим, що найбільш ефективною сферою застосування біометричного контролю є використання його для контролю фізичного або віртуального доступу, обліку робочого часу та ідентифікації осіб.

Наприклад, сьогодні біометричні системи контролю доступу використовують в університетах для забезпечення безпеки доступу до студентських гуртожитків, їдалень та комп'ютерних центрів, у медичних закладах для захисту сховищ, у школах та центрах продовженого дня для підтвердження особи батьків та забезпечення безпеки дітей. У сфері освіти біометричні засоби можуть допомогти у вирішенні багатьох завдань, починаючи від фіксації початку та завершення маршруту руху дитини на шкільному автобусі, забезпеченості контролю доступу до приміщення школи, авторизації доступу до комп'ютерної мережі, видачі книг у бібліотеках та їх тематики, організації харчування у кафетерії або їдальні. При цьому батьки дитини будуть мати можливість доступу до такої інформації.

Розповсюдженими засобами контролю доступу є також пристрої, якими обладнують вхідні двері приміщень. Так, це пристрій TAP-01 компанії Bio Life, який здатний утримувати в пам'яті до 2800 дактилоскопічних відбитків окремих осіб, яких можна розподілити на певні групи допуску. При цьому власник приміщення може з'ясувати особу відвідувача, не користуючись камерою спостереження або звичайним вічком. Компанія пропонує також обладнувати двері і засобами активного захисту – електрошоком. Час верифікації відбитків – не більше двох секунд, вірогідність помилки – менше 0,0001%, можливість відмови або збою – менше 1%. Журнал TAP-01 містить збереження до 120 000 записів про візити та дзвінки.

Подібним ефективним пристроєм є засіб для сканування райдужної оболонки ока, розроблений компанією Panasonic Asia Pacific. Показники цього пристрою набагато вищі за засоби ідентифікації за допомогою геометрії будови руки або голосу. Користувач повинен лише подивитися в екран, при цьому не використовують засобів, шкідливих для здоров'я особи (лазерні промені, спалахи світла), ідентифікація відбувається за 0,8 секунди (система перетворює дані про будову райдужної оболонки у цифрову модель і порівнює її з такою ж моделлю у пам'яті). Компанія пропонує обладнувати цим сканером системи контролю доступу до архівів залів засідань адміністрації, приміщень для проведення конфіденційних переговорів, лабораторій, у виробничих залах, у морських та повітряних портах (службові проходи, пункти міграційного контролю).

Значного поширення також набувають системи персоналізованого маркетингу у біометричній платіжній системі. Як свідчать статистичні дані, у 70% випадків рішення покупців у магазині щодо конкретної покупки приймають безпосередньо у торговельному залі. Будь-які спроби вплинути на цей процес, наприклад, шляхом розповсюдження купонів або «флаєрів», раніше не давали вагомого результату. Коефіцієнт корисної дії подібних акцій не перевищував одного відсотка, а великі фінансові ресурси витрачалися без користі. Причиною цього, як з'ясувалося, була відсутність по-справжньому особистого, персоніфікованого звернення до кожного покупця з урахуванням його індивідуальних смаків. Змінити становище має біометрична ідентифікація покупця. Покупець торкається сканера, розташованого біля касового апарату, а вартість обраних ним покупок автоматично відраховується з його рахунку. Проте цей процес може відбуватись і у зворотному напрямі. Так, біля входу до магазину покупця зустрічає сканер, і після ідентифікації покупець отримує персоніфіковану пропозицію, засновану на «історії» його минулих візитів до магазину з перерахуванням до півтора десятка товарів, які ним були придбані раніше. Кожен з таких або подібних товарів покупцю пропонують знову придбати з індивідуальною знижкою ціни або на інших вигідних умовах. Отримавши персональну пропозицію, покупець цілеспрямовано відбирає товари у торговельному залі, оплачує їх, знову торкається екрану сканера, але вже на касі на виході.

До числа подібних пристроїв, спрямованих на «контроль пересування», відносяться також різного роду засоби «електронного маркування». Ці пристрої можуть бути інтегровані в особисті речі громадян, документи, одяг, засоби комунікації або транспорт. Принципи використання аналогічні до принципів «маяків». Подібні пристрої можуть мати й аварійно-сигнальне значення.

Сьогодні є очевидним, що широке запровадження у практику засобів біометричного «розпізнання» є справою лише часу. Проте технічні можливості знову випереджають законодавче регламентування і викликають виправдану стурбованість громадськості.

Зокрема, це пов'язано з небезпекою збору та збереження даних щодо приватного життя людини, особливо про їх релігійний та політичний вибір, стан здоров'я, коло спілкування, пересування, з невиправданістю дистанційного впізнання громадян без їх згоди, особливо у місцях, де особа не зобов'язана називати себе.

Зрозуміло, що кожен повинен бути обізнаним зі змістом інформації у «електронному досьє» та мати можливість видаляти з нього відомості, які втратили актуальність. Перелік даних, що можуть вноситися на зберігання, необхідно чітко визначити та зробити загальновідомим. Важливим є також і мотив створення тих чи інших баз даних та обов'язкове роз'яснення природи символів, які були використані у ній. Засоби впізнання людини не повинні шкодити її здоров'ю, принижувати її честь та гідність. Є неприйнятними такі різновиди подібних засобів, які є невід'ємними від тіла людини. Повинно бути заборонене у системах обліку використання замість імені людини певного номеру, наданого їй. Подібно до номеру паспорта облікові номери повинні стосуватися не особистості, а запису у базі даних. І, нарешті, є неприпустимим, щоб громадяни, які з різних причин відмовилися від участі у новій ідентифікаційній системі, були обмежені у правах або дискриміновані у прийомі на роботу, наданні соціальної допомоги та ін. Для таких громадян повинна бути передбачена альтернативна система, яка дозволила б їм повноцінно жити у суспільстві незалежно від тих чи інших форм ідентифікації особи.

Технічні пристрої «контролю присутності» та «контролю пересування», методи ускладнення «доступу» можуть бути як ефективними засобами протидії злочинності, особливо тероризму та екстремістській діяльності, так і сучасним еквівалентом «рабського ошийника» – ярмом, відомим ще з часів стародавнього Риму, ідеальним всеохоплюючим методом обмеження особистої свободи людини у її різноманітних проявах. Виняткові можливості кіберпростору демонструють численні небезпечні виклики та загрози. Це зрозуміло. Якщо раніше юридична особистість, як правило, відображалась у паперових документах, то сьогодні вона все більше перетворюється на віртуальну і стає більш вразливою. Погодимося із словами І.М. Глєбова: «Загальна електронна ідентифікація небезпечна тим, що занурює особистість поза її волею у кіберпростір, поза яким вона у майбутньому практично не зможе існувати, особливо за переходу на електронні гроші та електронні обліки у сфері соціального забезпечення, освіти та правоохоронної діяльності. Особа, яка з будь-якої причини відмовиться грати за правилами кіберпростору, буде відкинута на узбіччя життя, наражатиметься на повне порушення її прав, може зазнати дискримінації у прийомі на роботу, отриманні соціальних послуг та навіть без вини виявитися кримінальною особистістю»[1, с. 19].

Є істотною небезпека залежності прав громадян від можливих помилок системи або персоналу, технічних засобів або втручання зловмисників. Неможливо виключити і антиконституційний збір комп'ютерної інформації про приватне та особисте життя громадян.

«Необхідність електронної ідентифікації у всіх можливих варіантах контактів особи з державними органами, торговельними установами, банками, транспортом містить численні небезпеки. Кіберпростір не залишає особі нічого особистого. У кіберпросторі є можливим контролювати геть усе: де індивід перебував, з ким зустрічався, що купує, що читає, від чого проходить лікування. Вже сьогодні можливо організувати тотальне спостереження, фабрикувати та змінювати будь-які електронні досьє», – зауважує І.М. Глєбов [1, с. 19]. А тому законодавство повинно містити вичерпний і вмотивований перелік даних, що можуть бути внесені до електронних баз. Є неприпустимим внесення до їх числа інформації, яка прямо або опосередковано має відношення до оцінки або може бути використана для втручання у приватне життя громадян.

Висновки. Повинна бути остаточно розв'язана і проблема ідентифікації особистості шляхом використання дистанційних технічних засобів – без відома особи, на відстані, у місці, де громадянин не зобов'язаний називати себе. Загалом на часі є доцільним визначитися із обсягом суспільних вимог до ідентифікації особи. У сфері обов'язку громадянина ідентифікувати себе повинен діяти диспозитивний принцип: «Дозволено все, що не заборонено законом». Відповідно до цього принципу право громадянина зберігати природну анонімність (неназваність) повинно відповідати, на наш погляд, такій формулі: «Громадянин (фізична особа) має право залишатися неназваним в усіх ситуаціях, крім тих, коли обов'язок його зовнішньої або самоідентифікації встановлено законом».

Людина, а не її документ або запис в електроному досьє, повинна залишатися суб'єктом правовідносин. Необхідно заборонити примусове нав'язування електронних систем людині. У кожного повинна залишатися можливість вибору – мати або не мати електронного дубліката особистості.

Створити ефективну систему правових гарантій – це головний і єдиний запобіжник на шляху зловживань з боку окремих осіб, корпорацій або органів державної влади.

У правовій системі України відсутні нормативно-правові положення, які би стосувалися процедури використання біометричних технологій як у приватній, так і у публічній сфері. Передбачаємо необхідність розробки деталізованих правових приписів, які повинні стосуватися процедури «відібрання» зразків для порівняльного математичного аналізу біометричними засобами (під час прийому

на роботу, вступу на службу, надання медичних послуг); процедури запису та збереження подібної інформації, порядку її оновлення, поновлення, виправлення; процедури доступу особи, біометричні дані якої зберігаються, членів її сім'ї та близьких родичів, представників правоохоронних органів, медичних установ та інших осіб; процедури підтвердження у разі фіксації відхилень від норми або відмови від верифікації. Зрозуміло, що використання будь-яких біометричних засобів контролю доступу не повинно бути пов'язане з автоматичним обмеженням доступу осіб, які не охоплені участю у біометричній ідентифікації, можливістю дублювання автоматизованих систем іншими засобами контролю (у тому числі і за участю фізичної особи – контролера). Особливим вимогам повинна відповідати процедура біометризації дітей, осіб, визнаних недієздатними, біженців. Використання біометричних засобів контролю не може бути засобом відокремлення «своїх» від «чужих» у расовому, етнічному, статевому, соціальному, релігійному аспекті. Ці ідеї не можуть лягти в основу політичних ідеологій або використовуватися у поєднанні з расистськими, фашистськими, неофашистськими та іншими екстремістськими програмами. Вважаємо, що приватні, корпоративні, державні центри збору та обробки біометричних даних не повинні об'єднуватися (інтегруватися) в одну мережу з доступом винятково з боку органів державної влади, а сам доступ має відповідати вимогам процесуального законодавства. Крім того, системи біометричного контролю не повинні за жодних обставин поєднуватися із системами активного захисту (за винятком «хімічних пасток»).

Список використаних джерел:

1. Глебов И.Н., Белянская Л.И. Парламентаризм и электронная идентичность // Вестник Московского университета МВД России. − 2006. − №5. − С.18-20.

2. Гуцалюк М.В. Ідентифікація фізичних осіб як протидія організованій злочинності та тероризму діяльність // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2005. – № 11.

РУМЯНЦЕВ Ю. В.,
аспірант
(ПВНЗ «Міжнародний університет бізнесу і права»)

УДК 346.77(378)

ПРОБЛЕМИ ЗАХИСТУ ПРАВ НА ОБ'ЄКТИ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

У статті визначено об'єкти інтелектуальної власності за законодавством України. Визначено форми захисту прав інтелектуальної власності та проаналізовано сучасні проблеми захисту прав на об'єкти інтелектуальної власності.

Ключові слова: *інтелектуальна власність, інтелектуальні права, об'єкт інтелектуальної власності, захист прав інтелектуальної власності.*

В статье определены объекты интеллектуальной собственности согласно законодательству Украины. Определены формы защиты прав интеллектуальной собственности и проанализированы современные проблемы защиты прав на объекты интеллектуальной собственности.

Ключевые слова: *интеллектуальная собственность, интеллектуальные права, объект интеллектуальной собственности, защита прав интеллектуальной собственности.*

The article defines the objects intellectual property under the laws of Ukraine. Some form of intellectual property protection and analyzes the current problems of protection of intellectual property.

Key words: *intellectual property, copyright, intellectual property, protection of intellectual property rights.*