

DOI: [https://doi.org/10.24144/2409-6857.2024.2\(64\).112-120](https://doi.org/10.24144/2409-6857.2024.2(64).112-120)
УДК 657.421.3

Єременко А.В.

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ НЕМАТЕРІАЛЬНИХ АКТИВІВ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ

Стаття присвячена забезпеченню захисту нематеріальних активів в інформаційних мережах. Встановлено, що наслідком інформатизації сучасної економічної системи стало виникнення «нових» об'єктів нематеріальних активів – баз даних та програмних продуктів, які охороняються авторським правом, та доменних імен, які де-факто є засобами індивідуалізації. З'ясовано, що на сьогодні існують розбіжності в визначенні цих інформаційних об'єктів як об'єктів нематеріальних активів, що призводить до недосконалості механізмів їх захисту в інформаційному середовищі, що зумовлено наступним: віртуальний характер цих інформаційних об'єктів; екстериторіальність глобальних комп'ютерних мереж; труднощі виявлення в інформаційному середовищі фактів контрафакції. Зроблено висновок, що захист інформаційних об'єктів повинен здійснюватися поєднанням правових методів та методів інформаційної безпеки і, передусім, це стосується захисту баз даних, в яких розміщена інформація, що є комерційною таємницею.

Ключові слова: нематеріальні активи, інтелектуальна власність, інформаційні мережі, авторське право, база даних, захист прав власників, комерційна таємниця, Інтернет.

Постановка проблеми. Одним з чинників успішної діяльності компаній є наявність потенціалу адаптації до умов глобального середовища, що передбачає існування ефективної системи моніторингу, яка дозволяє оперативно збирати, опрацьовувати та аналізувати персоналом компанії дані про зміни в міжнародному бізнес-середовищі та кон'юнктуру світових ринків. Зрозуміло, що умовою проведення моніторингу міжнародного бізнес-середовища є використання інформаційних систем та засобів комп'ютерних телекомунікацій. Інформаційні системи і засоби телекомунікацій використовуються для оперативного зв'язку між всіма підрозділами інтернаціональних бізнес-структур, між діловими партнерами, а також при проведенні маркетингових досліджень. Можливість доступу до інформаційних ресурсів всієї світової спільноти обумовлена інтеграцією локальних і корпоративних мереж підприємств і організацій в глобальну мережу Інтернет. Проте використання сучасних Інтернет-технологій має і негативні сторони. Передусім, це стосується проблемних питань правового регулювання нематеріальних активів (далі НМА), розміщених в інформаційних системах. Треба зазначити, що без надійного забезпечення охорони НМА, які в цьому випадку є інформаційними об'єктами, використання глобального інформаційного

середовища недоцільне, а це знижує рівень конкурентоспроможності бізнесу.

Аналіз останніх досліджень і публікацій. Дослідженню питань забезпечення захисту НМА в інформаційних мережах присвячені численні роботи відомих науковців: Г. Андрощук, Ю. Бошицький, В. Жаров, Ю. Капіца, Г. Огнев'юк, М. Паладій, О.О. Підпригори, О.А. Підпригори, П. Цибульов. Попри вагомий доробок вчених, існує об'єктивна необхідність розробки теоретико-прикладних засад і вдосконалення механізмів забезпечення захисту НМА в інформаційних мережах та їх гармонізація з вітчизняним законодавством.

Формулювання цілей статті. Метою дослідження є визначення ефективності забезпечення захисту НМА в інформаційних мережах та пошук механізмів його підвищення.

Опис основного матеріалу дослідження. З кожним днем динамічні та швидкозмінні процеси створення, розповсюдження і використання НМА, регулювання цієї сфери стає надзвичайно важливим завданням для забезпечення балансу між захистом прав творців та стимулюванням інновацій. Одним із ключових способів регулювання є оновлення законодавства, що відповідає викликам цифрового середовища, а саме внесення змін до авторського, патентного та інших видів правових актів, які визначають правила захисту НМА в онлайн-середовищі. Сучасні технології, такі як системи DRM (Digital Rights Management), блокчейн та інші, можуть використовуватися для захисту прав власників НМА в мережі, та дозволяють обмежувати

©Єременко А.В., к.е.н., докторант, ДННУ «Академія фінансового управління», Київ, Україна, тел.: +380503314661; e-mail: andreyu@ukr.net

доступ до матеріалів і контролювати їхнє використання. Вони надають власникам НМА можливість шифрувати, обмежувати копіювання та встановлювати обмеження на відтворення своїх творів, що сприяє захисту НМА [1].

Україна належить до ТОП-20 найбільших експортерів ІТ-послуг у світі. Понад 70% експорту ІТ-послуг України становить розробка програмного забезпечення на замовлення. З аналізу доповіді ВОІВ World Intellectual Property Report Breakthrough Innovation and Economic Growth видно, що Україна серед 20 країн-лідерів за кількістю патентів у сфері революційних технологічних інновацій: 3Dдруку (11-е місце) і робототехніки (17-е місце) [2].

Система міжнародного захисту інтелектуальної власності (далі ІВ) перебуває у тісній взаємозалежності із системами національного захисту на рівні держав та безпосередньо впливає на них [3]. Так, законодавчою реакцією на збройний конфлікт, що триває в Україні, з метою посилення захисту інтересів осіб у сфері ІВ, стало прийняття Закону України «Про захист інтересів осіб у сфері інтелектуальної власності під час дії воєнного стану, введеного у зв'язку із збройною агресією Російської Федерації проти України», який передбачає: призупинення під час дії воєнного стану перебігу строків, пов'язаних із охороною ІВ; призупинення строків щодо процедур набуття цих прав, визначених спеціальними законами України у сфері ІВ та підзаконними актами; можливість уповноваженим особам подати необхідні документи (заяви, клопотання, заперечення, відповіді тощо) протягом дев'яноста днів від дня скасування воєнного стану без сплати збору за продовження або відновлення відповідних строків [4].

Більшість чинників проблемних питань пов'язані з різною природою і формою вираження інформаційних об'єктів і традиційних об'єктів ІВ (ст. 2 Конвенції, що заснувала ВОІВ, 1967 р.) [5]. Зазначимо, що по суті і ті і інші несуть нові знання, отримані в результаті творчої діяльності людини. Проте для традиційних об'єктів ІВ ці знання матеріалізовані і представлені у вигляді текстових документів, літературних і художніх творів, графічних зображень, промислових зразків, аудіо- і відеозаписів тощо. Саме на подання об'єктів у речовій або матеріальній формі та можливість фіксації факту порушення прав власників ІВ розрахована існуюча нормативно-правова база, причому її юрисдикція розповсюджується тільки на територію певної країни.

До об'єктів ІВ, розміщених в інформаційних системах, передусім потрібно віднести програмні продукти і бази даних, для яких згідно положень Бернської конвенції основною формою захисту є авторське право [6].

Проте захист цих об'єктів, розміщених в пам'яті комп'ютера у вигляді файлів, має свою специфіку. Останнє пов'язано з природою інформаційних об'єктів, а також їх роллю у функціонуванні системи і можливістю різних наслідків несанкціонованого розкриття. Програмні продукти по суті є інструментарієм, за допомогою якого виконуються процеси обробки, передачі і відображення інформації, розміщеної в базах даних. Причому, ця інформація містить життєво важливі для підприємства відомості, доступ до яких безпосередньо впливає на ефективність бізнесу. Зрозуміло, що наслідки від незаконного доступу до програмних засобів і баз даних інформаційних систем для підприємств різні. Тому організація їхнього захисту як об'єктів НМА виконується різними методами, про що буде сказано нижче.

Термін, що отримав останнім часом, широке розповсюдження «інформаційно-орієнтована економіка» значною мірою зобов'язаний концепції баз даних. Бази даних, як і програмні засоби, згідно Бернської конвенції, є об'єктами ІВ і охороняються нормами авторського права як літературні твори. Крім того, в статті 10 Угоди про торговельні аспекти прав інтелектуальної власності (Угода ТРІПС) також встановлюється зобов'язання охорони баз даних авторським правом [7]. Але останніми роками відбулися істотні зміни в інформаційній індустрії світової спільноти, які створили передумови і для змін в методах захисту баз даних. Розвиток комп'ютерних інформаційних технологій і глобальної мережі Інтернет призвели до трансформації традиційних форм бізнесу в електронний, заснований на використанні інформаційних систем і, отже, баз даних. В них в цифровій формі зберігаються відомості про всі аспекти бізнесової діяльності компанії, включаючи виробництво, фінанси, кадрову політику, маркетинг тощо. В порівнянні з документацією на паперових носіях бази даних мають незаперечні переваги: швидкий пошук необхідної інформації; практично необмежений обсяг; простота копіювання, відображення, передачі, перетворення даних; реалізація технології гіпертекстових посилань; порівняно невеликі витрати на ведення і модифікацію бази даних. Вказані переваги зробили бази даних значущим чинником конкурентної боротьби і цінним товаром на ринку інформації, який

повинен бути захищений від незаконного використання.

Розглянемо наскільки ефективна охорона баз даних в умовах ведення сучасного бізнесу, передусім інтернаціонального, тільки правовими нормами. В національних законодавствах під базою даних, що охороняється авторським правом розуміється комп'ютеризована (електронна) збірка, яка містить тематичні підбірки фактичних даних і творів. Причому підбірка матеріалу здійснюється відповідно до певних критеріїв і його відображення на екрані монітора реалізовано в доступному і зручному для сприйняття вигляді. Прикладом подібних збірок є електронні бібліотеки, тематичні of-line довідники, електронні словники. Значну економічну цінність мають бази даних на сайтах міжнародних організацій і державних установ.

Проте потрібно мати на увазі, що авторським правом охороняються тільки бази даних, створені творчою працею людини. Ця обставина вносить неоднозначність щодо методів їх захисту. Так, для більшості баз даних процес створення і підтримки працездатності вимагає значних фінансових витрат і трудових зусиль. Якщо врахувати, що останні часто не є творчими, то формально ці бази даних не можуть бути об'єктами захисту авторським правом. Разом з тим, кожний, хто бере участь в створенні і веденні баз даних незалежно від її творчого або нетворчого характеру, зацікавлений в адекватній винагороді і захисті своїх економічних інтересів. Цілком закономірно, що прогалина в правовому захисті нетворчих баз даних повинна бути ліквідована особливо з урахуванням попиту на систематизовану інформацію.

Одним з чинників, який обумовлює труднощі у вирішенні цієї задачі, є те, що багато бізнес-структур територіально розташовані в країнах з різною оцінкою права на бази даних, створених творчою і нетворчою працею. Наприклад, в європейській практиці порівняно нещодавно з'явився інститут особливої охорони баз даних, який зветься також правом на бази даних [8]. Це право забороняє використання без дозволу автора навіть нетворчих баз даних, їх істотної частини або окремих фрагментів.

Ставлення до захисту авторським правом нетворчих баз даних неоднозначне. З одного боку, надання охорони нетворчим базам даних стимулює авторів до продовження діяльності в сфері накопичення і систематизації суспільно корисних знань, що підвищує рівень інформатизації бізнесу. З іншого боку, оплата інформації, розміщеної в базах даних, призведе до подорожчання всіх товарів і послуг, які

виготовляються з її використанням. Крім того, надмірно широке тлумачення автором поняття істотної частини баз даних призведе до заборони запозичення навіть її незначних фрагментів [9]. Останнє обмежує інтереси суспільства в доступі до інформації, що по суті є основною перевагою захисту авторським правом.

Якщо вважати більш значущими негативні наслідки введення особливої охорони баз даних, то автор практично одержує право тільки на результати суто творчої праці – підбірку і організацію інформації, але не на розміщені в базі відомостей. Очевидно, досягнення і підтримка балансу інтересів споживачів інформації і авторів баз даних є специфічною задачею для кожної країни і окремого суспільства. Проте при її розв'язанні не потрібно забувати, що в умовах кіберпростору бази даних з вільним доступом до інформації можуть стати донорами для компаній конкурентів, де базам даних наданий статус особливої охорони. Це зауваження, перш за все, стосується США, де сильні традиції вільного доступу до інформаційних ресурсів і будь-які бази даних є тільки об'єктами авторського права на відміну від європейських країн, в яких реалізована особлива охорона баз даних [10].

На підставі вищевикладеного можна стверджувати, що найвірогіднішою перспективою удосконалення нормативно-правової бази країн світової спільноти є введення інституту охорони нетворчих баз даних. При цьому необхідно забезпечити гарантію доступу до баз даних чи їх фрагментів тільки за умови відповідної оплати інформаційних послуг.

Правовий захист як творчих, так і нетворчих баз даних може бути здійснений виключно після доказу факту їх несанкціонованого використання як об'єктів НМА. Зважаючи на екстериторіальність Інтернет і латентність самого порушення досить важко своєчасно встановити цей факт. Тому для підвищення ефективності особливої охорони нетворчих баз даних потрібно паралельно забезпечити розмежування доступу до інформаційних ресурсів. Як правило, для цього застосовуються програмно-апаратні методи, засновані на криптографічному захисті даних, технології аутентифікації, а також технології виявлення в інформаційному середовищі підозрілих дій.

Слід зазначити, що в базах даних може міститися не тільки суспільно корисна інформація, що представляє інтерес для широкого кола користувачів. В умовах інтернаціоналізації бізнесу і широкого розповсюдження корпоративних інформаційних

систем, бази даних стають основною складовою НМА багатьох компаній. В них зберігається інформація щодо всіх аспектів життєдіяльності компанії, а саме: дані про виробничі процеси (технології і обладнання, організація збуту і постачань, оцінка якості і ефективності тощо); інформація про ринок (ціни, відносини з діловими партнерами, дані про конкурентів, аналіз поточних продажів і прогноз майбутнього попиту, умови договорів тощо); дані про організаційну структуру і фінанси (кадрова політика, персонал і повноваження, бухгалтерський облік, фінансова звітність тощо).

Судячи з обсягу і змісту вказаних відомостей, можна вважати, що економічна безпека компанії безпосередньо залежить від інформаційної безпеки її баз даних. При цьому база даних як інформаційний об'єкт має низку особливостей, які полягають в наступному: призначені для використання вузьким колом осіб; інформація має різний рівень конфіденційності і призначена для різних користувачів, що обумовлює необхідність розробки процедури управління доступом до ресурсів; основною цінністю є не форма подання і організація даних, а зміст; несанкціоноване ознайомлення з базою даних ставить під загрозу конкурентоспроможність компанії, якій вона належить.

Таким чином, інформація (або її істотна частина), що зберігається в базах даних, безпосередньо пов'язана з економічними інтересами компанії і, отже, є комерційною таємницею, яка повинна бути захищена законом про недобросовісну конкуренцію [11]. Проте даний закон може бути застосований тільки після доказу протиправного використання конфіденційної інформації з баз даних. Це пояснюється тим, що існуючі технології дозволяють «зламати» бази даних так, що втрата інформації залишається довгий час (або навіть назавжди) невиявленою. В результаті цього економічним інтересам компанії завдається серйозний збиток, її конкурентоспроможність знижується, тоді як менеджмент компанії не може дати правильну оцінку причинам спаду.

З точки зору економічних інтересів компанії захист баз даних повинен бути організований таким чином, щоб виключити або звести до мінімуму можливість несанкціонованого доступу до інформації, що є комерційною таємницею. Причому чинник правового захисту, направлений в основному на формування у потенційних правопорушників свідомості невідворотності порушення, не є головним при виборі методів охорони баз даних.

На підставі вищевикладеного можна зробити висновок, що захист баз даних, які розміщені в інформаційних системах бізнес-структур, тільки правовими методами не можна вважати достатнім. Для запобігання втрати економічно значущої інформації, що є комерційною таємницею, необхідно використовувати також методи інформаційної безпеки комп'ютерних систем. До цих методів потрібно віднести: управління доступом до інформаційних ресурсів; ідентифікація і перевірка справжності користувачів; криптографічний захист даних.

Найрадикальнішими методами захисту баз даних в даний час є криптографічні, які забезпечують конфіденційність інформації за допомогою шифрування, її цілісність і достовірність, а також постановку електронного цифрового підпису. В основі технологій захисту даних лежить концепція використання криптографічних протоколів.

Не менш важливою частиною інтелектуального капіталу підприємства є програмні продукти, що безпосередньо здійснюють обробку та аналіз інформації. Зазначимо, що з позиції захисту програмних продуктів як об'єктів НМА їх доцільно розділити на некомерційні і комерційні. Перші, як правило, розробляються для конкретної інформаційної системи і існують в обмеженому числі екземплярів на комп'ютерах підприємств. Комерційні програми створюються відомими компаніями (наприклад, Microsoft, Borland) і тиражуються у великому обсязі на магнітних носіях. З точки зору запобігання неліцензійного використання, методи захисту комерційних програмних продуктів в більшій мірі адекватні методам захисту традиційних об'єктів НМА, ніж у разі використання некомерційного програмного забезпечення.

Що стосується об'єктів НМА, розміщених в базах даних, то у вигляді безпосередньо придатному для сприйняття в реальному часі, вони не існують. Ці об'єкти формуються шляхом обробки відповідними програмними засобами інформаційних масивів і існують віртуально. Йдеться про створених на екранах моніторів зображеннях об'єктів НМА і пов'язаних з ними процесів, з якими можна працювати як з реальними об'єктами – вивчати, проводити обчислення, моделювання, приймати рішення тощо. Причому, виконувати ці дії може будь-який користувач Інтернет, фізично віддалений на сотні і тисячі кілометрів, але який має доступ до програмно-інформаційних ресурсів підприємства.

Таким чином, якщо прийняти до уваги такі моменти як мобільність створюваних в інформаційному середовищі віртуальних зображень об'єктів НМА, можливість збереження анонімності віддалених користувачів, які можуть мати доступ до інформаційних ресурсів, екстериторіальності Інтернет і відмінності нормативно-правових баз окремих країн в галузі захисту НМА, то стає очевидним, що надійний захист об'єктів НМА, розміщених в інформаційних системах, які мають вихід в Інтернет, забезпечити існуючими правовими методами неможливо [12]. Можна констатувати, що інтелектуалізація сучасного бізнесу і супроводжуваний його розвиток глобальної інфраструктури призвели до помітного відставання діючої нормативно-правової бази в галузі охорони НМА від реальних потреб. На думку автора, це відставання можна скоротити, здійснюючи дії в наступних напрямках: розробка більш ефективних правових актів з охорони НМА, що враховують специфіку інформаційного середовища; створення в інформаційних системах умов, що дозволяють підвищити ефективність використання існуючої нормативно-правової бази; застосування разом з правовими криптографічних методів, що більшою мірою враховують специфіку інформаційних ресурсів як об'єктів НМА і некритичних до відмінностей в галузі захисту НМА в національних законодавствах.

Один з найуразливіших інтелектуальних ресурсів сучасного бізнесу є програмне забезпечення персональних комп'ютерів, що виконує функції обробки і зберігання інформації, а також передачі її по локальним мережам і Інтернет [13]. Традиційні методи захисту НМА ґрунтуються на нормативно-правових актах, які стосовно програмного забезпечення можуть бути реалізовані на національному і міжнародному рівнях. На національному рівні правовий захист забезпечується національним законодавством, на міжнародному – відповідними конвенціями і угодами. Проте процедури правового регулювання відносин при створенні і використанні комп'ютерних програм навіть в національних законодавствах недостатньо визначені, не кажучи про механізми їхньої реалізації. Не слід також забувати, що далеко не всі країни, на території яких розміщені регіональні підрозділи компаній, дотримуються в повному обсязі міжнародних угод в галузі правового захисту об'єктів НМА.

Ефективність правового захисту програмних продуктів знижується і за рахунок того, що

норми існуючого законодавства не встигають пристосовуватися до стрімкого зростання комп'ютерних технологій, що дозволяє реалізувати несанкціонований доступ і копіювання програм. Це зауваження пов'язано з тим, що механізм виявлення порушників прав НМА в інформаційних системах і особливо в Інтернет визначає в значній мірі методи захисту.

Дієвість правової охорони комп'ютерних програм істотно залежить також від того, яким правом вони захищені – авторським або патентним. Відносно переваги вибору авторського права або патентного захисту існують різні думки [14]. Кожний з методів правового захисту має свої переваги і недоліки. Їх значущість змінюється залежно від таких чинників як: наявність на території країни крупних компаній з розробки і виробництва програмного забезпечення; рівень інформатизації суспільства, який визначає насиченість бізнесу інформаційними системами з виходом в Інтернет; наявність компетентних патентних відомств; рівень правосвідомості споживачів програмних продуктів.

В більшості країн на законодавчому рівні передбачений тільки один вид охорони програмного забезпечення – за допомогою авторського права. При цьому захищається виключно форма подання програми, але не її суть, що відображає семантичну сторону розробки продукту. Цей захист направлений на запобігання неліцензійного використання комп'ютерної програми, але не на виключення плагіату принципів і ідей, які містяться в її алгоритмі. Іншими словами, самі творчі аспекти створення програмних продуктів залишаються поза правового захисту.

Слід зазначити, що з часу підписання Бернської конвенції технологія створення програмних продуктів істотно змінилася, разом з коректністю їх порівняння з літературними творами. Цьому сприяли наступні обставини: поява спеціалізованих засобів розробки програмних продуктів з готовими типовими модулями; можливість використання фрагментів вже існуючих програм і відсутність контролю новизни і унікальності при реєстрації знову створюваних продуктів; поява значної кількості програм-аналогів за функціями, що виконуються; скорочення терміну життя програм до 5-7 років.

Все це ставить під сумнів правомірність використання для захисту програмних продуктів тільки інституту авторського права в існуючому його трактуванні. Найдоцільнішою системою захисту комп'ютерних програм потрібно вважати таку, яка б об'єднала експертну перевірку,

необхідну при патентній охороні, з наданням доступу широкому колу користувачів, що характерно для авторського права. Основними труднощами на шляху здійснення даного підходу є: необхідність узгодження нормативно-правової бази в багатьох країнах; відсутність кваліфікованих експертів-патентознавців із знаннями в галузі програмування; необхідність створення спеціалізованої бази даних з текстами вже існуючих програм у вихідних кодах.

Збиток, який наносить країні нелегальне використання програмних продуктів, важко оцінити. Проте, перш за все, це чисто економічні втрати, до яких потрібно віднести: недоотримання валового внутрішнього продукту і відповідне зменшення податкових надходжень. Вартість легально ввезеного і реалізованого з дотриманням існуючого законодавства програмного забезпечення набагато менше вартості всіх реалізованих програмних засобів; втрата на митних зборах і платежах, оскільки неліцензійне програмне забезпечення ввозиться контрабандним шляхом; зниження інвестиційної привабливості країни; міжнародно-економічні санкції; зниження інформаційної безпеки підприємств або компаній, що використовують в системах управління неліцензійні програмні продукти. Це пов'язано, перш за все, з тим, що контрафактні копії комп'ютерних програм часто бувають видозміненими або пошкодженими.

Одночасно з комерційними програмними продуктами в інформаційних системах бізнес-структур використовуються і некомерційні. Вони, на відміну від комерційних, розробляються по замовленню окремих компаній з урахуванням специфіки їх діяльності і призначені для роботи обмеженого числа співробітників.

Не викликає сумніву, що некомерційні програмні продукти, що є об'єктами НМА їх авторів або власників бізнесу, повинні мати статус правової охорони. Його особливість полягає в тому, що некомерційне програмне забезпечення, орієнтоване на певний бізнес, повинно бути захищено не так авторським правом, скільки законодавством про недобросовісну конкуренцію і про охорону комерційної таємниці. Дієвість правового захисту безпосередньо пов'язана зі встановленням факту неправомірного використання комп'ютерних програм. Несанкціонований доступ до програмних

продуктів, що представляють комерційну таємницю, може бути здійснений співробітниками компанії (для передачі конкуренту) або шляхом проникнення через мережу в комп'ютер, на якому розміщена програма.

Подальший розвиток глобальної інформаційної інфраструктури привів до появи нових об'єктів НМА, серед яких, перш за все, потрібно назвати доменні імена. Інтерес до доменних імен як об'єктів НМА пояснюється тим, що вони служать єдиним засобом ідентифікації Web-сайтів, які мають практично всі державні установи і бізнес-структури. Крім того, грамотний вибір доменних імен дозволяє реалізувати можливості мережі Інтернет відносно реклами і просування товарів до потенційних споживачів. Тому загальноприйнятою стала практика реєстрації (або викупу) назв доменних імен, ідентичних найменуванню компанії, її бізнесу або товарному знаку. Насправді, доменні імена трансформувалися в засіб, що виконує функції товарних знаків, і де-факто можуть бути віднесені до об'єктів НМА.

Поява «нових» об'єктів НМА в інформаційному середовищі вимагає вдосконалення як традиційних, так і розробку новітніх методів їх захисту (рис. 1).

Таким чином, не дивлячись на те, що доменне ім'я є тільки адресою в Інтернет, фактично відбувається його використання як засобу індивідуалізації з отриманням всіх корисних властивостей по просуванню в мережі інформації, розміщеної на сайті. В результаті цього доменні імена вводяться в комерційний обіг і дозволяють їх власнику успішно займатися електронним бізнесом. Право на захист доменного імені як об'єкта НМА належить власнику сайту, проте більш поширена практика охорони прав на товарні знаки при використанні їх в доменних іменах. Тільки власник товарного знаку володіє винятковим правом поширювати інформацію про товари і послуги, охоплювані цим товарним знаком, в мережі Інтернет. При цьому як доменне ім'я використовуються позначення, ідентичні або схожі з товарним знаком. Якщо ж сайт належить фізичній або юридичній особі, що не має дозвіл власника прав на товарний знак (наприклад, конкуруючому бізнесу), то на ринку

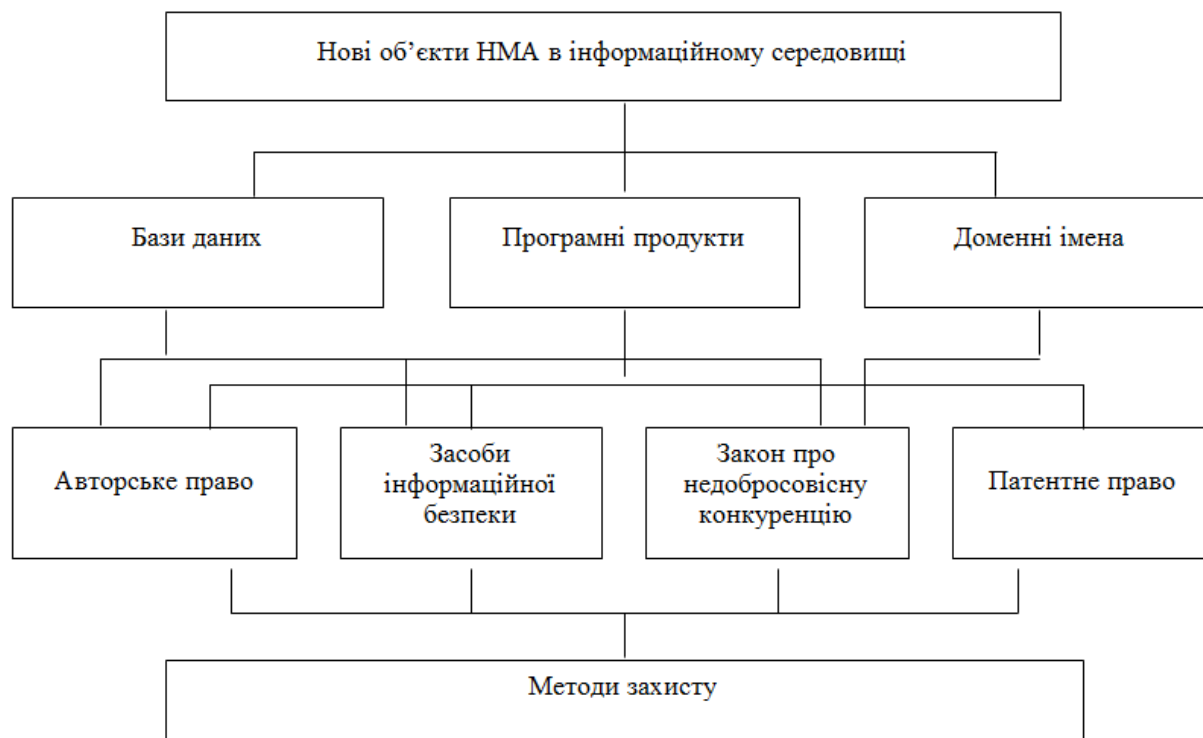


Рис. 1. Нові об'єкти НМА та методи їх захисту (складено автором)

відбувається змішування товарів і послуг. В результаті законному власнику товарного знаку може бути завданий збиток, оскільки продаж товарів і послуг більш низької якості знижує репутацію компанії. Для захисту прав власника товарного знаку в даному випадку потрібно використовувати закон про недобросовісну конкуренцію.

Висновки і перспективи подальших досліджень. Проведений аналіз дозволяє зробити наступні висновки: інтернаціоналізація сучасного бізнесу і, перш за все, інформаційна підтримка систем менеджменту та маркетингу пов'язані з використанням інформаційно-комунікаційних технологій, що призвело до появи «нових» об'єктів НМА – програмні продукти, бази даних, доменні імена; захист вказаних об'єктів НМА повинен бути організований з урахуванням специфіки інформаційної інфраструктури:

екстериторіальність і відсутність єдиного правового простору; віртуальний характер та мобільність інформаційних об'єктів; трудність доказу неправомірного використання об'єктів НМА; існуюча законодавча база в галузі охорони об'єктів НМА в Інтернет не повною мірою відповідає характеру інформаційних об'єктів і не враховує можливості сучасних технологій по неправомірному доступу і використанню цих об'єктів; для ефективного захисту об'єктів НМА в інформаційних системах необхідне поєднання правових методів і методів, що забезпечують інформаційну безпеку. Передусім це відноситься до об'єктів НМА, які представляють комерційну таємницю. Крім того, важливим для України є збереження на майбутнє тенденцій посилення правової охорони НМА відповідно до європейських стандартів, особливо по завершенню збройного конфлікту в нашій країні.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Digital Rights Management (DRM). URL: <https://www.fortinet.com/resources/cyberglossary/digital-rights-management-drm>.
2. World Intellectual Property Organization: web-site. Breakthrough Innovation and Economic Growth. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_944_2015.pdf.

3. Скалецька З. Міжнародний захист права інтелектуальної власності в умовах воєнного стану. Академічні візії. 2022. №14/2022. URL: <https://zenodo.org/records/7713709>.
4. Верховна Рада України: веб-сайт. Закон України «Про захист інтересів осіб у сфері інтелектуальної власності під час дії воєнного стану, введеного у зв'язку із збройною агресією Російської Федерації проти України» від 01.04.2022 р. № 2174-IX. URL: <https://zakon.rada.gov.ua/laws/show/2174-20#Text>.
5. World Intellectual Property Organization: web-site. Convention Establishing the World Intellectual Property Organization (WIPO Convention) (1967). URL: <https://www.wipo.int/wipolex/ru/text/283854>.
6. Верховна Рада України: веб-сайт. Бернська конвенція про охорону літературних і художніх творів. URL: https://zakon.rada.gov.ua/laws/show/995_051#Text.
7. Верховна Рада України: веб-сайт. Угода про торговельні аспекти прав інтелектуальної власності (Додаток 1С до Угоди про заснування Світової організації торгівлі). URL: https://zakon.rada.gov.ua/laws/show/981_018#Text.
8. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. URL: https://publications.europa.eu/resource/cellar/2d1f5a77-5982-11e8-ab41-01aa75ed71a1.0001.01/DOC_1.
9. Deanna J. Richards, Braden R. Allenby and W. Dale Compton. (2001). Information Systems and the Environment. National Academies Press. 228 p.
10. Sui Generis Database Protection. Has Its Time Come? URL: <http://www.dlib.org/dlib/june97/06band.html>.
11. Кручиніна М. Проблеми правової охорони інформації, що міститься в базах даних. ІВ. Авторське право та суміжні права. 2005. №8. С. 2-8.
12. Ушаков В. Розвиток міжнародної охорони інтелектуальної власності. ІВ. Промислова власність. 2002. №12. С. 30-35.
13. Степанов О. Міжнародно-правові засоби захисту інтелектуальної власності. ІВ. Авторське право і суміжні права. 2003. №1. С. 38-45.
14. Березанська В. Розробка проекту спеціального закону щодо охорони прав на комп'ютерні програми. Інтелектуальна власність. 2004. №6. С. 6-9.

REFERENCES

1. Digital Rights Management (DRM). URL: <https://www.fortinet.com/resources/cyberglossary/digital-rights-management-drm> [In English].
2. World Intellectual Property Organization: web-site. Breakthrough Innovation and Economic Growth. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_944_2015.pdf [In English].
3. Skaletska Z. International protection of intellectual property rights under martial law. Academic visions. 2022. No. 14/2022. URL: <https://zenodo.org/records/7713709> [In Ukrainian].
4. Verkhovna Rada of Ukraine: website. The Law of Ukraine "On Protection of the Interests of Individuals in the Field of Intellectual Property During the Martial Law Introduced in Connection with the Armed Aggression of the Russian Federation Against Ukraine" dated April 1, 2022 No. 2174-IX. URL: <https://zakon.rada.gov.ua/laws/show/2174-20#Text> [In Ukrainian].
5. World Intellectual Property Organization: web-site. Convention Establishing the World Intellectual Property Organization (WIPO Convention) (1967). URL: <https://www.wipo.int/wipolex/ru/text/283854> [In English].
6. Verkhovna Rada of Ukraine: website. Berne Convention on the Protection of Literary and Artistic Works. Retrieved from: https://zakon.rada.gov.ua/laws/show/995_051#Text [In Ukrainian].
7. Verkhovna Rada of Ukraine: website. Agreement on Trade Aspects of Intellectual Property Rights (Appendix 1C to the Agreement Establishing the World Trade Organization). Retrieved from: https://zakon.rada.gov.ua/laws/show/981_018#Text [In Ukrainian].
8. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. URL: https://publications.europa.eu/resource/cellar/2d1f5a77-5982-11e8-ab41-01aa75ed71a1.0001.01/DOC_1 [In English].
9. Deanna J. Richards, Braden R. Allenby and W. Dale Compton. (2001). Information Systems and the Environment. National Academies Press. 228 p. [In English].
10. Sui Generis Database Protection. Has Its Time Come? URL: <http://www.dlib.org/dlib/june97/06band.html> [In English].

11. Kruchynina M. (2005). Problems of legal protection of information contained in databases. Intellectual property. Copyright and related rights. No. 8. P. 2-8. [In Ukrainian].
12. Ushakov V. (2002). Development of international protection of intellectual property. Industrial Property. No. 12. P. 30-35. [In Ukrainian].
13. O. Stepanov. (2003). International legal means of intellectual property protection. Intellectual property. Copyright and related rights. No. 1. P. 38-45. [In Ukrainian].
14. Berezanska V. (2004) Development of a draft special law on the protection of rights to computer programs. Intellectual property. No. 6. P. 6-9. [In Ukrainian].

Отримано 19.07.2024