

3. Філатова Н. Ю. Особливості укладення договорів з використанням електронної форми представлення інформації / Н. Ю. Філатова // Проблеми вдосконалення приватноправових механізмів набуття, передачі, здійснення та захисту суб'єктивних цивільних прав : матеріали «круглого столу», присвяч. пам'яті проф. Ч. Н. Азімова, м. Харків, 16 груд. 2016 р. – Харків, 2017. – С. 235–243.
4. Пояснительная записка Секретариата ЮНСИТРАЛ к Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах. – режим доступа http://www.uncitral.org/pdf/russian/texts/electcom/06-57454_Ebook.pdf.

*Карпенко Вікторія Ігорівна, Карпенко Денис Ігорович,
студенти 5-го курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доцент Берназ-Лукавецька О.М.*

ЩО ТАКЕ КІБЕРСКВОТЕР ТА ЯК ЗАХИСТИТИ СЕБЕ ВІД НЬОГО У ЦИФРОВІЙ ДОБІ СЬОГОДЕННЯ?

На сьогоднішній момент немає точного визначення такого поняття як кіберсквотер, однак кожен з нас з ним зустрічається в день майже тисячу разів, отже, що це і як з ним боротися?

Якщо розглянути етимологію слова кіберсквотинг, то частка «сквотинг» (англ. squatting), за даними Оксфордського словника, буквально означає «іти й жити у порожній будівлі без дозволу її власника». На законодавчому рівні поняття «кіберсквотинг» не є визначеним. Одним із перших правових актів, який врегулював деякі аспекти кіберсквотингу, був Закон США «Про захист споживачів від кіберсквотингу» (англ. Anticybersquatting Consumer Protection Act, 1999) [1]. В законі немає поняття «кіберсквотингу», але є роз'яснення того, що особа, яка почала використання чужого доменного імені, а саме не належне їй право, то ця особа буде притягнена до цивільної відповідальності власником торговельної марки, власником персонального імені, яким було надано правову охорону як і знаку. Однак міститься вказівка на, те що особа яку буде притягнено до відповідальності повинна мати недобросовісний умисел своїх дій на отримання прибутку від самого початку використання чужого ім'я, але якщо особа не могла навіть здогадатися про існування такого імені, то вона може бути звільнена від відповідальності, якщо доведе відсутність у своїх діях умислу в судовому порядку, однак це не стосується уже давно відомих брендів, які визнані у всьому світі, відповідно відповідальність за їх використання

настає незалежно від умисної поведінки особи, яка почала використання такого бренду, для отримання прибутку [2].

Практика сьогодення показує, що часткова «успішність» кіберсквотингу залежить від принципу «first come – first get», дослівний переклад означає «перший прийшов – перший отримав», тобто все залежить від першості реєстрації заявки доменного імені. Так, відповідно до п.п. 2.4, 2.5 Правил домену.UA, адміністратор у порядку надходження обробляє заявки на надання будь-яких імен в публічному доступі, однак таке надання неможливо, якщо правилами окремого конкретного публічного домену не встановлено іншого. Однак публічний домен у відповідності до правил, може встановити «період одночасності», що в свою чергу означає – інтервал часу, а саме момент надходження першої заявки на доменне ім'я і надходження наступних заявок на це доменне ім'я, після надходження першої будуть вважатися такими, що отримані одночасно із надходженням першої.

Кіберсквотер полягає в умисній та недобросовісній реєстрації доменного імені з порушенням прав іншої особи на торговельну марку (ТМ). Простіше кажучи це таке собі викрадення, яке являє реєстрацію уже відомого доменного імені з деякими незначними змінами, для подальшого продажу таких доменних імен чи розміщення потрібної реклами лжевласниками такого доменного імені. Саме визначення поняття доменного імені міститься в Законі України «Про охорону прав на знаки для товарів і послуг» від 15.12. 1993 року, де зазначається, що доменне ім'я – ім'я, що використовується для адресації комп'ютерів і ресурсів в Інтернеті [4].

Для того, щоб вберегти себе від кіберсквотера чи простіше кажучи «захвату доменних імен», потрібно ознайомитися з наступними його видами:

– тайпосквотинг – реєстрація доменних імен, близьких по написанню з адресами популярних сайтів з розрахунку на помилку частини користувачів. Наприклад, «prawda.com.ua» з розрахунку на користувача, який хотів потрапити на «www.pravda.com.ua». При близькості до дуже популярних доменів тайпосквотер може зібрати на своєму адресі деякий відсоток відвідувачів, що «промахнулися», і за рахунок показу реклами заробити грошей.

– брендовий кіберсквотинг – реєстрація доменних імен, що містять товарні знаки, фірмові найменування, популярні власні імена, тобто, засоби індивідуалізації, що охороняються законом. Хоча при цьому у кіберсквотера є ризик позбутися домену і бути притягненим до відповідальності, але законні власники товарних знаків часто воліють не судитися, а викупляти захоплені домени.

—захисний кіберсквотинг — коли легальний власник популярного сайту (товарного знаку) реєструє всі доменні імена, близькі, співзвучні, схожі, зв'язані змістовно з його власним доменним ім'ям. Робиться для того, щоб не стати жертвою кіберсквотерів. Наприклад, власник популярного сайту «google.com», очевидно, захоче також зареєструвати домени «google.com», «gooogle.com» і «gooogle.com», щоб перенаправляти з них відвідувачів на свій основний сайт, а також «anti-google.com.com», щоб не використовувати його.

Виходячи з вищезазначеного, можна вивести характерні ознаки, які притаманні «кіберсквотингу», а саме:

—дії особи, які безпосередньо спрямовані на реєстрацію певного позначення у мережі Інтернет, а зазвичай це реєстрація уже існуючого доменного імені;

—діяльність особи пов'язана з реєстрацією такого доменного ім'я є неправомірною, тобтоздійснюються за відсутності будь-яких прав на таке ім'я;

—такі дії є умисними, недобросовісними та спрямованими на отримання прибутку від можливого перепродажу неправомірно зареєстрованого доменного імені.

Підсумовуючи, вищезазначене, для того щоб вберегти себе від кіберсквотеру у цифровій добі сьогодення потрібно дотримуватись простих правил, по-перше це заявити про першість реєстрації доменного імені у відповідності до діючого законодавства, керуючись вище описаним принципом «first come — first get»; по-друге створювати схожі доменні імені до свого домену, що звичайно буде дорожче для власника доменного імені, однак цим самим можна вберегти себе від недобросовісних осіб, що в майбутньому не зможуть отримати прибуток від такого доменного імені.

ЛІТЕРАТУРА:

1. The Anticybersquatting Consumer Protection Act (ACPA), enacted as P.L. 106-113 (November 29, 1999). URL:<http://www.law.cornell.edu/uscode/text/15/1125> (переклад авт.).
2. The Anticybersquatting Consumer Protection Act (ACPA), enacted as P.L. 106-113 (November 29, 1999). URL:<http://www.law.cornell.edu/uscode/text/15/1125> (переклад авт.).
3. Актуальні проблеми цивілістики у цифрову добу: монографія А437/за ред. Є.О. Харитонов, О.І. Харитонової; НУ ОЮА. — Одеса: Юридична література, 2018. — 248 с. — (Серія: Цивілістика та «ІТ-право»).
4. Про охорону прав на знаки для товарів і послуг: Закон України від 23 грудня 1993 року № 3689-XII (із змін. та доп.) // Відомості Верховної Ради України.— 1994. — № 7. — Ст. 7.