УДК 347.77

НАУЧНЫЙ ЖУРНАЛ
«БИЗНЕС И ОБЩЕСТВО»

Брик Ника Игоревна

студент магистратуры
Санкт-Петербургский государственный
экономический университет
Санкт-Петербург, Россия

КИБЕРСКВОТТИНГ: АНАЛИЗ И ПЕРСПЕКТИВА РЕШЕНИЯ ПО ПРОТИВОДЕЙСТВИЮ РЕГИСТРАЦИИ СХОЖИХ ДОМЕННЫХ ИМЁН

Аннотация

Рассматривается актуальная проблема – регистрация доменных имён, схожих с известными брендами и товарными знаками, с целью последующей их перепродажи или использования в корыстных целях. Такая практика имеет краткое название – киберсквоттинг. Особое внимание уделяется возможностям усиления ответственности за регистрацию схожих доменных имён, включая предложения по изменению нормативно-правовой базы и внедрению новых механизмов разрешения споров.

Ключевые слова: киберсквоттинг, доменное имя

В современном цифровом мире, где интернет стал важной частью жизни, бизнес-процессов и коммуникаций, незаконное использование имени или товарных знаков стали наиболее актуальными угрозами для компаний и брендов. Этот феномен, заключающийся в захвате доменных имён, называется киберсквоттинг и имеет достаточно большое распространение – уже складывается судебная практика по разрешению таких дел.

Актуальность изучения киберсквоттинга обусловлена значительным ростом использования цифровых платформ для ведения бизнеса и последующего увеличения дохода. На момент исследования доменные имена по закону не отнесены к средствам индивидуализации ввиду чего способ защиты ограничен. Изучение такого явления как захват доменного имени поможет выявить возможные пути решения.

Прежде чем начать подробное исследование вопроса предотвращения киберсквоттинга, стоит точнее раскрыть понятие и отличительные черты исследуемого феномена. Впервые термин «киберсквоттинг» (cybersquatting) был использован в Законе о защите прав потребителей от киберсквоттинга (Anticybersquatting Consumer Protection Act) [6]. Закон был принят Конгрессом США и подписан президентом Биллом Клинтоном для защиты услуг или товарных знаков частных лиц и предприятий в США [7]. Основная суть закона заключается в редакции ранее принятого Закона о товарных знаках 1947 года в части предоставления возможности законному владельцу возбудить судебное разбирательство против любого физического или юридического лица, которое со злым умыслом и

недобросовестно регистрирует доменное имя, которое имеет обманчивое сходство с известным товарным знаком или идентично ему, с намерением извлечь из этого выгоду. Благодаря тщательному анализу Конгресса были выявлены основные аспекты нового нарушения авторских прав на товарные знаки организаций и частных лиц:

1) Приводит к введению потребителей в заблуждение и создает путаницу в общественном восприятии относительно подлинного источника или финансирования товаров и услуг;

2) Наносит вред электронной коммерции, которая имеет важное значение для международной торговли и экономики Соединенных Штатов;

3) Лишает законных обладателей товарных знаков значительных доходов и доверия со стороны потребителей;

4) Налагает на владельцев товарных знаков неоправданное, чрезмерное и непосильное бремя по защите их ценных активов.

Первое дело, где напрямую был затронут киберсквоттинг, было рассмотрено Всемирной организацией интеллектуальной собственности (далее – ВОИС) в Женеве в 2000 году [8]. Ввиду того, что изначально регистрация новых доменных имён была бесплатной, пользователи сети Интернет регистрировали короткие и звучные имена, чтобы заинтересованный круг лиц мог быстро и просто находить нужную информацию. При рассмотрении нарушенного права компании было выявлено, что физическое лицо с целью вымогательства денежных средств создал копию существующего сайта организации. ВОИС, рассматривая это дело, вынес решение в пользу компании, ввиду прямого нарушения права на товарный знак. По мере развития сети Интернет, регистрация доменных имён стала платной.

Как было упомянуто ранее, по своей сути киберсквоттинг представляет собой регистрацию, торговлю или использование доменного имени в Интернете с недобросовестным намерением получить прибыль от деловой репутации товарного знака, принадлежащего кому-то другому. В данный момент достаточно сервисов для регистрации новых доменных имён, поэтому у администраторов нет никаких трудностей для дальнейших действий.

В своей работе Будагова М.М. подробно описала процесс киберсквоттинга, указав все этапы нелегальной деятельности.

Первоначально киберсквотер проводит анализ наиболее популярных поисковых запросов, учитывая временной фактор, географическое положение и сезонность.

Выявив увеличение спроса на конкретное словосочетание, он анализирует веб-сайты, содержащие это слово в доменном имени. На частоту запросов могут влиять актуальные новости, особенно те, которые затрагивают крупные компании. Выбрав подходящий набор символов, кибersквотер переходит к следующему этапу: отслеживанию дат регистрации интересующих его доменных имён. Доменные имена регистрируются на срок до одного года, и по истечении этого срока правообладатель должен продлить регистрацию. В противном случае доменное имя может быть захвачено кибersквотером [2].

Однако, просто создать доменное имя с набором цифр и букв в ссылке нельзя – для регистрации доменных имён предусмотрены правила, в зависимости от зоны регистрации. К примеру, в Российской Федерации Координационный центр доменов национального домена сети Интернет разработали и утвердили правила регистрации для регистрации доменных имён в доменах /РФ/.RU. Помимо технических особенностей, таких как:

1) Не более 63 символов в наименовании;

2) Не содержать символов, отличных от букв, цифр и дефиса.

Доменное имя может содержать в себе наименование товарных знаков [9]. Но в правилах фигурирует оговорка – «…пользователь (администратор) самостоятельно несёт ответственность за выбор доменного имени и за возможные нарушения прав третьих лиц, связанные с выбором и регистрацией доменного имени, а также несет риск убытков, связанных с такими нарушениями…». Важно обратить внимание на то, что в процессе регистрации доменного имени у пользователя есть возможность проверить существующие зарегистрированные доменные имена на сайте аккредитованных Координационным центром регистраторов.

В своей статье тему кибersквоттинга рассматривали Сафоненков П.Н. и Зубач А.В., анализируя возможность отнести кибersквоттинг к объектам правового регулирования. В ходе исследования поднимается вопрос о необходимости законодательного закрепления понятие доменного имени с последующими изменениями в гражданском законодательстве. Авторы работы отмечают актуальность проблемы правовой квалификации доменных имён и защиты прав интеллектуальной собственности в данной сфере – «...Представляется, что за легализацией понятия кибersквоттинга, за должной регламентацией порядка регистрации и использования доменных имён незамедлительно должны следовать изменения в законодательстве в

части установления публично-правовой ответственности за общественно опасные последствия, вызванные конкретной деятельностью киберсквоттеров» [5]. Продолжая мысль об изменении отношения к краже доменных имён, Дьякова Ю.С. справедливо отмечает актуальность проблемы защиты интеллектуальных прав в онлайн-пространстве. По ее мнению, стремительное развитие и расширение интернет-взаимодействия требуют разработки новых, инновационных методов обеспечения правовой защищенности [3]. Для решения этой задачи необходимо активное международное сотрудничество. Объединение усилий стран мира посредством подписания соответствующих соглашений позволит создать эффективный глобальный механизм борьбы с нарушениями прав интеллектуальной собственности в сети Интернет. Такое сотрудничество может способствовать унификации требований к защите, ужесточению мер наказания за правонарушения и, что особенно важно, созданию условий для неотвратимости ответственности за подобные преступления.

В свою очередь, Сальникова А.В. поднимала вопрос об ограниченности полномочий правоохранительных органов и регистраторов. По мнению Сальниковой А.В., регистраторы ограничены тем, что никак не могут противостоять регистрации «дублей», не смотря на существующие правила от Координационного центра доменов .RU/.РФ [10]. «Отказ в регистрации возможен только в том случае, если заявляемое к регистрации доменное имя в точности до символа копирует уже находящуюся в реестре позицию». При этом в правилах Центра указано, что проверку доменных имён, которые подают на регистрацию, осуществляет «..автоматизированные средства обработки заявок, регистратор не имеет технической возможности осуществлять сплошную проверку выбранных пользователями доменных имён..» ввиду чего, перестановку букв или символов, которые может добавить пользователь в доменное имя, система не опознает как нарушение прав правообладателей товарных знаков, которые могут быть нарушены во время регистрации «дубля». А.В. Сальникова также говорит о невозможности применения каких-либо иных мер со стороны правоохранительных органов, если будет обнаружено нарушение - полномочия государственных органов весьма ограничены ввиду временного отсутствия специалистов в сфере информационных технологий и, в частности, доменных имён. Создание специальной структуры или уполномоченной организации, которая будет ответственна за решение всех доменных споров, в особенности решение проблемы с киберсквоттингом [4].

Анализируя заключения исследователей-правоведов, можно прийти к выводу о том, что регулирование кибersквоттинга необходимо уже не только в рамках судебного делопроизводства по делу об использовании товарного знака в доменном имени, но и в качестве самостоятельного предмета спора. Такие изменения повлекут за собой изменения в законодательстве Российской Федерации, а также сам процесс претензионного порядка в случае нарушений прав. К примеру, в случае нарушении своих прав на товарный знак, который присутствует в доменном имени, правообладатель для выяснения данных стороны, которая владеет спорным доменным именем осуществляет запрос регистратору с подтверждением своих прав. Регистрация товарного знака в доменном имени «...может рассматриваться как подача охраняемого наименования для использования в гражданском обороте» [1]. Исходя из правил организации, регистратор может либо сразу предоставить необходимые данные заинтересованному лицу, либо попросит направить адвокатский запрос (в случае если в правилах организации указана строгая процедура предоставления данных ввиду действия Федерального закона «О персональных данных» от 27.07.2006 N 152-ФЗ) [5]. После получения данных от адвоката, правообладатель продолжает претензионный порядок и нередко доходит до суда. Так, в деле А41-85820/2019, индивидуальный предприниматель пользовался доменными именами, которые содержали в себе наименование товарных знаков общества с ограниченной ответственностью. В качестве подтверждения незаконного пользования ООО представило свидетельства на товарные знаки и иные документы, которые подтверждают незаконность предпринимательской деятельности ответчика, которую осуществлял кибersквоттер при помощи своих сайтов [11].

Для эффективного предотвращения кибersквоттинга в российском сегменте Интернета можно предпринять следующие действия:

1. Законодательное регулирование

Российские власти могут принять дополнительные правовые нормы, направленные на борьбу с кибersквоттиннгом:

a) Создание специализированных подразделений внутри органов исполнительной власти (Роскомнадзор, ФАС и др.) для оперативного реагирования на случаи кибersквоттинга.

b) Установление четких критериев идентификации кибersквоттинга и механизма быстрого прекращения противоправных действий.

c) Введение административной и уголовной ответственности за совершение кибersквоттинга, повышение штрафов и санкций для нарушителей.

2. Повышение осведомленности бизнеса и потребителей.

Организовать образовательные кампании среди предпринимателей и юридических лиц, разъясняя риски кибersквоттинга и методы противодействия. Это включает:

a) Проведение семинаров и тренингов по вопросам авторского права и интеллектуальной собственности.

b) Информирование общественности о рисках приобретения поддельных продуктов и услуг через нелегальные ресурсы.

3. Технические средства борьбы

Использование технических решений для обнаружения и блокировки подозрительных ресурсов:

a) Регулярные проверки регистрационных записей доменов на предмет соответствия информации заявленной торговой марки.

b) Автоматизированные алгоритмы распознавания признаков кибersквоттинга на основе анализа метаданных сайта и ключевых запросов.

4. Коллективные инициативы

Создание ассоциации организаций для совместной борьбы против кибersквоттинга:

a) Объединение усилий коммерческих структур и правоохранительных органов для координации мероприятий по предотвращению случаев незаконного захвата доменных имён.

b) Организация коллективных исков против злоумышленников и разработка стратегии по возврату незаконно занятых доменов.

5. Укрепление сотрудничества между участниками рынка

Организация регулярного обмена информацией между владельцами брендов, регистратурами доменов и провайдерами хостинга:

a) Создать единый реестр зарегистрированных брендов и доменных имён для повышения прозрачности процесса владения доменными ресурсами.

b) Заключение меморандумов и договоров о взаимодействии с международными организациями по борьбе с кибersквоттингом.

Предложения носят рекомендательный характер и вопрос о возможности их реализации в реалиях современного регулирования Интернет-пространства будет актуален в ближайшие несколько лет.

Список использованных источников

1. Агаларов В.К. Доменные споры: причины, участники и способы разрешения // Тенденции развития науки и образования. 2019. №53-2. С.20-22. DOI: 10.18411/lj-08-2019-35 EDN: PLSCFA

2. Будагова М. М. Киберсквоттинг как вид недобросовестного использования доменного имени // Вестник РГГУ. Серия «Экономика. Управление. Право». 2013. №19 (120). URL: https://cyberleninka.ru/article/n/kiberskvotting-kak-vid-nedobrosovestnogo-ispolzovaniya-domennogo-imeni-1 (дата обращения: 30.04.2024). EDN: RWBSUL

3. Дьякова Ю. С. Некоторые вопросы защиты прав интеллектуальной собственности в сети «Интернет» // Актуальные проблемы частноправового регулирования общественны отношений. Сборник материалов Международной научно-теоретической конференции. Ответственные редакторы В. И. Фатхи, Н. В. Пономарева. Издательство : Ростовский юридический институт Министерства внутренних дел Российской Федерации (Ростов-на-Дону), 2019. С. 61-67. EDN: AHQYFY

4. Сальникова А.В., Куренкова Е.И. Доменное имя как объект гражданских прав: проблемы правовой охраны // ИС. Промышленная собственность. 2025. N 1. С. 77-84. EDN: AQHZVQ

5. Сафоненков П.Н., Зубач А.В. Киберсквоттинг как объект правового регулирования // Вестник экономической безопасности. 2023. №4. URL: https://cyberleninka.ru/article/n/kiberskvotting-kak-obekt-pravovogo-regulirovaniya (дата обращения: 15.04.2025). DOI: 10.24412/2414-3995-2023-4-103-109 EDN: RETOMS

6. Серго А.Г. О некоторых подходах к правовому регулированию доменного имени // Информационное право. 2005. N 1. С. 31-35. EDN: OGJEHT

7. Anticybersquatting Consumer Protection Act / [Электронный ресурс] // ICANNWiki : [сайт]. — URL: https://icannwiki.org/Anticybersquatting_Consumer_Protection_Act (дата обращения: 12.04.2025).

8. First Cybersquatting Case under WIPO Process Just Concluded / [Электронный ресурс] // WIPO : [сайт]. — URL:

https://www.wipo.int/pressroom/en/prdocs/2000/wipo_pr_2000_204.html (дата обращения: 12.04.2025).

9. Регистраторы доменов / [Электронный ресурс] // Координационный центр доменов .RU/.РФ : [сайт]. — URL: https://cctld.ru/domains/reg/ (дата обращения: 12.04.2025).

10. Предоставление информации по запросам Адвокатов и Правообладателей // РЕГ.РУ URL: https://help.reg.ru/support/pravovyye-voprosy/personalnyye-dannyye/predostavleniye-informatsii-po-zaprosam-advokatov-i-pravoobladateley (дата обращения: 12.04.2025).

11. Определение Верховного Суда РФ от 01.02.2022 N 305-ЭС20-16127 по делу N А41-85820/2019. Доступ из справ.-правовой системы «КонсультантПлюс».