Защита доменных имен от киберсквоттинга

Юлиана Латыпова, Никита Пыжиков

С ростом цифровизации почти невозможно представить работу компании на международном рынке без собственного доменного имени.

Доменные имена представляют собой удобные формы интернет-адресов, которые обычно используются для поиска веб-сайтов.

Подбирая доменное имя, компания может обратиться к домену верхнего уровня с кодом страны или региона (country code top level domain, ccTLD — .ru, .fr, .be, .fi, dk, .eu и др.) либо выбрать общий домен верхнего уровня (generic top level domain, gTLD — .com, .net, .org и др.), в т.ч. домен специализированного характера, предназначенный, например, для авиаперевозок (.aero).

Действительным объектом правонарушений и последующих споров становятся, как правило, домены второго уровня (second level domain, SLD), которые, содержат товарный знак, знак обслуживания, фирменное наименование или коммерческое обозначение компании либо географическое указание, — т.е. такие объекты, которые охраняются соответствующими законами о защите прав интеллектуальной собственности (далее ИС), а иногда и законодательством о конкуренции.

Сложность охраны доменных имён возникает в связи с тем, что система их регистрации обычно работает по принципу «first-come, first-served», что дает право зарегистрировать доменное имя первому заявителю даже при отсутствии у него законного интереса и без наложения на него обязательств по коммерческому использованию доменного имени. Подобные причины порождают явление «киберсквоттинга» — регистрации доменных имен третьими лицами с целью дальнейшей перепродажи компаниям, которые еще не вышли на рынок или не успели зарегистрировать свое доменное имя. В отдельных случаях киберсквоттинг подразумевает регистрацию схожего доменного имени с целью ввести в заблуждение потребителя (например, “abibas.com”).

На международном уровне защита доменных имен от киберсквоттинга обеспечивается в соответствии с Единой политикой разрешения споров по доменным именам (UDRP), разработанной Интернет-корпорацией по присвоению имен и номеров (ICANN). UDPR обязателен для всех аккредитованных ICANN регистраторов доменных имен в Интернете, но действует только в отношении общих доменов верхнего уровня (.com, .net, .org и т.д.). В случае возникновения споров, их разрешением занимаются аккредитованные ICANN организации, среди которых есть и Всемирная организация интеллектуальной собственности (ВОИС). ВОИС также рассматривает споры в отношении доменов верхнего уровня с кодом страны, но только в случае, если UDPR был принят страной для таких доменных имен (Россия не приняла). Статистика разрешения споров ВОИС свидетельствует о стремительном росте количества дел (для доменов верхнего уровня), вызванных киберсквоттингом. За период 2003-2018 гг. число споров, инициированных правообладателями товарных знаков, увеличилось более чем в 3 раза (с 1,1 тыс. до 3,45 тыс.). Чаще всего инициаторами споров в 2018 г. выступали США, Франция и Великобритания — на их долю приходилось более 53% всех споров. Среди ответчиков лидируют США, Китай и Великобритания (44% всех споров). Россия встречается в соответствующих отчетах ВОИС, преимущественно, в качестве ответчика.

В качестве аналога UDRP, адаптированного под рассмотрение споров о доменах верхнего уровня с кодом страны (ccTLD), отдельные юрисдикции разрабатывают механизмы альтернативного разрешения споров (ADR), которые могут как дублировать UDRP, так и существенно от него отступать в части организации процедуры и оснований предъявления иска.

Например, в Дании Комиссия по рассмотрению жалоб в отношении доменных имен (The Complaints Board for Domain Names — специализированный орган, уполномоченный рассматривать споры по доменам верхнего уровня .dk) имеет постоянный состав членов. В соответствии с Правилами UDRP, три панелиста назначаются совместно истцом, ответчиком и организацией, которая выступает площадкой для разрешения спора.

Возможности защиты правообладателей средств индивидуализации от киберсквоттинга в разных странах мира зависят, как правило, от соответствующих законов, регулирующих рассматриваемый объект интеллектуальной собственности. В отдельных странах предусмотрено специальное законодательство, направленное на борьбу с киберсквоттингом.

В США с 1999 г. действует Закон «О защите потребителей от киберсквоттинга» (ACPA). Закон возлагает ответственность на лицо, которое с недобросовестным намерением извлечь выгоду, регистрирует, перемещает или использует доменное имя, идентичное, либо схожее до степени смешения с «отличительным» знаком. Если установлено нарушение ACPA, суд может распорядиться о конфискации, либо аннулировании доменного имени или

его передаче владельцу товарного знака. Обвиняемое лицо могут заставить возместить установленные законом убытки (от $1 тыс. до $100 тыс.). Фактические убытки включают прибыль, которую лицо зарегистрированного доменного имени получило от использования товарного знака, а также убытки, понесенные правообладателем знака в результате действий обвиняемого. Знак, состоящий из доменного имени, может быть также зарегистрирован в качестве товарного знака или знака обслуживания в Ведомстве по патентам и товарным знакам США.

В некоторых странах ЕС (например, в Дании, Финляндии, Франции и Бельгии) положения о недопустимости киберсквоттинга содержатся в законодательстве о доменных именах.

Согласно Закону Дании о доменных именах в интернете 2014 г., явным образом запрещается т.н. «складирование» — регистрация доменного имени исключительно с целью последующей перепродажи или передачи другому лицу.

Закон Финляндии о доменных именах 2003 г. запрещает подавать заявку о регистрации доменных имён с целью их «складирования» и перепоставки, однако умалчивает о том, каким образом подобные намерения могут быть установлены в момент подачи заявки, за исключением маловероятных случаев личного признания заявителя. Тем не менее, последующее обнаружение «складирования» является основанием для отзыва доменного имени.

По смыслу финского законодательства «складирование» и нарушение прав на средства индивидуализации представляют собой разные правонарушения. Возможное нарушение прав третьих лиц на товарный знак, «охраняемое наименование» или имя собственное должно быть проверено Финским агентством по регулированию в сфере коммуникаций (FICORA) ещё до регистрации доменного имени — профилактической проверки на намерение «складировать» доменные имена FICORA не осуществляет. Если же факт нарушения прав на средства индивидуализации открывается после регистрации в условиях, когда владелец доменного имени не может подтвердить своих законных прав на товарный знак, «охраняемое наименование» или имя собственное, элементы которых содержит доменное имя, FICORA отзывает регистрацию.

В отличие от приведенных выше примеров, в Китае, как и в большинстве стран, не предусмотрено специальных законов для борьбы с киберсквоттингом. Право на доменное имя в Китае можно рассматривать как расширение прав на соответствующий товарный знак. Процесс разрешения споров по данному вопросу сравним с процессом по товарным знакам. Институтами разрешения споров в Китае являются Китайская международная экономическая и торговая арбитражная комиссия (CIETAC) и Народный суд. Чтобы выиграть спор по киберсквоттингу в Китае необходимо соблюдение следующих условий:

— Во-первых, нужно доказать, что права заявителя являются законными и действующими (для этого необходимо иметь зарегистрированный на территории Китая соответствующий товарный знак);

— Во-вторых, нужно доказать, что обвиняемая сторона действовала недобросовестно. Согласно Закону Китая «О товарных знаках», ответчик действовал недобросовестно, в случае, если регистрация и использование доменного имени осуществлялись в коммерческих целях, а доменное имя совпадает с зарегистрированным товарным знаком заявителя или доменным именем. Сюда также относится случай, когда ответчик не использовал и не намеревался использовать доменное имя, но намеренно препятствовал регистрации доменного имени лицом, обладающим правами на него или предложил продать доменное имя.

Максимальный размер возмещения ущерба по подобным спорам в Китае не может превышать 250 тыс. юаней (или $36,6 тыс.).

В России, как и в большинстве стран мира нет специальных законов, регулирующих исключительное право на доменные имена. Упоминание доменного имени в нормативных правовых актах имеет место, в основном, применительно к использованию доменного имени для осуществления исключительного права на товарный знак (ст.1484 Гражданского кодекса РФ) и наименования места происхождения товара (ст.1519 ГК РФ).

Постановлением президиума Суда по интеллектуальным правам от 28 марта 2014 г. № СП-21/4 доменные споры определяются как споры по использованию доменных имен, тождественных или сходных до степени смешения с товарными знаками или иными средствами индивидуализации юридических лиц, товаров, работ, услуг и предприятий. Только 1,2% доменных имен в российском Интернете охраняются в качестве товарных знаков.

Правообладатель товарного знака может оспорить использование идентичного или схожего до степени смешения доменного имени в национальном суде. Подобная ситуация справедлива также для фирменного наименования компании, если доменное имя содержит в себе фирменное наименование организации, содержащееся в учредительных документах.

При рассмотрении ситуаций с использованием товарных знаков в доменном имени выделяются следующую виды нарушений:

— нарушение используется для создания препятствия правообладателю, для размещения информации о нем и его товарах (услугах) в указанном домене;
— у владельца доменного имени нет каких-либо законных прав и интересов в отношении доменного имени;
— доменное имя зарегистрировано и используется “недобросовестно”.

Доменные имена — одни из наиболее уязвимых объектов интеллектуальной собственности. Возможности для их защиты пока ограничены (в большинстве стран отсутствуют специализированные законы), а вероятность столкнуться с киберсквоттингом возрастает ежегодно, о чем свидетельствует статистика ВОИС. При этом международная система для разрешения подобных споров, касается пока только общих доменов верхнего уровня. Для борьбы с данной проблемой отдельные страны уже лоббируют включение в региональные торговые соглашения специальных положений о защите доменных имен от киберсквоттинга (пример — Всеобъемлющее и Прогрессивное Транстихоокеанское Партнерство (ВПТТП)). На международных площадках данная тема получила развитие, преимущественно, на полях ВОИС.