Мониторинг актуальных событий в области международной торговли

№ 33

17 июля 2019 года

ВСЕРОССИЙСКАЯ АКАДЕМИЯ ВНЕШНЕЙ ТОРГОВЛИ

АТЭС
Российский центр исследований АТЭС

КЛЮЧЕВЫЕ ВОПРОСЫ

Развитие цифровизации оказывает влияние на международную торговлю, с одной стороны снижая традиционные барьеры, с другой — формируя новые ограничения в ответ на вызовы, которые влечет развитие технологий. Вне зависимости от целей цифрового регулирования, в большинстве секторов оно создает дополнительные барьеры для доступа услуг на зарубежные рынки. Расчеты ИМЭФ показывают, что **либерализация цифрового законодательства может привести к существенному снижению общего уровня нетарифных ограничений, действующих как в отношении российских экспортеров услуг на зарубежных рынках, так и для иностранных компаний, поставляющих услуги в Россию**. Такая либерализация, однако, должна учитывать сопряженные с ней риски информационной безопасности.

Большинство стран занимается регулированием потоков персональных и других категорий чувствительных данных путем внедрения либо отдельного закона о защите персональных данных, либо внесения положений о защите персональных данных в соответствующие секторальные законы. Регулирование в данной сфере является одним из ключевых элементов обеспечения национальной и информационной безопасности. Одновременно, формирование требований к политике защиты персональных и других категорий чувствительных данных может создавать дополнительные сложности для торговли компаний в цифровую эпоху.

С распространением кибersквоттинга (регистрация доменных имен с целью перепродажи или введения потребителя в заблуждение) особенно актуальным становится защита доменных имен компаний, которые оказываются объектами недобросовестных «предпринимателей». **За период 2003–2018 гг. число споров в отношении доменных имен выросло в 3 раза.** Способы защиты и разрешения конфликтных ситуаций в отношении исключительных прав на доменные имена варьируются: у одних стран — специальное законодательство, у других они защищены в рамках действующих законов по охране прав интеллектуальной собственности, а иногда и законодательством о конкуренции.

Онлайн-урегулирование споров (ОУС) может упростить процедуры разрешения спорных ситуаций, возникающих как в онлайн-среде, так и офлайн в секторах C2C, B2C и B2B. Инициативы по развитию механизмов ОУС продвигаются на трех уровнях: международном, национальном и частном. **В России и ЕАЭС готовится необходимая законодательная база, однако, примеров применения ОУС не много.** Существуют перспективы развития ОУС в рамках ЕАЭС.

I. Возможности и риски от снижения цифровых барьеров

Цифровизация меняет традиционное представление о торговле товарами и услугами, размывая существующие барьеры. Возможности, формируемые цифровыми технологиями, уже вносят существенные коррективы в структуру и способ ведения торговли.

Цифровизация рынков требует существенных регуляторных изменений. Как многостороннее, так и национальное регулирование находятся на стадии формирования. Вопросы «барьерности» цифрового регулирования — предмет дискуссий международного сообщества. Одни страны называют цифровое регулирование торговым протекционизмом, другие считают такую политику необходимой для достижения законных целей. В некоторых случаях подобные меры более обременительны, чем того требует достижение легитимных целей национальной политики. Между тем, даже когда регулирование является оптимальным с точки зрения баланса защиты национальных интересов и обеспечения свободной торговли, оно может создавать барьеры для международной торговли.

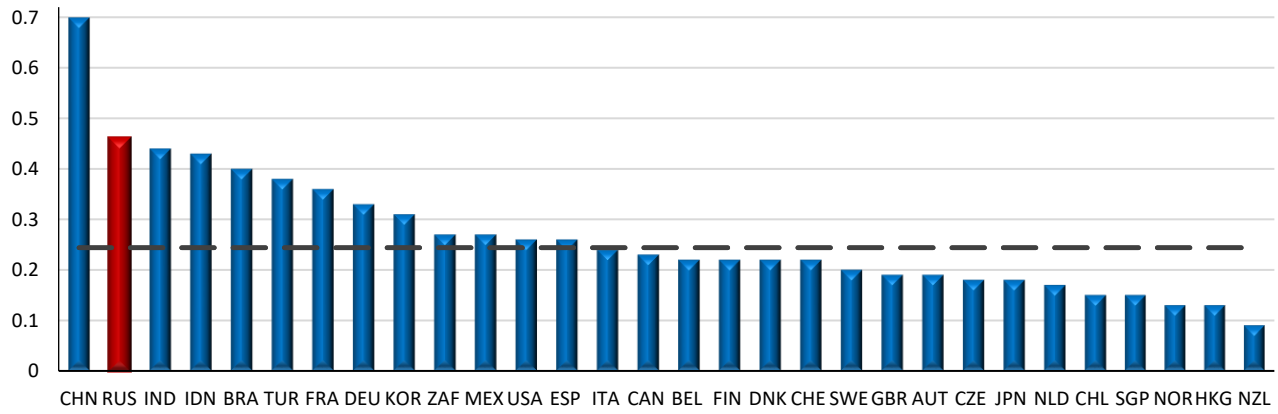
Систематизация и оценка уровня таких барьеров стали осуществляться относительно недавно. Наиболее известные — Индекс цифровых ограничений в торговле (DTRI) ECIPE и Индекс цифровых ограничений в торговле услугами (Digital STRI) ОЭСР. Оба показателя относят Россию к наиболее зарегулированным экономикам с точки зрения цифровых ограничений. Так, значение общего индекса DTRI для России составляет 0,46 — второй по величине показатель среди 64 стран, по которым рассчитывается индекс. По данным ОЭСР, Россия по уровню цифровых ограничений в торговле услугами находится на пятой позиции со значением индекса Digital STRI 0,34, уступая лишь Китаю, Индонезии, Саудовской Аравии и Бразилии.

Проведенная ВАВТ ИМЭФ работа подтверждает, что регулирование цифровой торговли в странах БРИКС действительно создает высокие барьеры для международной торговли, однако разрыв в показателях «барьерности» для стран с наиболее и наименее высокими уровнями цифровых ограничений преувеличен.

По оценкам ИМЭФ ВАВТ, по большому числу показателей (включая регулирование условий взаимодействия с действующими операторами связи, правила трансграничной передачи данных, вопросы защиты прав интеллектуальной собственности, регулирование осуществления электронных транзакций[1] и платежей) требования российского законодательства не являются более обременительными, чем в других анализируемых странах. В ряде случаев можно говорить о том, что в других странах, проанализированных ОЭСР, существуют барьеры, отсутствующие в России. В этой связи, целесообразно проводить работу по снижению существующих в странах-партнерах ограничений для российских экспортеров услуг.

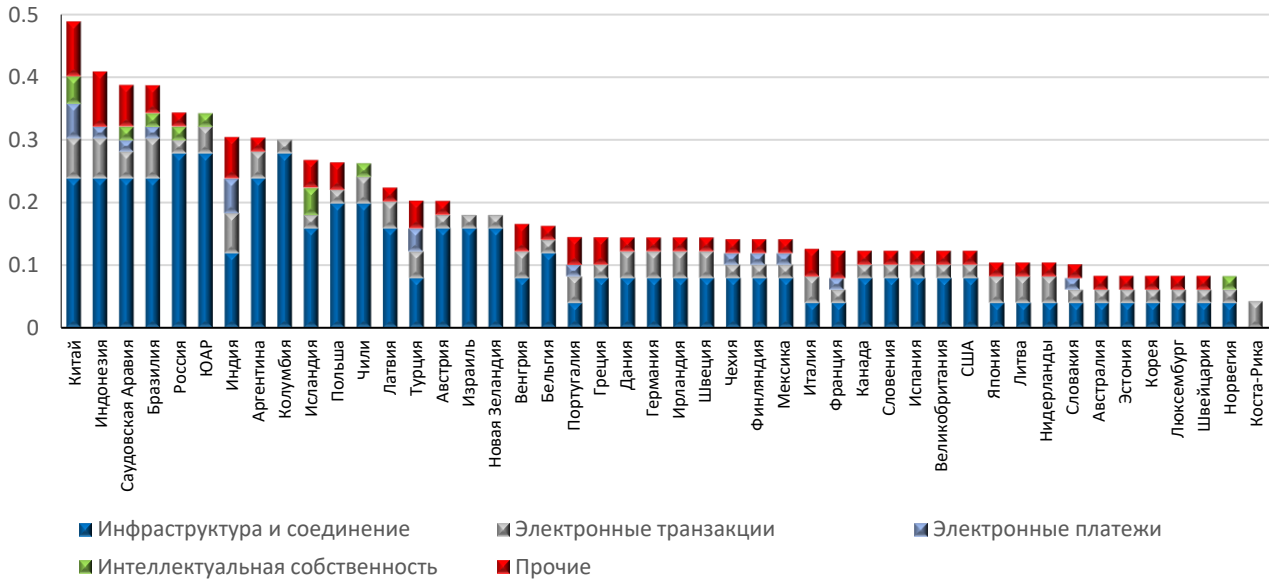
[1] О дискриминации иностранных поставщиков с точки зрения условий получения лицензий на осуществление электронной коммерции мы писали в Мониторинге №30.

Сравнение индекса ограничений DTRI для РФ с другими странами и со средним значением по 64 странам



Источник: ECIPE

Значения индекса Digital STRI по странам и группам ограничений в 2018 г.



Источник: ОЭСР

На сегодняшний день Россия не применяет общие дискриминирующие меры для проведения электронных платежей. Российские стандарты в части платежей соответствуют международным. Однако барьеры могут появиться в случае принятия законопроекта, который подразумевает, что иностранные платежные системы будут обязаны зарегистрироваться в России и подать соответствующее заявление о внесении в специальный реестр Банка России. Кроме того, в России действуют точечные дискриминационные меры в отношении отдельных стран.

Снижение уровня ограничений на электронные платежи в странах-партнёрах России позволит сократить общий уровень нетарифных барьеров на зарубежных рынках для российских поставщиков. Это произойдет, если страны откажутся от дискриминационных мер в отношении иностранных поставщиков, а также будут ориентироваться на международные стандарты платёжных систем. Положительные эффекты будут иметь место для таких секторов, как транспортные, страховые, финансовые, строительные, ИКТ услуги, поездки, услуги частным лицам и услуги в сфере культуры и отдыха (в последнем случае снижение нетарифных барьеров может достигать 33,7%).

Что касается устранения других барьеров для российских поставщиков услуг на зарубежных рынках, есть потенциал для снижения ограничений на рекламу онлайн, загрузку и передачу данных; инвестиционные ограничения в отдельных секторах, а также требования для получения национального доменного имени[2]. Аналогичных барьеров (за исключением фильтрации веб-контента) в российской практике выявлено не было, что дает возможность продвижения мер в области либерализации регулирования на рынках третьих стран и, тем самым, упрощения доступа на внешние рынки российских поставщиков услуг. Ожидаемое снижение нетарифных барьеров в случае устранения данных видов ограничений для поставщиков транспортных, строительных, страховых и ИКТ услуг, поездок, а также услуг по переработке товаров может достигать 25–40%.

В ряде случаев российская практика достаточно ограничительна с точки зрения развития электронной торговли услугами. Требования по локализации данных усложняют ведение торговли отдельными категориями услуг.

В случае устранения Россией требований по локализации данных существенное снижение общего уровня нетарифных ограничений на российском рынке произойдет по целому ряду секторов, включая страховые, финансовые, услуги частным лицам и услуги в сфере культуры и отдыха, плату за пользование интеллектуальной собственностью (максимальное снижение нетарифных ограничений в отношении услуг при снижении рассматриваемого барьера характерно для услуг частным лицам и

[2] Мы писали об этом подробно в Мониторинге №31.

услуг в области культуры и отдыха, показатель может составить от 10,8 % до 44,4%).

Устранение барьеров локализации на рынках стран-партнеров приведет к снижению общего уровня нетарифных ограничений и для российских экспортеров аналогичных услуг в среднем на рынках иностранных государств, в которых соответствующие барьеры присутствуют. В частности, возможное снижение нетарифных барьеров для страховых услуг может составить от 14,2 % до 38,4%.

Несмотря на положительные эффекты, связанные со снижением уровня барьеров в торговле, возможные меры по либерализации рынков должны учитывать и риски, ключевой из которых — угроза национальной и информационной безопасности, включая триаду угроз — использование ИКТ в террористических, преступных и военно-политических целях. В связи с наличием существенных рисков безопасности, будущее снижение цифровых барьеров будет сталкиваться с серьезным сопротивлением со стороны заинтересованных лиц.

II. Регулирование вопросов защиты данных: международная практика

Вопросы регулирования трансграничных потоков данных и обеспечения защиты конфиденциальности данных занимают не последнее место в международной цифровой повестке, а увеличение случаев утечек персональных и других категорий чувствительных данных и/или их использования в социальной инженерии продолжают привлекать интерес экспертов по всему миру. Это доказывает необходимость выработки таких механизмов обработки персональных и других типов данных, которые одновременно обеспечивали бы их надежную защиту и способствовали техническому прогрессу и инновациям (посредством предоставления легитимного доступа к данным для развития таких технологий, как Большие данные, искусственный интеллект и Интернет вещей).

В этой связи ОЭСР принял рекомендации по развитию искусственного интеллекта, поддержанные затем G20 и утвержденные в приложении к «Заявлению Министров торговли и цифровой экономики», 8–9 июня 2019 г. Рекомендации включают необходимость создания открытых баз данных (с привлечением государственных и частных инвестиций) и поощрение создания фондов данных для развития искусственного интеллекта. Одновременно, при формировании новых механизмов рекомендуется обеспечивать защиту персональных данных и соблюдение требований информационной (цифровой) безопасности с тем, чтобы новые технологии не навредили человеку и не создавали угроз его безопасности.

Тенденции последних лет показывают, что все больше стран занимаются регулированием потоков персональных данных путем внедрения либо отдельного закона о защите персональных данных, либо внесения положений о защите персональных данных в соответствующие секторальные законы, например в законы об информационной безопасности, телекоммуникациях, электронной коммерции (см. таблицу ниже). Основные вопросы касаются того, кто будет владеть данными (персональными, государственными и корпоративными) и как обеспечить их безопасный сбор, хранение, обработку и удаление, одновременно обеспечив возможность для их использования при дальнейшей оптимизации всех процессов, сохранив необходимую степень конфиденциальности данных. В 1990-х гг. в мире насчитывалось около 20 стран, регулирующих потоки персональных данных, однако уже к 2015 г. их количество превысило 100. И их количество только растет из года в год.

Согласно «Индексу ограничительности торговли услугами в секторе телекоммуникаций» ОЭСР, 37 стран применяют более строгое законодательство по сравнению с «Рекомендациями ОЭСР по защите персональных данных и трансграничным потокам персональных данных».

Передача отдельных видов данных (финансовой, медицинской и бухгалтерской информации, а также корпоративных данных), как правило, регулируется отдельными секторальными нормативно-правовыми актами, как в странах с всеобъемлющим, так и в странах с секторальным подходом.

ЮНКТАД определил 8 основных принципов защиты персональных данных, характерных для всех стран (см. рисунок ниже).

Подходы стран к регулированию вопросов защиты персональных данных

Всеобъемлющий подход	Секторальный подход		Комплексный подход
Отдельный закон о защите персональных данных	Нет отдельного закона о защите персональных данных, положения о защите персональных данных включены в секторальные законы		Защита персональных данных регулируется как отдельным законом, так и положениями в секторальных законах, а также законами отдельных штатов и/или территорий
	Различия по штатам (регионам) при секторальном подходе в целом	Секторальный подход на всей территории страны	
Россия, ЕС[3] («Общий регламент защиты персональных данных» (GDPR)), Израиль, Малайзия, Мексика, Сингапур, Турция, Южная Корея, Япония.	Индия, Китай (отдельно в Гонконге и на Тайване), ОАЭ (отдельно для свободных экономических зон), США.	Бразилия, Бруней-Даруссалам, Вьетнам, Индонезия (единый закон обсуждается), Иран, Нигерия, Чили.	Канада (отдельное регулирование принято в провинциях Альберта, Британская Колумбия и Квебек, наряду с всеобщим законом о защите конфиденциальности данных и электронных документах (PIPEDA), Австралия.

[3] Подход ЕС является примером для многих стран. При этом, что вопросы локализации данных рассматриваются каждой страной отдельно.

Восемь основных принципов защиты персональных данных, выявленных ЮНКТАД

Открытость	•организации обязаны быть открытыми в отношении порядка сбора и использования персональных данных (ПД)
Ограничения на сбор ПД	•сбор ПД должен быть ограниченным, законным и справедливым, обычно с оповещением и/или с согласия субъекта ПД
Указание цели	•цели сбора и разглашения ПД должны быть четко обозначены в момент сбора ПД
Ограничения по использованию	•использование или раскрытие ПД должно быть ограничено обозначенной целью или тесно связанными целями
Безопасность	•ПД должны быть обеспечены надлежащей степенью защиты
Качество данных	•ПД должны быть актуальными, точными и вовремя обновляться
Ответственность	•операторы обработки ПД обязаны соответствовать принципам обеспечения защиты ПД

На международных площадках ведутся активные дискуссии о целесообразности локализации отдельных категорий данных, а также других мер регулирования трансграничных потоков данных в контексте возможных ограничений для бизнеса в цифровую эпоху. Однако в ходе исследования ИМЭФ ВАВТ были выявлены другие аспекты политики защиты персональных данных, которые могут усложнять торговлю компаний в цифровую эпоху:

— Нетранспарентность и разрозненность нормативно-правовой базы. Например, в США нет федерального закона о персональных данных. Данная сфера регулируется рядом отдельных законодательных актов, таких как «О неприкосновенности частной жизни», отдельными законами штатов (в одной только Калифорнии принято около 25 законов в данной области), а также секторальными законами (например, о финансовой и медицинской информации). Помимо этого, отдельные ведомства выпускают руководства для бизнеса, например, «Рекомендации для бизнеса и регуляторов о защите персональных данных потребителей в эпоху быстрых изменений» Комиссии США по торговле.

— Высокая стоимость сертификации компаний о соответствии требованиям законодательства в области защиты персональных данных.

— Высокая стоимость мер обеспечения соответствия законодательству (например, для соответ-

ствия GDPR, согласно расчетам Ernst & Young, 500 крупнейших компаний мира должны будут потратить $7,8 млрд).

— Слишком высокие штрафные санкции за несоблюдение мер и отсутствие досудебного порядка разрешения возникших разногласий и споров. Например, Uber согласился выплатить $148 млн штрафа за утечку данных в 2018 г., а в ЕС компании обязали выплатить штрафы, общим объемом в €56 млн (из них €50 млн — Google) за 9 месяцев действия GDPR.

— Отсутствие регулирования или недостаточная степень его проработанности, что создает повышенные риски утечки данных на территории некоторых стран (особенно актуально для наименее развитых стран).

С учетом высокой значимости и необходимости законодательных инициатив в защите персональных и других категорий чувствительных данных, в связи с наличием рисков для национальной и информационной безопасности, обеспечения прав интеллектуальной собственности, защиты прав потребителей и конкуренции на рынке целесообразно принятие следующих мер для снижения издержек:

— формирование общих принципов защиты данных в зависимости от их категории;

— координация действий для предотвращения утечек данных;

— выработка единых стандартов обеспечения защиты данных и качества соответствующих услуг;

— внедрение мер по снижению стоимости услуг по обеспечению защиты данных;

— продвижение международных инициатив по гармонизации и взаимному признанию законодательства в области защиты персональных и других категорий данных (например, «Конвенция 108 +» Совета Европы или двухсторонние и многосторонние соглашения)[4];

— повышение транспарентности законодательства стран, обмен опытом и практиками.

[4] Подробнее о подобных международных инициативах в Вестнике АТЭС (Выпуск 6, январь 2019 г.) «Цифровая экономика: от общего к частному» (статья «Защита персональных данных в АТЭС: подходы экономик и международные инициативы»).

III. Защита доменных имен от кибersквоттинга

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 «кибersквоттинга» — 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 кибersквоттинг подразумевает регистрацию схожего доменного имени с целью ввести в заблуждение потребителя (например, “abibas.com”).

На международном уровне защита доменных имен от кибersквоттинга 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 кибersквоттингом. 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 кибersквоттинга 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 кибersквоттингом.

В США с 1999 г. действует Закон «О защите потребителей от кибersквоттинга» (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 кибersквоттинга 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 кибersквоттингом. 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 кибersквоттингу 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 кибersквоттингом 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 кибersквоттинга (пример — Всеобъемлющее и Прогрессивное Транстихоокеанское Партнерство (ВПТТП)). На международных площадках данная тема получила развитие, преимущественно, на полях ВОИС.

IV. Онлайн-урегулирование споров: международные и российские практики

Онлайн-урегулирование споров (англ. Online dispute resolution, далее по тексту — ОУС) — это способы урегулирования конфликтов с применением Интернет-технологий, считающиеся эквивалентами методов альтернативного урегулирования споров: переговоры, медиация или Третейский суд. ОУС применяется для урегулирования межличностных споров (C2C), коммерческих споров (B2C и B2B) и может в будущем даже быть адаптировано для урегулирования межгосударственных конфликтов.

Законодательные инициативы и уже действующие нормативные документы, регулирующие ОУС, можно подразделить на три группы: международные, государственные и частные. Что касается международных инициатив в данной сфере наиболее активны ICANN, ООН и Европейская Комиссия.

Международные инициативы по ОУС

Название	Инициатор	Год	Краткое описание
Политика разрешения споров в сфере распределения доменных имен (UDRP — Uniform Domain Name Dispute Resolution)	Международная Корпорация по управлению доменными именами и IP-адресами - ICANN	1999	Регулирование споров, связанных с доменными именами, IP-адресами и т.д.
Единая европейская процедура урегулирования малых претензий (ESCP)[5]	Европейская Комиссия	2009	Процедура вступила в силу для всех стран-членов ЕС, она предусмотрена для разрешения трансграничных конфликтов, размер которых не должен превышать €5000 (не включая расходы)
Положение об ОУС в потребительской сфере № 524/2013 (The Regulation on consumer ODR)	Европейская Комиссия	2013	Положение создает основу платформы ОУС для регулирования споров, возникающих в ходе онлайн-торговли.
Технические комментарии ЮНСИТРАЛ по урегулированию споров в режиме онлайн (UNCITRAL Technical Notes on Online Dispute Resolution)	ЮНСИТРАЛ	2017	Комментарии и рекомендации по урегулированию споров онлайн
Разработка «Рамочного соглашения АТЭС для совместного разрешения споров онлайн для малых и средних предприятий (МСП) в сфере B2B» и соответствующих процедурных правил	АТЭС	с 2017	Соглашение должно сформировать основные принципы ОУС в АТЭС, которые планируется применить на практике в рамках региональных пилотных проектов.

[5] Многие эксперты относят ESCP к УСО, однако, данная процедура больше подходит под определение альтернативного регулирования споров (ADR), ставшего предтечей УСО.

Законодательных и пилотных инициатив отдельных государств на данный момент существует немного. Больше всего в этой сфере продвинулись Канада, Китай и США, активно развивающие законодательную базу ОУС в своих странах:

Примеры национальных законодательных инициатив ОУС

Название	Инициатор	Год	Краткое описание
Единый закон о медиации США	США	2001	Законодательное регулирование процесса медиации в процессе решения различных споров.
Муниципальный суд Франклина	США	2018	Онлайн-переговоры и медиация для небольших кейсов (налоги и др.).
Центр разрешения споров по доменным именам Китайской международной экономической и торговой арбитражной комиссии (The Domain Name Dispute Resolution Center of CIETAC)	КНР	2000	Урегулирование споров в сфере B2B, однако, дела в сферах B2C и C2C также встречаются.
Интернет-суд	Гуанчжоу, Пекин (КНР)	2017-2018	Данные суды призваны рассматривать дела в сфере электронной коммерции, права собственности, доменных имен, кражи или фальсификации персональной информации, финансовых операций.
Положения по ряду вопросов, связанных с рассмотрением дел Интернет-судами	Верховный суд КНР	2018	Данные положения определяют сферу ответственности Интернет-судов, распространяющаяся на споры в сфере электронной коммерции, права собственности, авторского права, кражи конфиденциальной информации, доменных имен.
Закон об информационных технологиях[6]	Индия	2000	Благодаря закону электронная коммерция и технологии электронного правительства в стране получили правовую основу.
Закон о судебном разрешении гражданских споров	Британская Колумбия (Канада)	2012	Создает основу для первого онлайн-суда по разрешению гражданских споров, а также дорожно-транспортных споров.

[6] Закон не содержит прямого упоминания ОУС, однако, ряд экспертов сходится во мнении, что данный закон создает достаточную правовую основу для развития ОУС в Индии.

В некоторых странах развиваются частные инициативы по внедрению ОУС (в таблице ниже). В основном они касаются продвижения использования ОУС в различных странах, разработки решений для электронной коммерции и альтернативного регулирования споров.

Примеры частных инициатив по ОУС

Название	Инициатор	Год	Краткое описание
Технический юридический центр передового опыта по онлайн разрешению споров в Индии (Techno Legal Centre of Excellence for online Dispute Resolution in India — TLCEODRI)	Индийская юридическая организация Perry4Law	2012	Организация активно занимается вопросами распространения информации о сфере ОУС, а также предлагает свои варианты внедрения ОУС в стране. Данная инициатива направлена на продвижение технологий и методов онлайн-урегулирования споров в стране.
Основные стандарты практики разрешения споров онлайн в целом	США	2009	Рекомендации по эффективному урегулированию споров онлайн на основе анализа международных практик (не имеют законодательной силы).
Центр разрешения конфликтов eBay	США	2003	Собственный центр eBay, разрешает около 60 млн споров в год (по состоянию на 2014 г.).
PARLe	Канада	2016	Платформа позволила рассмотреть более 4 тыс. кейсов B2C за первые 22 мес. работы (67,8% были урегулированы).

Россия отстает от наиболее развитых государств в области ОУС. В нашей стране классическая медиация в процессе разрешения споров в целом менее востребована, чем на Западе.

Тем не менее, в 2010 г. был принят ФЗ РФ № 193-ФЗ «Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)», который может стать первым шагом в

создании правовой основы для ОУС. В 2019 г. Министерство Юстиции России разместило для обсуждения законопроект по внесению изменений в ФЗ «О защите прав потребителей» и в вышеупомянутый ФЗ №193 с целью их адаптации к ОУС. Проект закона учитывает рекомендации ОЭСР в отношении использования механизма ОУС, как меры онлайн-защиты потребителей и технические комментарии ЮНСИТРАЛ, а также обеспечивает свободу выбора модели ОУС для реализации механизма на практике. Он уже прошел общественные обсуждения. Ведутся обсуждения по внедрению ОУС в ЕАЭС.

Тема ОУС является довольно новой для российских компаний, применяющих более традиционные методы рассмотрения жалоб потребителей (через системы отзывов и предложений, фактически в ручном режиме). Согласно паспорту законопроекта, одними из немногих компаний, прорабатывающих механизмы, ОУС являются «Ассоциация компаний Интернет-торговли» и ООО «Яндекс.Маркет». Интересным является и сервис «debetok» по взысканию дебиторской задолженности онлайн, разработанный АО «Центр развития экономики».

Развитие механизмов ОУС имеет значительный потенциал не только на отечественном рынке, но и для их экспорта, благодаря новизне данного направления, небольшому количеству конкурентов на рынке и широте возможного охвата услуг.

Главные новости

— Китай пообещал снизить ограничения на участие иностранного капитала в секторе страхования к 2020 г. (на год раньше, чем планировал ранее), стимулировать иностранные инвестиции в автопром и другие обрабатывающие сектора, а также сократить число отраслей закрытых для иностранных инвесторов.

— Министерство торговли США введет тарифы до 456% на сталь из Кореи и Тайваня, поставляемую в США через Вьетнам после незначительной переработки. Импорт коррозионностойкой стали из Вьетнама увеличился на 332%, холоднокатаной стали — на 916% после того, как США ввели дополнительные пошлины на сталь из Кореи и Тайваня.

— Россия и Китай подписали межправительственное соглашение о переходе на расчеты в национальных валютах. Проводить платежи будут ВТБ и Торговый банк Китая. По итогам прошлого года товарооборот между РФ и КНР составил $107 млрд, а доля рубля и юаня составила 11% по экспорту из России и 24% по импорту из Китая.

— British Airways могут оштрафовать на рекордные для Великобритании £183 млн из-за утечки данных клиентов и нарушения GDPR. Штрафы за нарушение GDPR могут составлять до 4% глобальных годовых продаж компаний, в данном случае — 1,5%. Компания планирует оспорить это решение. Федеральная торговая комиссия США одобрила соглашение с Facebook на сумму $5 млрд по делу об утечке данных пользователей и их использованию Cambridge Analytica, произошедшей в прошлом году.

— Нигерия и Бенин подписали AfCFTA на саммите Африканского союза. Теперь из всех африканских стран Соглашение не подписала только Эритрея. Секретариат AfCFTA будет в Гане, а Африканский экспортно-импортный банк поддержит создание платформы онлайн-платежей для AfCFTA.

— Россия запросила консультации с США в ВТО в отношении американских антидемпинговых мер на углеродистую сталь.

— Индия поддержала планы АСЕАН завершить переговоры по ВРЭП до конца года. Партнеры Индии по переговорам попросили её обозначить список секторов услуг, которые Индия не готова либерализовать. Следующие министерские встречи по ВРЭП пройдут в августе в Пекине и в сентябре в Бангкоке. Переговорщики достигли предварительных соглашений по антимонопольной политике и разрешению споров.

— Сенат Франции одобрил закон о цифровом налоге. Налог в размере 3% от дохода коснется 30 компаний, преимущественно из США. В ответ США запустили расследование и могут ввести ответные меры в случае выявления дискриминации.

— Индия и Россия отказались от доллара при оформлении сделок по линии военно-технического сотрудничества, чтобы избежать рисков, связанных с угрозами санкций США. Индия — один из главных партнеров России в сфере ВТС.

— Беларусь — крупнейшая экономика из всех активных присоединяющихся к ВТО стран — подтвердила свое намерение присоединиться к ВТО в 2020 г. Она начала процесс присоединения к ВТО в 1993 г.

Выпуск подготовлен совместно Всероссийской академией внешней торговли и Российским центром исследований АТЭС: Гущин Е.С., Исмагилова О.Д., Кнобель А.Ю., Кудакаева К.Р., Кутовая А.Н., Латыпова Ю.Р., Прока К.А., Пыжиков Н.С., Флегонтова Т.А.