Содержание

Кибербезопасность и интеллектуальная собственность. Часть 1

Cybersecurity and itellecrual property. Part 1

Авторы
Карцхия Александр Амиранович, кандидат юридических наук, профессор
Журнал
Вопросы кибербезопасности
Выпуск № 1 (2) / 2014
***Ключевые слова**: интеллектуальная собственность, кибербезопасность, защита интеллектуальной собственности от киберугроз, права на результаты интеллектуальной деятельности.*

Цикл статей посвящен современному механизму защиты интеллектуальной собственности в глобальной информационной среде. Поощрение инновационной деятельности и защита правообладателей от киберугроз выходит на первый план в государственных (национальных) стратегиях интеллектуальной собственности. Интеллектуальная собственность как особо ценный нематериальный актив (базы данных, коммерческие секреты и ноу-хау, компьютерных программ и т.д.) является предметом новых угроз в киберпространстве. Кибербезопасность предотвращает нарушение прав интеллектуальной собственности, а также обеспечивает правообладателям конфиденциальность баз данных, коммерческой тайны и ноу-хау. Защита интеллектуальной собственности в киберпространстве (в том числе современные технические средства) создает необходимый уровень конкурентоспособности для правообладателей.
В первой части цикла рассмотрены вопросы влияния глобализации информационной среды, стратегии информационной безопасности и IP в России и за рубежом с точки зрения юриста. Во второй части будут рассмотрены проблемы интеллектуальной собственность в структуре кибербезопасности, коммерческая тайны и ее защита от киберугроз.
В третьей части предполагаетсяя рассмотреть новые проблемы - защиты доменных имен различного уровня и товарных знаков, юридические проблемы глобализации интернет-торговли и иных услуг в сети Интернет.

Ключевые слова: интеллектуальная собственность, защита интеллектуальной собственности от киберугроз, права на результаты интеллектуальной деятельности.

Новые цифровые технологии и глобальные информационные сети, совершившие настоящую революцию в сфере накопления и обмена информацией, потребовали изменения установившихся принципов защиты интеллектуальной собственности, которая создавалась в совершенно иной технологической среде. Глобальная интернет-среда и развитие информационно-коммуникационных технологий требуют адекватного регулирования отношений с использованием интеллектуальной собственности.

Новые реалии современных IT-технологий и Интернета, полученные знания в сфере биотехнологий и фармакологии ставят новые задачи, для выполнения которых традиционный механизм прав интеллектуальной собственности не всегда приспособлен.

Последние годы произошло усиление коммерциализации интеллектуальной собственности, повышение значения коммерческой аспекта использования и инвестиционной привлекательности прав интеллектуальной собственности, применение исключительных прав как инструмента в конкурентной борьбе. В совместном докладе о правах интеллектуальной собственности Европейского патентного ведомства и Комиссии по гармонизации на внутреннем рынке, представленном в октябре 2013 года отмечалось, что отрасли европейской экономики, которые непосредственно связаны с интенсивным использованием прав интеллектуальной собственности, составляют 39% общего объема промышленной деятельности (ежегодно около € 4700 млрд.), обеспечивая 26% всех рабочих мест (т.е. 56 млн. рабочих мест). В этих отраслях средняя заработная плата выше на 40%, чем в других отраслях промышленности. К аналогичным результатам в отношении экономики США пришли в проведенном в 2012 году исследовании Ведомства США по патентам и товарным знакам совместно с Агентством экономики и статистики администрации США.

Глобализация информационной среды

Современная эпоха, эпоха «интеллектуального капитализма», основана на базовых институтах капитализма (право частной собственности, частный интерес в извлечении прибыли, конкурентные рынки и свободное предпринимательство), где производственные активы и процессы, также как коммерческие сделки и товары, связаны преимущественно с рыночным оборотом нематериальных (интеллектуальных) ценностей, в отличие от товарных рынков материальных активов и продукции. Права интеллектуальной собственности обеспечивают инвесторам своеобразные гарантии инвестиционных рисков и уже рассматриваются как товарная продукция, или даже как своеобразная «валюта».

Вместе с тем, созданная для ускорения инновационного развития посредством защиты интересов правообладателей и стимулирования процесса инноваций система защиты прав интеллектуальной собственности имеет оборотную сторону: стабильное экономическое и технологическое развитие сопровождается снижением конкуренции, высокими затратами по доступу к современным товарным продуктам и технологиям, более высокими ценами на них. Кроме того, оказавшись в центре международного внимания в последние два десятилетия, сфера отношений интеллектуальной собственности породила острые дискуссии и не менее острые вопросы: что такое «интеллектуальная собственность», является ли она финансовым активом или средством национальной и международной конкуренции, либо «моральной» (нематериальной) субстанцией, или же представляет собой средство быстрого разрешения сложных технологических проблем.

Новый облик глобальных экономических отношений, обозначенный как «турбокапитализм», связан с серьезными рисками «практически непредсказуемого возникновения и разрастания кризисных процессов в любых национальных или отраслевых сегментах глобальной экономики», рисками, непосредственно влияющими на осуществление права собственности и социальных прав огромными массами людей. Эти риски находятся вне сферы полноценного правового регулирования и приводят к эрозии национальных систем правовой регуляции экономических отношений. В итоге глобальные процессы «либерализации» экономического законодательства и его трансформации в направлении «свободы рынка», неуклонно сужавшие права государства по контролю за деятельностью бизнес-структур, привели к целой серии корпоративных крахов в период мирового экономического кризиса.

Основная проблема современного экономического развития, по мнению В.Д.Зорькина, «заключается в усилении дисбаланса между ценностями экономической свободы и социальной

справедливости в условиях экспансии финансового турбокапитализма и необузданной игры суперкорпораций на глобальных рынках, не может быть решена на уровне национального правового регулирования. Решение этой проблемы требует введения активизма крупнейших транснациональных игроков глобального рынка в рамки глобального правопорядка». В качестве примера правовых деформаций приводятся факты несоблюдения норм Всемирной торговой организации национальными юрисдикциями за счет искусственного выстраивания разного рода протекционистских барьеров (лицензирование импорта, антидемпинговые расследования и др.).

По оценкам экспертов, транснациональные корпорации отвели существенное место интеллектуальной собственности в стратегиях усиления своих позиций на мировых рынках в целях получения конкурентных преимуществ и монополизации отраслевых товарных рынков и услуг. Применение высокоэффективных стратегий ведения «патентных воин», связанных с переходом от защиты отдельных изделий к агрессивным формам защиты перспективных секторов рынка наукоемкой продукции и формированием мощного портфеля патентов для блокировки научно-технических разработок и производства конкурирующих компаний, изменил условия реализации прав интеллектуальной собственности.

Стремительное увеличение оборота разнообразной информации (включая коммерческую информацию, информацию о новых технологиях, информацию в составе баз данных), глобализация доступа к ней и появление новых средств ее формирования, распространения и использования актуализировали вопросы сохранности и легального использования массивов информации. Информационная безопасность выходит за рамки потребностей отдельных обладателей и выступает уже в качестве одного из направлений национальных стратегий развития.

Во многих странах в настоящее время уже имеется действующее законодательство, связанное с обеспечением информационной безопасности в информационно-коммуникационных сетях, применяются собственные стратегии информационной безопасности. Однако геополитический скандал с незаконным получением информации Агентством национальной безопасности США вновь привлек внимание государственных структур и общественное мнение к проблемам информационной безопасности и защиты частной жизни, в том числе защиты от кибератак и сохранности персональных данных в сети Интернет.

Достаточно показателен в этом отношении тот факт, что Европейский Союз инициировал пересмотр заключенного с Министерством торговли США соглашения Safe Harbor, предусматривающего возможность передачи персональных данных за пределы ЕС американскими компаниями, ведущими деятельность в Евросоюзе. Это происходит на волне публичного скандала с программой сбора данных PRISM Агентства национальной безопасности США. Европейцы утверждают, что Safe Harbor не соответствует Директиве ЕС о защите данных (EU Data Protection Directive) и может входить в конфликт с новым законодательством ЕС о защите персональных данных.

Последствия киберугроз и незаконных действий в информационно-коммуникационной среде приводят не только к имущественным, но и репутационным потерям для обладателей информации. К примеру, в начале сентября 2013, оператор мобильной связи Vodafone (Германия) обнародовал данные о краже данных более чем у двух миллионов из 36 миллионов своих немецких пользователей, включая имена, адреса, банковские коды и номера счетов. Хотя эти данные не давали прямого доступа к личным банковским счетам, а риск реального ущерба был сведен к минимуму, благодаря оперативному установлению и привлечению к ответственности источника инсайдерской информации, эта ситуация наглядно демонстрирует реальность угроз кибербезопасности.

По недавним оценкам органов государственного контроля Великобритании затраты на борьбу с киберпреступностью обходятся стране ежегодно в сумме от 18 до 27 млрд. фунтов стерлингов. Такая ситуация в информационно-коммуникационной среде вынуждает правительства многих стран принимать активные контрмеры по защите государственных и частных интересов в киберпространстве, включая разработку нового законодательства в этой сфере.

Стратегии информационной безопасности и IP в России и за рубежом

Обеспечение информационной безопасности как принципиальный момент соблюдении национальных интересов Российской Федерации, как отмечается в Доктрине информационной безопасности Российской Федерации, подразумевает, в том числе, укрепление механизмов правового регулирования отношений в области охраны интеллектуальной собственности и создание условий для соблюдения установленных федеральным законодательством на доступ к конфиденциальной информации, а также противодействие угрозам информационной безопасности. Важная роль в обеспечении информационной безопасности России отводится определению приоритетных направлений и механизмов реализации государственной политики Российской Федерации в области международной информационной безопасности в целях противодействия основным угроз в этой области. Представляется исключительно актуальным и важным инициатива по разработке концепции стратегии кибербезопасности Российской Федерации, проект которой в настоящее время предложен к обсуждению в Совете Федерации Федерального Собрания РФ.

Российское законодательство устанавливает, что информация, являясь объектом публичных, гражданских или иных правовых отношений, может свободно использоваться и передаваться любым лицом, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения. Закрепив право на доступ к информации и определив общие требования о защите информации и ответственности за правонарушения в сфере информации, информационных технологий и защиты информации, Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации» определил правила ограничения доступа к информации в сети Интернет, включая распространение информации с нарушением исключительных прав на фильмы, в том числе кинофильмы, телефильмы. Законом также предусмотрен порядок ограничения доступа в информационно-коммуникационных сетях (включая Интернет) к информации, распространяемой с нарушением закона, в которой содержаться призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях.

Проблемы информационной безопасности выходят на первый план и в национальных стратегиях других стран. В частности, в феврале 2013 года Еврокомиссия утвердила Стратегию кибербезопасности в Европе (EU Cyber Security Strategy). Стратегия устанавливает общие минимальные требования к сетевой и информационной безопасности между государствами-членами; определяет согласованную линию на профилактику, обнаружение и смягчения последствий и механизмов киберугроз, а также предусматривает повышение уровня готовности и участия в общей стратегии частного бизнеса. Стратегия направлена на стимулирование спроса на высоко безопасные продукты информационно-коммуникационных технологий и их сертификацию путем создания платформы для выявления и разработки стандартов кибербезопасности, включая сферу «облачных» вычислений. Стратегия опирается

на ранее принятые акты в области защиты от киберинцедентов, в частности: Директиву об охране частной жизни в цифровом пространстве (E-Privacy Directive (2002/58/EC), требующей в целях управления рисками в киберсети от поставщиков электронных коммуникаций сообщать о значительных нарушениях безопасности или целостности сети; Директива о критической инфраструктуре (European Critical Infrastructures Directive (2008/114/EC), в целях безопасности обязывающая операторов сетевой инфраструктуры разрабатывать планы обеспечения безопасности, включая анализ рисков и противодействия для прерывания обслуживания или уничтожения сетевой инфраструктуры; Директива о защите данных (Data Protection Directive (95/46/EC), обязывающая обладателей соответствующих баз данных реализовывать соответствующие технические и организационные меры для защиты персональных данных.

Защите данных информационных систем посвящена специальная Директива Европарламента и Еврокомиссии от 12 августа 2013г. (Directive 2013/40/EU on attacks against information systems). В настоящее время новый проект правил о защи- те персональных данных (General Data Protection Regulation) обсуждается в Европейском парламенте. Она включает в себя новые обязательства, такие как обязательства назначить представителя данных в ЕС и уведомлять об утечке персональных данных. Одновременно со Стратегией предложен проект Директивы о кибербезопасности, на основе которой каждое государство-член Евросоюза должно принять свою собственную стратегию сетевой и информационной безопасности («NIS»).

В 2011 году Федеральным министерством внутренних дел Германии принята общенациональная Стратегия кибербезопасности, направленная на применение эффективных мер и выработке взаимодействия государственных органов, частных предприятий и общественности в сфере кибербезопасности. В стране также обсуждается проект Закона ФРГ об IT безопасности. С учетом разработанной Национальной стратегии кибербезопасности в Великобритании в настоящее время тестируется новая форма взаимодействия государства и частного бизнеса в сфере информационной безопасности - Партнерство по обмену информационной безопасности (Cybersecurity Information Sharing Partnership («CISP»). CISP призвана установить новую «защищенную среду» обмена и получения информации между государственными органами и частным бизнесом. Современное законодательство Великобритании уже обязывает всех операторов данных применять соответствующие технические и организационные меры против незаконной обработки данных, а в случаях серьезного нарушения информационной безопасности могут налагаться денежные штрафы в размере до £500 000. Кроме того, финансовые компании обязаны исполнять дополнительные нормативные требования, включая организацию систем и средств контроля соблюдения правил финансовых операций.

Особое значение придается кибербезопасности в США. Наряду с уже действующим законодательством указом Executive order) Президента США в феврале 2013 года определена государственная политика по повышению кибербезопасности критической инфраструктуры США. Жизненно важные для США системы и активы (физические или виртуальные), недееспособность или уничтожение которых будет иметь пагубные последствия для национальной и экономической безопасности страны или здоровья и безопасности ее граждан (критическая инфраструктура) и ее защита от киберугроз отнесены эти документом к сфере исключительных национальных интересов США. Национальная политика кибербезопасности США должна обеспечить повышение безопасности и устойчивости важнейших объектов инфраструктуры нации, поддержание киберусловий, способствующих эффективности, инновациям и экономическому процветанию, обеспечивать конфиденциальность в бизнесе и неприкосновенность частной жизни и гражданских свобод. Поставленные задачи планируется достичь в рамках партнерства с владельцами и операторами критической инфраструктуры, мерами улучшения обмена информацией по кибербезопасности и разработкой и внедрением

стандартов о рисках.

Выработка многими странами стратегий информационной безопасности тесно связана с национальными стратегиями развития интеллектуальной собственности. Так, в США в 2013 году принят очередной стратегический план стимулирования и защиты интеллектуальной собственности в 21 веке, который определяет ориентиры в борьбе правительства с контрафактной продукцией и интеллектуальным пиратством, пресечением нарушений прав IP в интернете; предусматривает повышение открытости правоприменительной политики и международных переговоров, а также улучшение взаимодействия государственных органов и всех заинтересованных сторон в области интеллектуальной собственности; акцентирует внимание авторов на применение доктрины добросовестного использования (fair use); предусматривает повышении эффективности взаимодействия федеральных, органов штатов и местных правоохранительных органов (включая выявление новых технологий защиты IP при пограничном и иных формах контроля); усиление защиты от угроз нарушения IP на иностранных интернет-сайтах и защиты доменов первого уровня в сочетании с поддержкой национальных предприятий на внешних рынках; предусматривает систематизацию действующего законодательства по IP.

В материалах к стратегическому плану отмечается, что информационная безопасность является необходимым условием инноваций. Инновационный процесс, посредством которого новые идеи генерируются и успешно внедряются на рынке, как предусматривает национальная стратегия, служит основной движущей силой экономического роста и национальной конкурентоспособности США. Подобно тому, как использование торговых марок американскими компаниями позволяет отличить их товары и услуги от конкурентов, предоставление дополнительной поддержки инновациям позволяет национальным компаниям захватить долю рынка, что способствует росту американской экономики. Поощрение и защита прав интеллектуальной собственности является жизненно важным для продвижения инноваций и составляет важный элемент свободного предпринимательства и рыночной системы. Патенты, товарные знаки и авторские права являются основным средством используется для установления прав собственности на изобретения и творческие идеи в их различных формах, обеспечивающих правовую основу для создания ощутимых выгод от инноваций для компаний, работников и потребителей. Без этих правовых рамок создатели интеллектуальной собственности, как правило, не могут воспользоваться экономическими плодами своей собственной работы, тем самым подрывая стимулы к осуществлению необходимых инвестиций в развитие Р. Более того, без защиты Р, новатор (изобретатель), вложивший время и деньги в разработку нового продукта или услуги (невозвратные издержки) всегда будет в невыгодном положении по сравнению с компанией, просто копирующей инновационный продукт и выводящей его на рынок, без необходимости окупить такие невозвратные издержки или выплачивать более высокую заработную плату разработчикам, обладающим творческими талантами и навыками. В результате преимущества от американских инноваций будут иметь тенденцию утекать за пределы США.

В стратегиях развития Р активизируется и Китай. Национальная стратегия интеллектуальной собственности, принятая в КНР в 2013 году на пятилетний период, определила несколько главных целей:

1. поощрение создания интеллектуальной собственности, т.е. повышение качества прав интеллектуальной собственности и инновационной эффективности, улучшение оценки патентов, товарных знаков, авторских прав, новых сортов растений и др., совершенствование системы оценки эффективности Р, поощрение создателей Р и переход от количества к качеству и значению ^ для модернизации;
2. усиление влияния Р в ключевых отраслях экономики через государственное

планирование использования ИС в стратегических новых отраслях промышленности с применением преференциальной экспертизы патентных заявок на изобретения в этих отраслях и новейших технологиях (в т.ч. энергосбережение и охрана окружающей среды, информационных технологий нового поколения, биологии, производства высококачественное оборудование, новой энергии, новых материалов, а также технологии, поддерживающие зеленый развития, такие как низкоуглеродистых технологий и ресурсосберегающих технологий);

3. содействие внедрению Р посредством укрепления ключевой роли в использовании ^ предприятиями и улучшение коммерциализации нового поколения прав ИС в коммуникационных технологиях, трансфера прав на технологии военного и гражданского назначения, улучшения менеджмента ИС, применения финансовых инструментов использования ИС (залог и кредит прав ИС), прав на лицензии, прав в уставных капиталах и других активов;
4. усиление защиты Р путем совершенствования законодательства и оценки эффективности защиты ИС, повышение эффектив ности судебной защиты прав интеллектуальной собственности и потенциала административного правоприменения, включая международные споры;
5. повышение эффективности управления ИС, включая информационные, сервисные и юридические и патентные услуги по продвижению патентов, товарных знаков, авторских прав, правовой оценке ИС;
6. развитие культуры обращения ИС.