КИБЕРБЕЗОПАСНОСТЬ И ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ Часть 3

Карцхия Александр Амиранович,
кандидат юридических наук, профессор

В части 3 цикла статей, посвященных вопросам кибербезопасности интеллектуальной собственности и защите прав на результаты интеллектуальной деятельности и приравненных к ним средств индивидуализации юридических лиц, товаров, работ и услуг в киберпространстве, рассматриваются особенности защиты коммерческой тайны и ноу-хау от киберугроз.

***Ключевые слова**: интеллектуальная собственность, защита интеллектуальной собственности, киберугрозы, информация и право, киберпространство, права на результаты интеллектуальной деятельности, промышленная собственность.*

CYBERSECURITY AND INTELLECTUAL PROPERTY Part 3

***Alexsandr Kartskhiya**, Ph.D. (Jur.Sci), Professor*

Part 3 of the series of articles is devoted to the problems of cybersecurity and the protection of the intellectual property rights to the results of intellectual activity and means of individualization of legal persons, goods, works and services in cyberspace. The article discusses the legal means of trade secrets and know-how protection against cyberthreats.

***Keywords**: intellectual property, intellectual property protection, cyberthreats, cyberspace, information and law, rights to the results of intellectual activity, industrial property.*

Роль правового института интеллектуальной собственности в сфере информационной и кибербезопасности был отмечен определяющим фактором - интеграции интеллектуальной собственности в глобальную информационно-коммуникационную среду и был рассмотрен в первых двух частях цикла статей. Механизм охраны интеллектуальной собственности и защиты прав интеллектуальной собственности становится составной частью общей системы информационной безопасности в киберпространстве.

События последних месяцев, связанные с политическим кризисом вокруг Украины, наглядно показали критическую значимость систем информационной безопасности в киберпространстве (кибербезопасности). В условиях высокой динамики развития ситуации и связанным с этим информационным фоном актуализировались вопросы по защите прав интеллектуальной собственности, обеспечением публичных (национальных) и частных (коммерческих) интересов правообладателей. На первый план выходит задача создания эффективной защиты интеллектуальной собственности в киберпространстве и обеспечение сохранности государственной, служебной и коммерческой тайны в глобальной информационно-коммуникационной среде.

Не менее важно укрепление международного сотрудничества в сфере кибербезопасности, которое устанавливается на двусторонней основе между Россией и другими государствами. Создание более эффективной информационной модели интернета, которая могла гарантировать национальный суверенитет, безопасность и соблюдение норм российского права, а также принципов международного права в сочетании с соблюдением принципа неприкосновенности

частной жизни, имеет саму непосредственную связь с эффективностью защиты интеллектуальной собственности в киберпространстве.

Информация в сети Интернет – ответственность и безопасность

Эффективному решению проблем безопасности, законности и доступности информации в Интернете способствует активизация законотворческой деятельности по защите прав интеллектуальной собственности в Интернете. Принятый в 2013 году Федеральный закон об усилении защиты интеллектуальных прав правообладателей в сети Интернет[1] (так называемый «антипиратский закон») предусматривает возможность ограничивать доступ к ресурсам информационно-коммуникационных сетей (включая Интернет) по заявлению правообладателя на основании решения Московского городского суда в случае размещения в этих сетях аудиовизуальных произведений (кинофильмов, телефильмов и др.) с нарушением исключительных прав правообладателей.

Помимо этого, в Гражданский кодекс РФ введена специальная статья 1253.1 об ответственности информационного посредника, в качестве которого выступает лицо, осуществляющее передачу материала в информационно- телекоммуникационной сети (включая сеть «Интернет»), либо лицо, предоставляющее возможность размещения материала или информации, необходимой для его получения с использованием информационно-телекоммуникационной сети, либо лицо, предоставляющее возможность доступа к материалу в этой сети. Предусмотренные этой статьей правила применяются в отношении лиц, предоставляющих возможность доступа к материалу или информации, необходимой для его получения с использованием информационно-телекоммуникационной сети.

Информационный посредник несет ответственность за нарушение интеллектуальных прав в информационно-телекоммуникационной сети на общих основаниях, предусмотренных Гражданским кодексом РФ, при наличии вины и с учетом особенностей, предусмотренных законом.

Вместе с тем, информационный посредник (например, интернет-провайдер), осуществляющий передачу материала или предоставляющий возможность его размещения в информационно-телекоммуникационной сети, освобождается от ответственности за нарушение интеллектуальных прав при соблюдении ряда предусмотренных законом условий, в частности: если он не знал и не должен был знать, что использование соответствующего результата интеллектуальной деятельности или средства индивидуализации, содержащихся в размещаемом материале, является неправомерным и др.

При этом, даже если информационный посредник не несет в указанных случаях ответственность за нарушение интеллектуальных прав, к нему могут быть предъявлены требования о защите интеллектуальных прав (п. 1 ст. 1250, п. 1 ст. 1251, п. 1 ст. 1252 Гражданского кодекса РФ), не связанные с применением мер гражданско-правовой ответственности, в том числе об удалении информации, нарушающей исключительные права, или об ограничении доступа к ней. Закон также предусматривает возможность принятия судом обеспечительных мер.

В правовом механизме защиты прав интеллектуальной собственности в Интернете участвует уполномоченный государственный орган – Роскомнадзор[2], который осуществляет контрольные функции в сфере информационных технологий. На него возложены обязанности по взаимодействию с интернет-провайдерами. В настоящее время Роскомнадзор на основании решений Мосгорсуда о прекращении доступа и удалении контента в Интернете, нарушающего авторские права на кино и видеофильмы, выносит соответствующие предписания. Ответственность по закону несут владельцы незаконно размещенных кино и видеофильмов, но не пользователи. Правообладатели уже активно используют новую возможность защиты своих прав, представляя в Роскомнадзор решения Мосгорсуда о приостановлении размещения незаконного контента на сайтах хостинг-провайдеров.

---

1 Федеральный закон от 02.07.2013 N 187-ФЗ “О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях”. Официальный интернет-портал правовой информации http://www.pravo.gov.ru, (03.07.2013).

2 Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) Публичный доклад 2012. М, 2013. http://www.rsoc.ru/docs/pd2012.pdf

Применение законодательных норм о правах интеллектуальной собственности в новой сфере – в сети Интернет- неизбежно влечет необходимость правового определения понятий, которые используются в глобальной сети. Не всегда они устанавливаются в законе, как это было сделано в отношении интернет-посредника (интернет-провайдера). Понятие «доменное имя» упоминается законом в связи с охраной интеллектуальной собственности как способ адресации (ст. 1484, 1519 ГК РФ), при регистрации и использовании которого необходимо избегать нарушения исключительных прав других правообладателей на товарные знаки или наименования места происхождения товара.

Разъясняя понятие «контент», Президиум ВАС РФ в Постановлении от 22.04.2008 №255/08 по делу №А63-14046/2006-С1 указал, что «сайт… состоит из специально подобранных и расположенных определенным образом материалов (текстов, рисунков, фотографий, чертежей, аудиовизуальных произведений и т.д.), которые могут быть использованы с помощью компьютерной программы (компьютерного кода), являющейся элементом сайта. Эта комбинация, по выражению специалистов в области программирования, является контентом сайта». К элементам контента в этом постановлении отнесен и «дизайн сайта» в целом. При этом, ввиду отсутствия единства судебной практики, контент сайта может рассматриваться как совокупность отдельных самостоятельных авторских произведений и иных объектов, либо как единое составное авторское произведение, состоящее из системы взаимосвязанных элементов.

Для формирующейся правоприменительной практики в сфере информационно-коммуникационных технологий помимо закона важное значение имеют правовые позиции и разъяснения Конституционного Суда РФ как судебного органа конституционного контроля, решения которого обязательны как для всех граждан и юридических лиц, так и для судов и органов государственной власти. Принципиально важной в этой связи является позиция Конституционного Суда РФ о защите прав интеллектуальной собственности и ответственности за их нарушение в сети Интернет, которая изложена в Постановлении Конституционного Суда РФ от 09.07.2013 N 18-П[3]. В нём Конституционный Суд РФ указал, что «информация, распространяемая посредством сети «Интернет», размещается на сайтах, ресурсы которых, как правило, технически и технологически объективно доступны неопределенному кругу лиц, что не исключает возможность их анонимного использования, в том числе в противоправных целях, например для распространения сведений, порочащих честь, достоинство или деловую репутацию граждан.

Тот факт, что противоправные действия с применением ресурсов сети «Интернет» совершены неизвестным лицом, не отменяет общего принципа, в силу которого ответственность за эти действия несет именно правонарушитель. Однако, даже фактическая невозможность в подобных случаях установить и привлечь к ответственности виновное лицо, равно как и отсутствие правовых оснований для привлечения к ответственности владельца соответствующего сайта, не являющегося средством массовой информации, или иного уполномоченного им на размещение информации лица, в качестве способа защиты прав потерпевшего не означает, что эти права не подлежат защите иными способами, такими как восстановление положения, существовавшего до нарушения права, и пресечение действий, нарушающих право или создающих угрозу его нарушения (статья 12 ГК Российской Федерации).»

Следует также учесть то, что Уголовный кодекс РФ (ст.272-274 УК РФ) в настоящее время предусматривает уголовную ответственность за неправомерный доступ к охраняемой законом компьютерной информации (не только ЭВМ или их сети), за создание, распространение или использование вредоносных компьютерных программ, а также за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации (информационно-телекоммуникационных сетей).

В международной практике стремления максимально усилить позиции правообладателей интеллектуальной собственности, ввести максимально жесткие меры ответственности (включая ужесточение уголовного наказания) за нарушение авторских и иных прав, ужесточить контроль за соблюдением этих прав с использованием принципа экстерриториальности встречает, как правило, неприятие общественности, пользователей и профессиональных участников рынка Интернет-услуг.

3 См.: п. 4 Постановление Конституционного Суда РФ от 09.07.2013 N 18-П. Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 11.07.2013)

Примером могут служить два широко комментируемых законопроекта, которые вызвали волну активных протестов в США. Первый проект «антипиратского» закона Stop Online Piracy Act (SOPA) 2011 года, который обязывал интернет-провайдеров, хостинг-провайдеров и поисковые системы по первому запросу правообладателя не только полностью блокировать сайты, нарушающие авторские права, но и предоставляет возможность расторгать рекламные контракты, вводить ограничения платежных систем в Интернете, а также устанавливает суровую уголовную ответственность за нарушения авторских прав в сети Интернет.

Второй законопроект - Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011(известен как Protect Intellectual Property Act или PIPA) - направлен на борьбу с реальными сетевыми угрозами экономическому творческому потенциалу и кражам интеллектуальной собственности и значительно расширяет возможности правообладателей авторских прав блокировать сайты в сети Интернет, нарушающие авторские права и предлагающие к продаже контрафактные товары. Особенность этого акта в том, что он расширяет юрисдикцию правоохранительных органов и судов США в отношении интернет-ресурсов (сайтов), зарегистрированных за пределами США. В результате протестов дальнейшее принятие и обсуждение этих законопроектов было остановлено, но отдельные их положения предлагается реанимировать при более детальном анализе и взвешенном подходе к решению вопросов защиты прав интеллектуальной собственности в Интернете[4].

Защита коммерческой тайны и ноу-хау от киберугроз: российский и зарубежный опыт

Одной из сторон информационной безопасности наряду с защитой авторских и патентных прав является сохранение коммерческой тайны, сведений о передовых технологиях и инновациях, иных секретах производства, имеющих коммерческую ценность. Этой сфере защиты информации в последние годы уделяется более пристальное внимание в законодательной и правоприменительной практике многих стран. В большинстве европейских государств ноу-хау не рассматривается как объект интеллектуальной собственности. Защита секретов производства (ноу-хау) может осуществляться на основе норм о недобросовестной конкуренции (Германия) или отдельного закона (Швеция), либо иным способом. В странах общего права (Великобритания, США, Ирландия) защита ноу-хау осуществляется на основе норм общего права. В Российской Федерации секреты производства (ноу-хау) являются объектом интеллектуальной собственности, исключительное право на который защищается гражданско-правовыми способами.

В Российской Федерации секретом производства (ноу-хау) в соответствии с новой редакцией ст.1465 ГК РФ признаются сведения любого характера (производственные, технические, экономические, организационные и другие) о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности, имеющие действительную или потенциальную коммерческую ценность. Как устанавливает закон, коммерческая ценность сведений, составляющих секрет производства (ноу-хау), обусловливается неизвестностью этих сведений третьим лицам, если к таким сведениям у третьих лиц нет свободного доступа на законном основании и обладатель таких сведений принимает разумные меры для соблюдения их конфиденциальности, в том числе путем введения режима коммерческой тайны. К секретам производства не относятся сведения, обязательность раскрытия которых либо недопустимость ограничения доступа к которым установлена законом или иным правовым актом.

Обладатель секрета производства (ноу-хау) наделяется исключительным правом использования таких секретов любым не противоречащим закону способом, в том числе при изготовлении изделий и реализации экономических и организационных решений, а также может распоряжаться указанным исключительным правом, заключая лицензионные договоры и договоры отчуждения секрета производства или иным образом. Лицо, ставшее добросовестно и независимо от других обладателей секрета производства обладателем сведений, составляющих содержание охраняемого секрета произ-

4 The Department of Commerce. Internet Policy Task Force. July 2013. Report: Copyright Policy, Creativity and Innovation in the Digital Economy. http://www.uspto.gov/news/publications/copyrightgreenpaper.pdf

водства, приобретает самостоятельное исключительное право на этот секрет производства (ст.1466 ГК РФ).

Непосредственно сам режим коммерческой тайны (включая меры по охране конфиденциальности информации), перечень не подлежащих охране сведений и порядок предоставления составляющей коммерческую тайну информации определяются в соответствии с Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (в ред. 12.03.2014г.) (далее – Федеральный закон «О коммерческой тайне»). Коммерческая тайна определяется этим законом как «режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду», а к информации, составляющей коммерческую тайну отнесены «сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны».

Обладатель таких сведений вправе самостоятельно относить их к информации, составляющей коммерческую тайну, и определять в соответствии с законом перечень и состава такой информации. Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом. Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания (ст.4 Федерального закона «О коммерческой тайне»).

До тех пор, пока сохраняется конфиденциальность сведений, составляющих содержание секрета производства, действует и исключительное право на него. С момента утраты конфиденциальности соответствующих сведений исключительное право на секрет производства прекращается у всех правообладателей (ст.1467 ГК РФ).

Режим коммерческой тайны не может быть установлен в отношении ряда сведений, в том числе: содержащихся в учредительных документах юридического лица и в документах, дающих право на осуществление предпринимательской деятельности; о численности, о составе работников, о системе оплаты труда, об условиях труда; о задолженности работодателей по выплате заработной платы и по иным социальным выплатам; о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений; обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

К ответственности за нарушение исключительного права на секрет производства (ст.1472 ГК РФ) может быть привлечено любое лицо, разгласившее сведения, составляющие секрет производства (или допустившее иные нарушения исключительного права), в том числе публично-правовое образование (Российская Федерация, субъект Российской Федерации, муниципальное образование), если его орган, получивший доступ к соответствующей информации, такую информацию разгласил (ст.14 Федерального закона «О коммерческой тайне»).

Законодательство европейских стран по защите коммерческой тайны (trade secrets) отличается значительным разнообразием. В связи с этим в ноябре 2013 года в Европарламент был представлен на обсуждение проект Директивы ЕС о защите ноу-хау и бизнес информации (коммерческой тайны)[5], призваный гармонизировать законодательство о коммер-

5 EU Directive2013/0402 (COD) on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

ческой тайне во всех странах ЕС, на базе уже имеющееся национального законодательства, и создать минимальный уровень защиты для коммерческой тайны по всей Европе для поощрения инноваций и инвестиций в европейский бизнес на равной конкурентной основе с предприятиями за пределами Европы.

Проект запрещает «незаконное приобретение, разглашение и использование коммерческой тайны» и водит единое понятие «коммерческая тайна», которое в настоящее время различно в праве европейских стран. Предусмотрен двухлетний срок исковой давности по требованиям о защите, что намного короче действующих сроков исковой давности в большинстве государств-членов ЕС. Установлен общий набор средств правовой защиты, при незаконном приобретении, разглашении или использовании коммерческой тайны. К ним относятся временные и постоянные судебные запреты, арест и уничтожение товаров, которые являются результатом неправомерного использования коммерческой тайны, возмещение понесенного ущерба владельцу коммерческой тайны. Предусматриваются процедуры обеспечения конфиденциальности коммерческой тайны в ходе судебного разбирательства.

Не смотря на то, что Директива не содержит каких-либо новых правовых средств усиления защиты прав обладателей торговых секретов (например, право принудить ответчика предъявить документы для получения доказательств злоупотреблений), минимальный уровень защиты для торговых секретов по всему ЕС облегчит трансграничные операции и запретит злоупотребления конфиденциальной информацией мобильными работниками в юрисдикциях, где коммерческая тайна обычно не защищена.

В юридической терминологии информация, которая является конфиденциальной и используемой для поддержания конкурентоспособности и получения прибыли, называется «коммерческая тайна» (trade secrets), «нераскрытая информация» (undisclosed information), «конфиденциальная бизнес информация « (business confidential information) или «секретное ноу-хау» («secret know-how»). На практике также используются такие понятия как («фирменное ноу-хау» или « фирменная технология « («proprietary technology»).

Коммерческие секреты не менее важны в защите инноваций в сфере услуг, общий объем которых составляет примерно 70% ВВП Евросоюза. Конфиденциальность в этой ключевой части экономики ЕС применяется для использования так называемых «мягких инноваций» («soft innovation»), охватывающих использование и применение разнообразного набора стратегической коммерческой информации, которая выходит за рамки технического знания, например: информация о клиентах и поставщиках, о построении бизнес-процессов, о бизнес-планах, маркетинговых исследованиях и стратегиях и др.

Несмотря на то, что развитие и управление знаниями и информацией становятся все более важны для экономики ЕС, раскрытие ценных технологий (know-how) и информации (trade secrets) посредством кражи, шпионажа или других методов незаконного присвоения существует и продолжает увеличиваться в силу факторов глобализации, использования аутсорсинга, удлинения цепочки поставок товаров, более широкое использование информационно-коммуникационных технологий и т.д.). Поэтому предложено унифицированное определение термина «trade secret», которое охватывает бизнес-информацию, технической информацию и ноу-хау, представляющую интерес для содержания в коммерческой тайне.

В соответствии с законодательством европейских стран владелец коммерческой тайны не обладает исключительным правом на информацию, охватываемую коммерческой тайной. Допускается самостоятельное получение одного и того же ноу-хау или информации независимо несколькими лицами. Конкуренты владельца коммерческой тайны (коммерческих секретов) также могут свободно получить доступ к таким секретам путём обратного инжиниринга (reverse engineer) любой законно приобретенной продукции.

В случае незаконного приобретения, использования или раскрытия коммерческих секретов лицом, которое знало или имел достаточных оснований знать о неправомерности своих действий, обязано возместить ущерб, понесенный обладателем коммерческих секретов. В сумме убытков, присуждаемых потерпевшему обладателю, подлежит учёту все соответствующие факторы, такие как потери дохода владельцем коммерческой тайны, или получение необо-

снованной прибыли правонарушителем от неправомерного её использования, а также любой моральный ущерб, причиненный владельцу коммерческой тайны.

В США действует несколько федеральных законов, обеспечивающих защиту коммерческой тайны (trade secrets). В феврале 2013 года одобрена Стратегия Администрации США по противодействию краже коммерческих секретов (далее -Стратегия) [1]. Согласно законодательству США, коммерческие секреты (trade secrets) включают коммерчески ценную информацию, которая не является общеизвестной или закрыта для беспрепятственного доступа к ней при соблюдении обладателем информации разумных мер для поддержания её конфиденциальности. Защита коммерческой тайны в США в первую очередь осуществляется законами штатов, принятых на основе федерального закона Uniform Trade Secrets Act (UTSA) 1980 года, который определяет, что коммерческие секреты (trade secrets) означают информацию (в т.ч., формулу, модель, компиляцию, программное устройство, способ, метод или процесс, которые обладают независимой экономической ценностью (фактической или потенциальной), которые, как правило, не известны другим лицам и не могут быть получены правомерными способами, и в отношении которых поддерживается разумный режим секретности.

Судебная практика относит к коммерческим секретам техническую и не техническую информацию, в том числе: формулы, рецепты, списки клиентов, бизнес ноу-хау, информацию о бизнес-операциях (например, ценообразование, разработка продукта, бизнес-цели, маркетинговые стратегии), или технологии производства и чертежи. Не подлежат защите общедоступная информация, например рецепты блюд, метод приготовления еды для барбекю, или списки клиентов, опубликованные на вебсайте компании.

В настоящее время федеральный Закон США об экономическом шпионаже 2012 года (Economic Espionage Act, 2012) усилил уголовную ответственность за некоторые формы кражи коммерческой тайны. Экономический шпионаж связан с умышленной кражей или присвоением коммерческой тайны в целях извлечения выгоды любым иностранным правительством, иностранной организацией, или иностранным агентом. Законом предусмотрена ответственность за кражу или присвоение коммерческих секретов в экономических интересах любого лица (исключая владельца этих секретов). Закон применяется к нарушениям коммерческой тайны, совершенным как внутри страны, так и за пределами США (в отношении американских резидентов). Кража или присвоение коммерческой тайны квалифицируется при незаконном использовании коммерческих секретов, которые связаны, содержаться или включены в продукт, который производится или предлагается к продаже во внутренней и внешней торговле.

Важное место в правоприменительной практике судов США также занимает доктрина о неизбежном раскрытии (doctrine of inevitable disclosure) коммерческой информации гражданского назначения. Доктрина допускает, что работник, который обладает коммерческими секретами в силу своих трудовых функций, при смене места работы может «неизбежно» раскрывать коммерческую тайну конкурентам.

В отличие от других прав интеллектуальной собственности защита законом прав коммерческих секретов за рубежом предоставляется при условии принятия мер владельцем по сохранению в тайне эти сведений (информации), а ответственность за воровство секретов не может наступить при отсутствии разумных усилий и специальных мер по поддержанию режима секретности (конфиденциальности). Наличие режима конфиденциальности часто является ключевым вопросом при предоставлении судебной защиты коммерческой тайны, что особенно важно в условиях современного цифрового пространства. Правовая защита при нарушении прав обладателя коммерческой тайны предоставляется на основе норм о недобросовестной конкуренции («passing-off»), либо на основе правил о причинении ущерба (деликта) («tort»).

Достаточно показательным является отмеченный в Стратегии США тот факт, что технологии, которые сделали возможной информационно-цифровую революцию, сами стали представлять значительные угрозы, в том числе, для защиты интеллектуальной собственности и коммерческой тайны. Новейшие достижения в области технологии, повышение мобильности, глобализация, и анонимная природа Интернета создают растущие проблемы в области защиты коммер-

ческой тайны. Те же технологии, которые были катализатором экономического роста для бизнеса и экономики в целом, создали новую информационную среду, требующую повышения степени защиты их жизненно важных активов. Судебная практика в США исходят из того, что публикация коммерческой тайны в Интернете приводит к потере секретного статуса информации, что делает претензии о защите секретов не имеющими законной силы.

Особую озабоченность у США, как указано в Стратегии, вызывают угрозы бизнесу от экономического шпионажа, скоординированного иностранными правительствами. В отличие от промышленного шпионажа эти действия не только могут лишить американские компании ценной информации и секретов (часто в пользу иностранных конкурентов), но и составить серьезный вызов в противодействию ресурсам иностранной разведки. В Стратегии приводятся конкретные случаи экономического шпионажа в пользу иностранных конкурентов или иностранных государств.

Современные реалии убедительно показывают, что новейшие технологии облегчают хранение, доступ, распространение и обнародование конфиденциальной информации, тем самым значительно повышая вероятность раскрытия коммерческой, частной или государственной тайны.

В целом, с точки зрения автора настоящей статьи, механизм правовой защиты секретов производства (ноу-хау), коммерческих секретов, иной ценной информации (сведений), в том числе, в цифровой среде Интернет, направлен на обеспечение надлежащего функционирования критически важной инфраструктуры государства, сохранение конфиденциальности сведений (информации) в интересах правообладателей интеллектуальной собственности, а в целом ряде случаев – на обеспечение безопасности государства и его граждан.

Литература:

1. Joint Strategic Plan on Intellectual Property Enforcement 2013. www.uspto.gov/web/offices/com/strat21/index.htm.

References:

1. Joint Strategic Plan on Intellectual Property Enforcement 2013. www.uspto.gov/web/offices/com/strat21/index.htm.