# КИБЕРБЕЗОПАСНОСТЬ И ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ Часть 2

***Карцхия Александр Амиранович**, кандидат юридических наук, профессор*

*В части 2 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, рассматривается значение интеллектуальной собственности в структуре кибербезопасности, а также особенности защиты прав интеллектуальной собственности от киберугроз.*

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

# CYBERSECURITY AND INTELLECTUAL PROPERTY Part 2

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

*In part 2 of the series of articles devoted to the problems of cybersecurity and the protection of intellectual property rights to the results of intellectual activity and means of individualization of legal persons, goods, works and services in cyberspace, as well as discusses the importance of intellectual property in the structure of cybersecurity, especially intellectual property rights protection against cyberthreats.*

***Keywords**: intellectual property, intellectual property protection against cyberthreats, rights to the results of intellectual activity, industrial property.*

Интенсификация процесса мировой глобализации в значительной степени порождается развитием информационно-коммуникационных технологий и Интернета, которые в свою очередь стали основным инструментом глобальной коммуникации. Сфера интеллектуальной собственности оказалась глубоко интегрирована в глобальные процессы, которые выявили новые риски и поставили новые вопросы, связанные с защитой прав интеллектуальной собственности, обеспечением публичных (национальных) и частных (коммерческих) интересов правообладателей, созданием эффективной защиты интеллектуальной собственности в киберпространстве, сохранности государственной, служебной и коммерческой тайны.

Современные инновации, связанные с бурным развитием информационно-коммуникационных технологий, интернета, генной инженерии, биотехнологий и фармацевтики стимулируют появление новых концептуальных подходов в вопросах интеллектуальной собственности. Приобретают особую актуальность проблемы эффективности охраны интеллектуальной собственности и защиты интеллектуальных прав, а также совершенствования правового режима охраны инноваций (изобретений и других патентоспособных объектов, авторских произведений, программ для ЭВМ и др.) при условии соблюдения рационального баланса интересов правообладателей и общества, доступности результатов новых разработок и технических решений в интересах научно-технического, социального и общекультурного развития общества [1].

Анализ концептуальных подходов и национальных стратегий развития интеллектуальной собственности в России и зарубежных странах, а также целенаправленность стратегий кибербезопасности позволяют сделать определенные вывод. Учитывая возрастающее соперничество стран в глобальной экономике и усиление конкуренции на всех уровнях, России необходимо

иметь собственную стратегию кибербезопасности, определяющую приоритеты государственной политики в этой области на ближайшую перспективу и место страны в глобальном информационном пространстве. Среди основных вопросов этот документ должен определять направления государственной политики в отношении охраны интеллектуальной собственности, использовании инструментов поощрения и защиты прав интеллектуальной собственности в целях безопасности информационно-коммуникационной среды, включая защиту интересов российских правообладателей за рубежом в глобальной информационно-коммуникационной среде. В этом отношении важно поддержать инициативу по разработке концепции стратегии кибербезопасности Российской Федерации с учетом опыта разработки проекта федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», который предусматривал организационные и правовые основы обеспечения безопасности критической информационной инфраструктуры России.

*Интеллектуальная собственность в структуре кибербезопасности*

Правовой институт интеллектуальной собственности занимает одно из ключевых мест в законодательстве России. Результаты интеллектуальной деятельности и средства индивидуализации товаров, работ, услуг и юридических лиц, которым в силу закона предоставляется правовая охрана и которые определяются как интеллектуальная собственность в ст.1225 Гражданского кодекса РФ, представляют собой нематериальные активы, обладающие материальной, товарной стоимостью. Патенты на изобретения, полезные модели промышленные образцы, товарные знаки, программы для ЭВМ и авторские произведения, секреты производства (ноу-хау) и другие интеллектуальные нематериальные активы, содержащие новаторские технические и гуманитарные знания и умения, в условиях глобальных рыночных отношений приобретают особую ценность для их правообладателей.

Информация (сведения) о характере и содержании новаторских достижений имеет важнейшее значение в современной высоко конкурентной среде. Независимо от того, является ли содержание таких нематериальных активов доступным неограниченному кругу лиц (описание изобретения в патенте, условное обозначение как товарный знак, обнародованное авторское произведение), или сведения о передовых разработках и технологиях «скрыты» коммерческой тайной (ноу-хау) или охраняются государственной тайной, закон предоставляет защиту прав на такие нематериальные активы их правообладателям. Использование же патентов, товарных знаков, программ для ЭВМ и других объектов интеллектуальной собственности в гражданском, товарном обороте допускается с соблюдением исключительного права его законного обладателя. Формы такого использования очень разнообразны и включают как непосредственной применение, так и использование результатов интеллектуальной деятельности и средств индивидуализации в товарах, выводимых на рынки или иным образом включаемых в гражданский оборот.

Кибербезопасность, т.е. безопасность в сфере глобального Интернета и других цифровых информационно-коммуникационных сетях, тесно связана с решением задач и достижением целей, поставленных в Доктрине информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 N Пр-1895) (далее -Доктрина). Те виды угроз, которые обозначены в Доктрине, в большинстве своем могут быть отнесены и к угрозам в сфере кибербезопасности с учетом особенностей киберпространства. При этом, следует учесть, что в число основных объектов обеспечения информационной безопасности Российской Федерации в сфере духовной жизни Доктриной включены и объекты интеллектуальной собственности.

В предложенном в начале 2014 года Проекте Стратегии кибербезопасности Российской Федерации (далее – Стратегия), содержаться ряд терминологических определений, включая следующие: «информационная безопасность» -состояние защищенности личности, организации и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве; «киберпространство» -сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства); «кибербезопасность» – совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.

С точки зрения автора настоящей статьи Стра-

тегия также должна включать положения об эффективной защите передовых научно-технических достижений и авторских разработок с позиции применения и совершенствования правового механизма защиты прав интеллектуальной собственности (прав на результаты интеллектуальной деятельности). Совершенствование этого механизма должно преследовать цель максимальной защите интересов правообладателей, также как и соблюдение баланса публичного (общественного) интереса и частного интереса правообладателей в отношении охраняемых законом результатов интеллектуальной деятельности (изобретения, промышленные образцы, программы для ЭВМ и базы данных, селекционные достижения, секреты производства (ноу-хау), передовые авторские научно-технические разработки и др.), которые могут обладать как большой интеллектуальной значимостью, так и высокой коммерческой ценностью.

В этом аспекте под кибербезопасностью возможно понимать готовность к защите интересов правообладателей интеллектуальной собственности от имеющихся и потенциальных киберугроз.

*Киберугрозы и права интеллектуальной собственности*

Киберугрозы в отношении интеллектуальной собственности связаны с риском нарушения интеллектуальных прав на объекты интеллектуальной собственности. Риск, как определенная вероятность наступления неблагоприятных последствий, выражается применительно к интеллектуальной собственности в возможности (с той или иной степенью вероятности) нарушения интеллектуальных прав (прежде всего, исключительного права). Нарушение прав интеллектуальной собственности заключается в неправомерном использовании результата интеллектуальной деятельности или средства индивидуализации, влекущее причинение ущерба правообладателю в форме неполученного дохода или репутационных (имиджевых) потерь. Нарушение прав интеллектуальной собственности может выражаться в непосредственном использовании, к примеру, запатентованных технических решений при производстве продукта или с использованием запатентованного способа. Косвенное нарушение прав интеллектуальной собственности происходит при импорте или ином введении в гражданский оборот контрафактной продукции (товаров).

Эффективность защиты прав интеллектуальной собственности в цифровом пространстве Интернета определяется возможностью противостоять таким нарушениям и угрозам их наступления. Угрозы нарушения прав интеллектуальной собственности в киберпространстве (киберугрозы) связаны с определенными рисками и могут оказывать влияние на само существование объекта интеллектуальных прав. В частности, в результате кибератак могут быть изменены или полностью утрачены базы данных, содержащих определенную коммерчески ценную информацию, либо могут быть разглашены сведения, содержащие коммерческую тайну, что влечет утрату конфиденциальности и прекращение права на секреты производства (ноу-хау) в соответствии со ст. 1467 ГК РФ.

Киберугрозы нарушения прав интеллектуальной собственности в сфере цифрового пространства Интернет, имеют свою специфику. В частности, к видам нарушений прав интеллектуальной собственности в киберпространстве с использованием электронно-цифровых средств можно отнести:

- незаконный доступ, получение и раскрытие сведений, составляющих коммерческие секреты (ноу-хау) служебную или государственную тайну, включая преднамеренные действия («хакерские атаки»);

- несанкционированное вмешательство в базы данных, создание и применение компьютерных программных средств для изменения или блокировки сведений в составе баз данных и иной цифровой информации (сведений);

- распространение в сети Интернет ложной (недостоверной) информации о физическом или юридическом лице либо иное нарушение права на частную жизнь или ущемление деловой репутации;;

- нарушение права авторства и иных авторских и смежных прав на авторские произведения в киберпространстве;

- незаконное использование товарных знаков, наименований юридических лиц и других средств индивидуализации, включая незаконное использование обозначений в доменных именах или в контентах web-сайтов;

- преднамеренное незаконное использование средств индивидуализации (коммерческих обозначений, фи рменных наименований, товарных знаков, географических обозначений) для нанесения прямого или косвенного ущерба правообладателю.

Следует при этом иметь в виду, что в силу закона правообладателем патентов, товарных зна-

ков, ноу-хау, топологий интегральных микросхем, программ ЭВМ, авторских произведений и иных объектов интеллектуальной собственности могут быть как частные лица и организации, так и Российская Федерация, субъекты РФ и муниципальные образования. В связи с этим, защита интеллектуальной собственности от киберугроз, обеспечивается не только в отношении правообладателей, обладающих различным правовым статусом, но подразделяется в зависимости от уровня защиты. Каждый уровень защиты может иметь свой правовой режим защиты, который должен обеспечивать необходимую защиту интересов правообладателя интеллектуальной собственности.

В частности, особые режимы защиты интеллектуальной собственности от киберугроз предполагает установление режима государственной тайны, а также служебной или коммерческой тайны, которые основаны на нормах федеральных законов: Закон РФ от 21.07.1993 №5485-1 (в ред. от 21.12.2013) «О государственной тайне», Федеральный закон от 29.07.2004 №98-ФЗ (ред. от 11.07.2011г.) «О коммерческой тайне». Сохранение коммерческой, служебной и иной охраняемой законом тайны предусмотрено и другими законами, в частности: ст.9 Федерального закона от 27.07.2006 №149-ФЗ (в ред. от 28.12.2013) «Об информации, информационных технологиях и о защите информации», ст.26 Федерального закона от 26.07.2006 №135-ФЗ (ред. от 28.12.2013) «О защите конкуренции» и др.

Защита сведений об охраняемых результатах интеллектуальной деятельности, составляющих государственную или коммерческую тайну, в специальном правовом режиме предусматривается также нормами части 4 Гражданского кодекса РФ. К таким охраняемым объектам прав интеллектуальной собственности относятся, в частности, программы для ЭВМ и базы данных, в которых содержатся сведения, составляющие государственную тайну (ст.1262 ГК РФ); секретные изобретения (ст. 1349 ГК РФ) и промышленные образцы (1390 ГК РФ), содержащие сведения, составляющие государственную тайну; топологии интегральных микросхем, содержащие сведения, составляющие государственную тайну (ст.1452 ГК РФ), а также охрана секретов производства (ноу-хау), основанный на введении режима конфиденциальности, включая режим коммерческой тайны (ст. 1465 ГК РФ).

Специальный правовой режим установлен для защиты персональных данных в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ (ред. от 23.07.2013) «О персональных данных» и постановлением Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и изданным в его исполнение приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 18.02.2013г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

*Интеллектуальная собственность и новые угрозы в киберпространстве*

Задачи повышения эффективности защиты интеллектуальной собственности от новых киберугроз связаны с расширением разнообразия самих объектов ИС. Проблемы защиты доменных имен различного уровня и товарных знаков, глобализация интернет-торговли и иных услуг в сети Интернет (включая электронную биржу интеллектуальной собственности) и связанный с этим оборот контрафактной продукции, распространение «виртуальных» денег и интернет-валют, расширение возможностей 3D-принтинга, существенной повышение требований к кибербезопасности персональных данных и информационных баз данных, защита авторских прав и прав личности в интернете (включая право авторства, право на «личный имидж» или «личные бренды») - эти и другие новые факторы влекут за собой необходимость совершенствования механизма защиты в киберпространстве. Новые вызовы времени требуют новых подходов и адекватных ответов.

Современное законодательство пополняется новыми законодательными нормами, повышающими эффективность защиты интеллектуальной собственности в киберпространстве. В конце 2013 года в Гражданский кодекс РФ введены нормы об ответственности интернет-операторов (информационных посредников), которые обязаны соблюдать права обладателей интеллектуальной собственности и теперь несут самостоятельную ответственность за нарушение этих прав (ст.1253.1 ГК РФ). Информационный посредник, осуществляющий передачу материала в информационно-телекоммуникационной сети, несет ответственность за нарушение интеллектуальных прав в информационно-телекоммуникационной сети на общих основаниях, предусмотренных Гражданским кодексом РФ при наличии вины с учетом некоторых особенностей.

К информационному посреднику в судебном порядке могут быть предъявлены требования о защите интеллектуальных прав, не связанные с применением мер гражданско-правовой ответственности, в том числе об удалении информации, нарушающей исключительные права, или об ограничении доступа к ней.

Кроме того, эти правила об ответственности применяются в отношении лиц, предоставляющих возможность доступа к материалу или информации, необходимой для его получения с использованием информационно-телекоммуникационной сети. В частности, правонарушителю суд может запретить размещать информацию, необходимую для получения с использованием сети «Интернет» видеофильмов на сайте информационно-телекоммуникационной сети «Интернет» без согласия правообладателя или иного основания, предусмотренного Гражданским кодексом РФ.

В Федеральном законе №149-ФЗ «Об информации, информационных технологиях и о защите информации» установлены правила ограничения доступа к информации в сети Интернет, включая распространение информации с нарушением исключительных прав на фильмы, в том числе кинофильмы, телефильмы. 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.

Значение защиты ценных технологий и информации от кражи, шпионажа или других методов незаконного присвоения возрастает в силу факторов глобализации, использования аутсорсинга, удлинения цепочки поставок товаров, широкого использования информационно-коммуникационных технологий и т.д.), Увеличиваются риски того, что украденная коммерческая информация (trade secrets) будет использоваться в третьих странах для производства контрафактных товаров [2].

Серьезную озабоченность вызывают угрозы бизнесу от промышленного шпионажа в пользу конкурентов и экономического шпионажа в пользу иностранных государств. Особое значение приобретает сохранность и защита коммерческой информации (коммерческих секретов), которыми обладают работники при выполнении своих трудовых функций. О вопросах защиты коммерческих секретов и иных средств индивидуализации пойдет речь в следующей части цикла статей.

### Литература


1. Карцхия А.А. Права промышленной собственности в российском праве: навстречу вызовам современности. Lambert Academic Publishing. Germany, 2013.
2. EU Directive on the protection of undisclosed know-how and business information (trade secrets)against their unlawful acquisition, use and disclosure http://ec.europa.eu/


### References


1. Kartskhiya A.A. Industrial property rights in the Russian law: towards challenges. Lambert Academic Publishing. Germany, 2013.
2. EU Directive on the protection of undisclosed know-how and business information (trade secrets)against their unlawful acquisition, use and disclosure http://ec.europa.eu/