СУДЕБНАЯ ЭКСПЕРТИЗА В СПОРАХ О НАРУШЕНИИ IT-ПАТЕНТА

FORENSIC ANALYSIS ON IT PATENT INFRINGEMENT DISPUTES

А. А. Эккарт,
патентный специалист ООО «ИНКО ПАТЕНТ», Новосибирск, a.ekkart@incopatent.ru

A. A. Ekkart,
Patent specialist of INCO PATENT LLC, Novosibirsk, Russia, a.ekkart@incopatent.ru

Е. Л. Шехтман,
российский и евразийский патентный поверенный, директор «ИНКО ПАТЕНТ», ст. преподаватель НГУ, Новосибирск, Российская Федерация, es@incopatent.ru

E. L. Shekhtman,
Patent attorney, Director of INCO PATENT LLC,
Senior lecturer of NSU, Novosibirsk, Russia, es@incopatent.ru

Получение патента на изобретение, основанное на применении программы для ЭВМ, является непростой задачей для патентных специалистов. Еще более сложной процедурой является выявление нарушения таких патентов. Необходимо установить соответствие последовательности действий или системы нарушителя формуле, а не сравнивать код. При этом, нарушители могут скрывать детали работы продукта. Авторы на примере реального судебного спора рассуждают о возможностях установления нарушения IT-патентов.

Obtaining a patent for an invention based on the use of computer software is a challenging task for patent specialists. Even more complex is the procedure of identifying infringements of such patents. It is necessary to evaluate the correspondence between the method or the system used by the infringer and the claims, rather than comparing the program code. We need take into account that infringers may conceal details of the product's operation. Authors discuss the possibilities to prove the infringements of IT patents using a real court case as an example.

Ключевые слова: изобретение, судебная защита исключительных прав.

Key words: invention, infringement of patent rights, patent rights prosecution.

В законодательстве Российской Федерации возможности правовой охраны в качестве изобретений технических решений, представляющих собой способ с использованием программ для ЭВМ, достаточно ограничены. Для отнесения к объектам патентного права компьютерно-реализуемого способа, описывающего алгоритм работы программы для ЭВМ, необходимо показать, что этот способ является техническим решением, то есть соблюдается требование «технического характера» решения.

Согласно п. 59 Правил [1], заявленное изобретение признается техническим решением, относящимся к продукту или способу, в том числе к применению продукта или способа по определенному назначению, если формула изобретения содержит совокупность существенных признаков, относящихся к продукту или способу, в том числе к применению продукта или способа по определенному назначению, достаточную для решения указанной заявителем технической проблемы и достижения технического результата (результатов), обеспечиваемого изобретением. В частности, в п. 2.4.36 Руководства [2] говорится, что заявка на изобретение может относиться к алгоритму программы для ЭВМ, изложенному в виде обеспечивающей достижение технического результата последовательности действий над сигналами (материальный объект), осуществляемых с помощью вычислительной техники (материальных средств). В таком случае имеются основания для признания заявленного объекта техническим решением.

Таким образом, алгоритм может быть признан способом, если за счет него достигается технический результат, который, в частности, может выражаться, например, в защите ЭВМ от ботовых атак, т. е. обеспечении постоянной работоспособности сайта. При соблюдении условий патентоспособности, установленных ст. 1350 ГК РФ, такое техническое решение способно получить патентную охрану в качестве изобретения.

При этом сложности часто возникают не только в процессе экспертизы Роспатента в рамках установления технического характера конкретного алгоритма, но и при установлении нарушения запатентованного компьютеризированного способа. Это связано, в частности, с тем, что одна и та же логика и последовательность действий, т. е. один и тот же способ, могут быть выражены в программном продукте с использованием разных языков программирования и разным образом. В связи с этим установление нарушения путем сравнения программных кодов не всегда является возможным. Также важно отметить, что во многих случаях, даже имея программный код потенциального нарушителя, однозначное выделение из него способа может быть крайне трудоемко в связи со сложной структурой программного продукта. Проведение экспертизы путем сравнения

двух программ может привести к ложным выводам относительно нарушения патента, т. к. сама программа может содержать куда больше признаков и функций, нежели указано в независимом пункте патентной формулы. Более того, сами программы являются объектами авторского права, поэтому их сравнение является бессмысленным для целей установления нарушения исключительного права на изобретение.

Ввиду этого, в рамках патентных споров, касающихся нарушения прав на IT-патенты, экспертиза часто сводится до уровня сравнения описания технологии потенциального нарушителя с признаками независимого пункта формулы изобретения.

В частности, такой подход для установления нарушения патента использовался в рамках производства по делу № А40-29590/2020, где эксперту для анализа были предоставлены в том числе: копия патента на изобретение № 2686003 [3]; протоколы осмотра сайтов: www.samsung.com; developer.samsung.com; www.google.com; www.cybersource.com и иные протоколы осмотра сайтов, содержащих описание технологии потенциального нарушителя; протокол осмотра мобильного приложения *Samsung Pay* и информационный буклет *Samsung Pay.* Однако нарушители в своих рекламных материалах могут не раскрывать всех деталей работы их программного продукта. В таких случаях возможно устанавливать использование признаков, прямо не указанных в описании технологии потенциального нарушителя такими словами, как они названы в формуле изобретения, — по косвенным упоминаниям, следуя формальной логике. Например, если в формуле изобретения охарактеризован способ бесконтактной оплаты при помощи мобильного устройства, содержащего NFC-метку, а в описании технологии потенциального нарушителя наличие NFC-метки не упоминается напрямую, но в описании раскрывается, что оплата производится с использованием технологии NFC, а терминал оплаты включает считыватель NFC-метки, то из этого очевидным образом следует, что нарушитель использует мобильное устройство с NFC-меткой. Также установление использование признаков, нераскрытых в описании технологии потенциального нарушителя, может осуществляться посредством проведения дополнительного технического исследования.

Важно отметить, что для таких технических исследований может потребоваться использование дополнительных технических средств. Проведение технического исследования может осуществляться посредством эксплуатации программного продукта потенциального нарушителя, что также было сделано экспертом в рамках экспертизы по вышеупомянутому делу. Для этого эксперту был предоставлен смартфон с предустанов-

ленным приложением *Samsung Pay*, а также посредством демонстрации функционирования программного продукта потенциальным нарушителем. Так эксперт мог проанализировать использование признаков изобретения при непосредственной эксплуатации приложения *Samsung Pay.*

Согласно п. 3 ст. 1358 ГК РФ изобретение признается использованным в продукте или способе, если продукт содержит, а в способе использован каждый признак изобретения, приведенный в независимом пункте содержащейся в патенте формулы изобретения, либо признак, эквивалентный ему и ставший известным в качестве такового в данной области техники до даты приоритета изобретения. Вопрос об использовании признаков должен быть сформулирован в отношении каждого независимого пункта формулы в отдельности, поскольку для установления нарушения прав на изобретение достаточно использование каждого существенного признака хотя бы одного независимого пункта формулы, необязательно всех независимых пунктов.

При этом разделение независимых пунктов на отдельные признаки относится к компетенции экспертов и специалистов. От того или иного разделения может зависеть установление факта использования изобретения. В частности, если признак способа характеризует этап и выполнение данного этапа с использованием определенного компонента компьютера, разделение такого признака на два отдельных признака для анализа — действие, совершаемое на данном этапе, и то, какими техническими средствами это действие совершается, может приводить к другим выводам. Например, если нарушитель изменит средства выполнения этапа на эквивалентные, то при оценке использования признака, характеризующего средство выполнения этапа, отдельно от действия, совершаемого этим средством, эксперт может прийти к выводу об отсутствии использования признака, характеризующего средство выполнения. Тогда как при оценке использования признака без его дробления на действие и средство выполнения эксперт мог бы прийти к выводу об использовании признака или эквивалентного ему, т. к. оба элемента выполняют одну и ту же функцию.

Другой пример. В рамках подготовки иска по делу № А45-5068/2023 было составлено заключение специалиста с целью установления использования признаков независимых пунктов формулы изобретения по патенту № 2768567 [4] в технологии *Servicepipe Cybert*, принадлежащей ответчику. Большинство признаков независимых пунктов формулы следовали из описания напрямую и были раскрыты в рекламных материалах ответчика теми же словами, что и в формуле изобретения. Однако,

некоторые из признаков не упоминались на сайте вовсе, что требовало дополнительного исследования.

Так, в частности, в формуле изобретения содержится признак «*полученные метрики сводят в единый вектор факторов запроса и выполняют нормализацию*». Такой признак не был описан в буклете, описывающем технологию *Servicepipe Cybert*. Тем не менее, в указанном буклете раскрывалось сведение метрик в вектор факторов запроса, а также применение машинного обучения для анализа данного вектора. Обоснование использования указанного признака на основании информации из буклета было приведено по косвенным упоминаниям путем следования формальной логике с использованием специальных технических знаний и научно-технической литературы. Согласно современным научно-техническим знаниям в области информационных технологий все известные алгоритмы машинного обучения, за исключением алгоритма, основанного на древе принятия решений, требуют предварительного проведения того или иного вида нормализации данных. Таким образом, в рамках заключения специалиста был сделан вывод о том, что если в технологии *Servicepipe Cybert* используется алгоритм машинного обучения, не основанный на древе принятия решений, в технологии должна осуществляться предварительная нормализация вектора факторов запроса, и, как следствие, указанный признак используется в технологии как таковой.

Другой признак — «*осуществляют дополнительную проверку в отношении подозрительного пользователя для уточнения его легитимности, при этом на основании осуществления анализа его поведения предлагают ему для решения генерируемую компьютерной системой задачу с применением криптографических алгоритмов с использованием асимметричного шифрования*» требовал дополнительного технического анализа. В рекламных материалах технологии *Servicepipe Cybert* упоминалось, что в отношении подозрительного пользователя осуществляется дополнительная проверка JS-стека браузера. Тем не менее, в буклете не раскрывалось, какой именно криптографический алгоритм — симметричный, асимметричный или их сочетание применяется.

Ввиду того, что запатентованная технология и технология потенциального нарушителя направлены на предотвращение вредоносных автоматизированных атак, для установления конкретного используемого алгоритма технический анализ заключался в проверке реакции программного продукта на обычное пользовательское поведение, подозрительное поведение и ботовое поведение путем имитации каждого из них на ресурсе, находящимся под защитой потенциального нарушителя.

Был выявлен ряд сайтов, доступ к которым определялся IP-адресами ООО «Сервиспайп», после чего на этих сайтах установление реакции технологии на обычное пользовательское поведение было проверено прямым заходом на сайт через браузер. В результате технология защиты предоставляла доступ к сайту, в связи с чем у пользователя оставалась возможность пользоваться ресурсом. Ботовое поведение, как и подозрительное, имитировалось разными способами.

Большинство ресурсов, находящихся под защитой ООО «Сервиспайп», идентифицировали такое поведение как подозрительное, и в результате в командной строке появлялся код криптографической задачи. В этом коде содержался открытый RSA-ключ. Согласно статье [5] об алгоритме RSA в асимметричном шифровании используют два ключа: публичный (открытый) и приватный (закрытый), где закрытый ключ — это ключ дешифрования, а открытый ключ — ключ шифрования. Там же указано, что в RSA-алгоритме шифрования также используют два ключа: приватный и публичный [5]. Из этого следует, что RSA-алгоритм является криптографическим алгоритмом, использующим асимметричный метод шифрования. Таким образом, использование упомянутого признака в технологии *Servicpipe Cybert* было установлено.

На основании сказанного становится очевидным, что для установления нарушения IT-патента как специалист, так и эксперт должны обладать и юридическими компетенциями, и техническими в соответствующей области техники.

Отсутствие специальных технических знаний может свести установление нарушения к исключительно формальному подходу сравнения текстов рекламных материалов и описания к патенту. Однако такой подход сравним с лингвистической экспертизой, которая не может применяться при установлении нарушения патента. Сопоставление должно проводиться исходя из существа технологий, а не слов, которыми эти технологии обозначены.

Отсутствие же юридических знаний и опыта в составлении патентных заявок у специалиста или эксперта может привести к чрезмерному сужению объема патентной охраны, т. к. технический специалист также может подходить к интерпретации признаков патента исключительно формально. Анализ эквивалентности признаков, в свою очередь, не представляется возможным без сочетания технических и юридических компетенций, т. к. требует одновременно глубоких технических познаний и юридического понимания того, что из себя представляют понятия «сущность изобретения», «технический результат», «равноценность средств замены» и «из-

вестность средств замены до даты приоритета изобретения». При этом определение нарушения патента на изобретение не может проводиться без анализа эквивалентности средств замены, если использование признаков не было установлено напрямую, т. к. это будет приводить к неправомерному сужению объема охраны изобретения экспертами и судами.

Список использованных источников

1. Правила составления, подачи и рассмотрения документов, являющихся основанием для совершения юридически значимых действий по государственной регистрации изобретений. Утверждены приказом Минэкономразвития РФ от 21 февраля 2023 г. № 107).

2. Руководство по осуществлению административных процедур и действий в рамках предоставления государственной услуги по государственной регистрации изобретения и выдаче патента на изобретение, его дубликата. Приказ Роспатента от 27.12.2018 № 236.

3. Гульченко В. Система электронных платежей. Патент РФ № 2686003, дата публикации 23.04.2019.

4. Золотарев В. Г., Барабанов А. А., Лексунин О. А. Способ и система предотвращения вредоносных автоматизированных атак. Патент РФ № 2768567, дата публикации 24.03.2022.

5. Calderbank M. The RSA cryptosystem: history, algorithm, primes. URL: https://math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALAPP/Calderbank.pdf; дата обращения: 27.05.2024.