11. Burrow-Giles Lithographic Co. v. Sarony. URL: https://www.law.cornell.edu/supremecourt/text/111/53

12. Харитонова Ю. С. Правовой режим результатов деятельности искусственного интеллекта // Современные информационные технологии и право: монография / Московский госуниверситет им. М. В. Ломоносова, Юридический факультет / отв. ред. Е. Б. Лаутс. М.: Статут, 2019.

13. Аникин А. С. К вопросу об охраноспособности результатов деятельности искусственного интеллекта как объекта интеллектуальной собственности // Цивилист. 2022. № 2.

14. Duffy S. H., Hopkins J. P. Sit, Stay, Drive: The Future of Autonomous Car Liability // SMU Science & Technology Law Review. 2013. Vol. 16.

15. Colonna K. Autonomous Cars and Tort Liability // Case Western Reserve Journal of Law, Technology & the Internet. 2012. Vol. 4.

О. Г. Кирсанова,
кандидат экономических наук, доцент,
Финансовый университет
при Правительстве Российской Федерации
(Смоленский филиал)

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНСТИТУТА КОММЕРЧЕСКОЙ ТАЙНЫ И ЕЕ ЗАЩИТА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

Аннотация. В статье рассмотрены актуальные проблемы защиты коммерческой тайны в условиях цифровизации экономики. Проанализированы основные подходы к определению содержания категории «коммерческая тайна», приводится правовая статистика в рамках рассмотрения дела, связанных с нарушением коммерческой тайны. Выявлены основные угрозы и направления правового регулирования института коммерческой тайны и ее защиты.

Ключевые слова: коммерческая тайна, разглашение информации, конфиденциальность, информационная безопасность, защита

LEGAL REGULATION OF THE INSTITUTE OF TRADE SECRETS AND ITS PROTECTION IN THE CONDITIONS OF DIGITALIZATION OF THE ECONOMY

Abstract. The article discusses the current problems of protecting trade secrets in the conditions of digitalization of the economy. The main approaches to the definition of the content of the category “trade secret” are analyzed, legal statistics are considered and analyzed in the framework of the consideration of causes related to the violation of trade secrets. The main threats and directions of legal regulation of the institute of commercial secrets and its protection are identified.

Keywords: trade secret, disclosure of information, confidentiality, information security, protection

Процессы цифровизации, которые в последнее время достаточно активно и тесно интегрируются в коммерческую деятельность субъектов хозяйствования различных организационно-правовых форм, наряду с возможностями, которые открываются в рамках расширения сферы присутствия, наращения клиентской базы посредством использования современных технологий продвижения бренда или продукта, создают угрозы потери конкурентных преимуществ, прежде всего в силу утраты или публичного разглашения коммерческой тайны, являющейся одним из наиболее привлекательных объектов для коммерческого или промышленного «шпионажа» или пришедших им на смену более эффективных хакерских атак на IT-инфраструктуру предприятия, что актуализирует роль правового регулирования и защиты института коммерческой тайны.

Изучение содержания коммерческой тайны и механизма ее правового регулирования и защиты возрастает в условиях цифровизации социально-экономических процессов, которая сопровождается расширением присутствия бизнеса в виртуальной среде, что в свою очередь, способно привести к риску утраты информации, составляющей коммерческую тайну, что подтверждается ростом в течение трех последних лет числа утечек внутренней корпоративной информации различного содержания (преимущественно персональных данных, финансовой информации и т. п.).

Согласно данным ГК InfoWatch, в течение 2019–2022 гг. по ст. 183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайны», было осуждено: в 2019 г. – 41 чел.; в 2020 г. – 35 чел., в 2021 г. – 41 чел., в 2022 г. – 47 чел. Положительная динамика в течение 2019–2022 г. составила 6 случаев, что соответствует 13,7 % [6].

Согласно данным ГАС «Правосудие», в 2019 г. в рамках обозначенной статьи УК РФ в течение 2019–2022 г. было осуждено 69 чел., 70 чел., 40 чел., 42 чел. соответственно, что соответствует росту в 2022 г. в сравнении с 2021 г. на 5,4 %, отражая положительную динамику последних двух лет.

На фоне общего объема утечек информации, рост которых в течение 2022 г., согласно данным ГК InfoWatch, составил 45 %, на долю потери данных, которые составляют категорию коммерческой тайны, пришлось 13 %, что соответствует 305 базам похищенной информации или 187,6 млн записей. В течение 2022 г. профильные компании отразили в 4,5 раза больше атак в сравнении с 2021 г., что к росту затрат, необходимых для ликвидации кибератак и проникновения хакеров в IT-инфраструктуру хозяйствующих субъектов на 20 %. При этом, как отмечает руководитель направления аналитики и спецпроектов ГК InfoWatch Андрей Арсентьев, данные, которые составляют коммерческую тайну, являются востребованными в настоящее время по причине возрастания конкурентной борьбы, преследуя цель причинения максимально возможного экономического ущерба конкуренту, в том числе посредством кражи конфиденциальных данных. Сложившаяся ситуация для бизнеса влечет за собой рост затрат, связанных с потребностями

и задачами улучшения информационной безопасности, что, согласно экспертной оценке заместителя генерального директора дата-центра и облачного провайдера Oxygen Кирилла Орлова, в общем IT-бюджете крупных корпораций составит 12–15 %, в то время как для небольших компаний станет достаточно обременительным [7].

Приведенные данные позволяют сделать вывод об актуальности правового регулирования и защиты института коммерческой тайны как конкурентного фактора хозяйствующего субъекта, который имеет длительную историю и зависим от экономической и технологической трансформации общества.

В. Д. Саттаров отмечает, что формирование и правовое регулирование института коммерческой тайны в российском праве можно проследить, начиная с периода Российской империи вплоть до перехода к рыночных отношениям в 1990 гг., анализ которого достаточно подробно представлен в исследованиях А. А. Фатьянова, в то же время в работах З. Р. Игбаевой и И. С. Корокрина можно увидеть указание на более ранний период формирования коммерческой тайны и ее правового регулирования, который начинается в период Античности [4. С. 120].

В настоящее время институт коммерческой тайны регулируется нормами ст. 23 Конституции Российской Федерации, ч. 2 которой закреплено право каждого на тайну переговоров, переписки, сообщений, при этом под «каждым» целесообразно понимать и хозяйствующие субъекты, являющиеся обладателями коммерческой тайны. Коммерческая тайна, как отдельный институт и объект правового регулирования, определена в ч. 1 ст. 3 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне», и представляет собой сведения, наделенные следующими признаками: наличие потенциальной или реальной ценности, способной принести ее обладателю прибыль либо любую иную выгоду; ограниченность доступа к данным сведениями для третьих лиц, которые, находясь за пределами бизнес-единицы могут не знать о наличии коммерческой тайны или ее содержании; доступ к такой информации ограничен для круга лиц, отвечающих непосредственно на реализацию режима коммерческой тайны, вводимого ее обладателем для защиты сведений, составляющих коммерческую тайну [6. С. 330].

Другими словами, коммерческая тайна в рамках правового регулирования отнесена к информации ограниченного доступа, при этом перечень субъектов, которые могут быть допущены к сведениям, устанавливается ее обладателем, что определяет особенности ответственности и обязанности его в рамках защиты коммерческой тайны от разглашения во внешней среде.

Ценность коммерческой тайны, обуславливающей высокие риски и угрозы ее разглашения, обусловлена тем, что содержащаяся в ней информация позволяет обеспечить формирование конкурентных преимуществ обладателя, сократить его затраты на реализацию хозяйственных процессов, либо получить более высокую в сравнении с конкурентами прибыль. Как правило, к таким сведениям могут быть отнесены перечень клиентской базы с персональными данными клиентов, результаты маркетинговых исследований рынка или научно-технических изысканий, полезные модели, позволяющие оптимизировать производственный цикл и снизить его затраты и прочие сведения, которые представляют корпоративную

ценность и не могут быть опубликованы во внешней среде, поскольку направлены на получение ее обладателем более высокого дохода или обретения конкурентного преимущества.

Особенностью правового регулирования института коммерческой тайны является право, предоставленное ее обладателю, самостоятельного определения ценности имеющейся информации и отнесения ее к категории повышенной конфиденциальности, что в ряде случаев может привести к злоупотреблению правом и сокрытию информации, которая будет иметь важное общественное значение. Во избежание подобных ситуаций ст. 5 Федерального закона № 98-ФЗ «О коммерческой тайне» определен перечень сведений, которые не могут быть отнесены к категории коммерческой тайны, подлежат опубликованию, субъект, осуществивший их разглашение не может быть привлечен к ответственности.

В. Д. Саттаров выделяет три информационных блока таких сведений:

– информация, обеспечивающая предпринимательскую деятельность, в т. ч. в части взаимодействия бизнес-единицы с другими субъектами, например, ФНС России, банками, инвесторами, социальными фондами и т. п.;

– информация, имеющая общественно важный характер (например, сведения о кандидатах, баллотирующихся в органы государственной власти или местного самоуправления, сведения об исполнении бюджета, данные о доходах государственных служащих и т. п.);

– информация, содержащая общественно важные сведения, обязательное опубликование которых прямо закреплено правовыми нормами (например, опубликование данных о выбросах в атмосферу отравляющих веществ или иных техногенных рисках, сейсмологических угрозах и выявленных в процессе фитосанитарного и ветеринарного контроля рисках заражения домашних животных и т. п.) [5. С. 122].

В данном случае прослеживается взаимосвязь со шведским правовым институтом коммерческой тайны «whistle-blowing», буквально означающего «право свистеть», который В. Н. Монахов характеризует как «нельзя держать в секрете то, что в интересах общества должно быть разглашено» [4. С. 122], что положено в основу регулирования отношений, связанных с разрешением спроса между администрацией предприятия и его сотрудниками, которые опубликовали информацию, имеющую общественно важное значение (например, о выбросе отравляющих веществ в атмосферу и т. п.), в отношении которых сформирована соответствующая судебная практика.

В 2019–2022 гг. в судах первой инстанции 53,7 % дел были рассмотрены в рамках только ст. 183 УК РФ, направленной на защиту интересов субъектов бизнеса, ущерб которым был причинен разглашением коммерческой тайны, 46,3 % дел были сопряжены с обвинениями по другим статьям, например, ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», в большинстве случаев по ч. 3 «Деяния, …, совершенные группой лиц по предварительному сговору или организационной группой лиц либо одним лицом с использованием служебного положения».

В случае применения только ст. 183 УК РФ большая часть дел (56,1 %) была рассмотрена по ч. 3 упомянутой статьи, 36,59 % дел были рассмотрены в рамках ч. 2 и 7,31 % – в рамках ч. 1, что позволяет сделать вывод о том, что как правило, преступления и правонарушения, касающееся разглашения коммерческой тайны и опубликования данных, осуществляются должностными лицами организации – обладателя по предварительному сговору и большей части в корыстных целях [7. С. 10].

В большинстве случаев возбужденные дела касались разглашения и намеренной передачи сотрудниками операторов связи информации абонентов (персональных данных, детализации звонков и т. п.), передачи банковскими служащими информации, относимой «банковской тайне» (информация о картах, состоянии счетов клиентов банков и т. п.).

По результатам рассмотрения дел в 44,3 % судами были вынесены обвинительные приговоры, в 39,9 % дела прекращались на основании примирения сторон либо по ходатайству следователя, а также по иным основанием. В отношении 1,1 % дел были вынесены оправдательные приговоры, а также 1,6 % были возвращены следствию [7. С. 12].

При вынесении обвинительных приговоров суды в большинстве случаев (44,7 %) назначали административный штраф, средний размер которого составил 123,8 тыс. руб., максимальный размер – 1 млн руб., минимальный – 8 тыс. руб.). В 36,9 % случаях вынесения обвинительного приговора судами назначен условный срок отбывания наказания (от 6 мес. по одной статье, до 4 лет – по совокупности статей). В 9,2 % обвинительных приговоров были назначены исправительные работы, а также в 9,2 % обвинительных приговоров судами было определено отбывание наказания в исправительных колониях общего режима.

Набирающий в настоящее время процесс цифровизации оказывает все большее влияние на предпринимательский сектор, вынуждая субъекты бизнеса, которые хотят сохранить свою конкурентоспособность и привлекательность среди клиентов и партнеров, расширять сферу присутствия в виртуальной бизнес-среде, вырабатывая новые подходы к формированию баз данных и управлению информацией.

Актуальным трендом, который обозначился в период пандемии COVID-2019, стал удаленный формат работы, закрепивший к настоящему времени практику взаимодействия с клиентами или стейкхолдерами в дистанционном формате, используя современные коммуникационные технологии (например, платформы конференцсвязи) и онлайн-банки при осуществлении необходимых расчетных операций. Параллельно активными темпами осуществляется процесс цифровизации внутренней информации хозяйствующего субъекта, касающейся персональных данных, сведений о способах осуществления производственной и коммерческой деятельности, результатов исследований рынков, ноу-хау и иной информации, которая может обеспечить конкурентное преимущество данного субъекта и принести ему прибыли, и перевод ее в облачные системы хранения, что приводит к замещению классических схем «промышленного шпионажа» хакерскими атаками, которые могут быть куда более болезненными для бизнес-субъекта в части причинения коммерческого ущерба.

Начавшаяся несколько лет назад цифровизация общественной жизни привела, по мнению В. Н. Монахова, к существенным изменениям коллективного сознания, что обусловило переход к поиску новых форм работы с информацией и ее защите [4. С. 123].

В настоящее время риски утраты и опубликования коммерческой тайны возрастают вследствие расширения присутствия ее обладателя в виртуальной среде. Согласно данным записей ГАС «Правосудие», в рамках ст. 183 УК РФ в 37,4 % случаев опубликование коммерческой тайны осуществлялось при помощи ресурсов сети Интернет; 37,4 % – с помощью сервисов мгновенной передачи сообщений (мессенджеров); в 6 % случаев информация передавалась при помощи электронной почты; в 3,6 % – на съемных носителях; в 12 % – на бумажных архивах; в 3,6 % – при помощи устных сообщений. В 70,4 % случаев субъектами, которые осуществили разглашение информации, содержащей коммерческую тайну, являлись непривилегированные сотрудники, занимающие невысокое должностное положение в организации [7. С. 17–18].

Как отмечалось, основным инструментом защиты коммерческой тайны, создающим возможности для разрешения противоречий в рамках судебного процесса, является обязанность ее обладателя установить режим коммерческой тайны, наделяющий его правом самостоятельного определения и регулирования правил доступа к информации, отнесенной им же к категории коммерческой тайны. При этом законодатель подчеркивает, что защиты коммерческой тайны посредством соответствующего режима является не правом, а обязанностью ее обладателя и традиционно предусматривает следующие мероприятия:

– формирование перечня сведений, которые составляют коммерческую тайну на основе признаков, ее характеризующих;

– определение круга пользователей сведений, содержащих коммерческую тайну, которые могут их использовать в процессе решения текущих задач, или определение круга субъектов, которые являются представителями внешней бизнес-среды, однако будут наделены правом доступа к коммерческой тайне в силу взаимных коммерческих интересов;

– формирование системы учета и контроля использования сведений, составляющих коммерческую тайну, и предупреждение их нежелательного опубликования во внешней среде.

Вместе с тем, как показывает статистика, наработанных к настоящему времени мер и рекомендаций по защите коммерческой тайны в актуальных условиях цифровизации информационных потоков недостаточно. Очевидно, что существующие традиционные направления защиты должны претерпеть правовую и цифровую трансформацию.

В качестве предупредительных мер на уровне администрации по защите коммерческой тайны повышается роль криптографического преобразования информации. Вследствие высокого уровня риска ее разглашения посредством сетевых ресурсов или мессенджеров в ряде компаний ограничивается доступ к средствам связи в течение рабочего дня не только для допущенных к работе со сведениями, содержащими коммерческую тайну, сотрудников, но и всего коллектива в целом.

При этом в части рассмотрения дел, связанных с утечкой информации посредством ее размещения на личных страницах в социальных сетях или хранения в электронном почтовом ящике, к настоящему времени отсутствует однозначная правовая позиция.

Так, Постановлением Конституционного суда России от 26.10.2017 № 25-П определено, что случай, связанный с отправлением работником на личный адрес электронной почты персональных данных других сотрудников, служебных документов и прочей конфиденциальной информации в целях продолжения работы с ними дома, следует считать разглашением коммерческой тайны, поскольку компания – владелец почтового сервера получила доступ к пересылаемым охраняемым законом данным. Увольнение сотрудника было признано правомерным. Подобную правовую позицию достаточно часто можно встретить в судебных решениях по аналогичным ситуациям.

Постановление Пленума Верховного Суда Российской Федерации от 17.04.2003 № 2 «О применении судами Российской Федерации Трудового кодекса Российской Федерации» делает обязательным доказывание обладателем ценности разглашенной сотрудником информации как коммерческой тайны, на основе которой оценивается объективность и целесообразность принятого решения об увольнении такого сотрудника и возмещении при необходимости причиненного материального ущерба. На наш взгляд, регулирование процедуры доказывания представляет собой правовой пробел, поскольку в настоящее время сохраняется высокий уровень субъективности в доведении информации до суда, который, в свою очередь, также принимает решение, основываясь на внутреннем убеждении.

Считаем целесообразным в рамках развития института коммерческой тайны и правового регулирования механизмов ее защиты проработать в целях большей объективности аспект, связанный с доказыванием настоящей или будущей ценности разглашенной информации, и определением размера ущерба, который был причинен обладателю коммерческой тайны противоправными действиями третьих лиц.

В настоящее время законодатель предоставляет обладателю коммерческой тайны достаточно широкое правовое поле для ее защиты, ограничивая его лишь гарантией и защитой конституционных прав и свобод человека и гражданина. Следовательно, права и обязанности обладателя коммерческой тайны должны быть направлены на формирование и внедрение внутренних регламентов ее защиты, которые могут быть представлены в виде локального нормативного акта, основанного на нормах действующего законодательства и четко прописывающего основные положения механизма защиты коммерческой тайны, приоритетными из которых являются следующие:

– формирование практики разработки и подписания соглашений о неразглашении информации сотрудниками, имеющими к ней допуск с обязательным ознакомлением с правовыми последствиями в виде различных форм и видов ответственности, предусмотренной отдельными правовыми нормами;

– организация и совершенствование системы контроля физического и электронного доступа к информации на уровне внутренних регламентов использования

внешних съемных носителей, общения в социальных сетях, которые в последнее время активно используются для внутрикорпоративного обмена информацией или сервисах мгновенной передачи сообщений;

– формирование многоступенчатой системы защиты информации с сужением круга лиц, допущенных к ее использованию с подписанием на каждом уровне соответствующего соглашения о неразглашении;

– обучение сотрудников основам работы с информацией, составляющей коммерческую тайну в информационно-коммуникационных сетях (в ряде случаев ее разглашение осуществляется непроизвольно вследствие недостаточно развитых навыков работы с такими ресурсами), а также формирование высокого уровня корпоративной культуры, приоритетным элементом которой станет защита коммерческой тайны.

Подводя итог, отметим, что в настоящее время защита коммерческой тайны от ее неправомерного использования является одним из наиболее острых и проблемных аспектов информационного и предпринимательского права, что обусловлено влиянием процесса цифровизации на принципы и способы работы с корпоративной информацией. Законодатель, создавая обширное правовое поле для защиты конфиденциальной информации, наделяет существенными правами ее обладателя в части защиты коммерческой тайны, фактически вменяя данный процесс в его прямые обязанности, что позволяет выработать и развивать эффективную систему защиты коммерческой тайны в рамках действующего законодательства.

Анализ правоприменительной практики по ст. 183 УК РФ позволяет сделать вывод о возрастающей динамике случаев разглашения коммерческой тайны, что особенно опасно в условиях расширения сферы применения информационных ресурсов в практике хозяйственной деятельности и присутствия бизнес-субъекта в виртуальной бизнес-среде. Следовательно, сформированных к настоящему времени механизмов защиты коммерческой тайны силами ее обладателей недостаточно, что обуславливает актуальность проведения дальнейших исследований практических аспектов работы с информацией, составляющей коммерческую тайну и совершенствование правовых механизмов ее регулирования.

Список литературы

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020. URL: https://www.consultant.ru

2. Уголовный кодекс Российской Федерации: федеральный закон от 13.06.1996 № 63-ФЗ. URL: https://www.consultant.ru

3. О коммерческой тайне: федеральный закон от 29.07.2004 № 98-ФЗ. URL: https://www.consultant.ru

4. Монахов В. Н. Утро пятой свободы (к проблеме совершенствования правового режима свободы информации и знаний как ценностей и драйверов развития) // Право. Журнал Высшей школы экономики. 2014. № 3. С. 121–135.

5. Саттаров В. Д. Право коммерческой тайны в условиях цифровизации общества // Пермский юридический альманах. 2019. № 2. С. 119–127.

6. Сафиуллин А. Р., Смирнова В. С. Коммерческая тайна и ее защита в цифровой экономике // Вузовская наука в современных условиях: сборник материалов 57-й научно-технической конференции. Часть 2. Ульяновск: Издательство УлГТУ, 2023. С. 330–332.

7. Исследование судебной практики по уголовным делам, связанным с незаконным получением и разглашением сведений, составляющих коммерческую, налоговую или банковскую тайну, 2019–2021 гг. // Экспертно-Аналитический центр InfoWatch, 2022 г. 25 с.

8. В России растет число утечек данных, составляющих коммерческую тайну. URL: https://habr.com/ru/news/682834

Ю. А. Комнатная,
кандидат юридических наук,
Белгородский государственный национальный
исследовательский университет

ПРАВО НА ИНФОРМАЦИЮ И ИНФОРМАЦИОННАЯ ВОЙНА

Аннотация. Статья посвящена вопросам соотношения понятий «право на информацию» и «право на доступ к информации» с целью выяснения содержания данных прав для определения их пределов, гарантирующих цифровую и, соответственно, национальную безопасность. Уделено внимание истории развития информационных войн, эффективности различных методов информационной войны при отсутствии должного контроля за информационными потоками со стороны государства. Определен главный критерий информации, а также обозначена необходимость введения института ответственности международных должностных лиц за распространение и использование недостоверной информации, который позволит обеспечить минимальную безопасность государств на международном уровне.

Ключевые слова: информация, право на информацию, право на доступ к информации, информационная война, достоверность информации, цифровая безопасность

THE RIGHT TO INFORMATION AND INFORMATION WARFARE

Abstract. The article is devoted to the relationship between the concepts of «right to information» and «right to access to information» in order to clarify the content of these rights to determine their limits, guaranteeing national security. Attention is paid to the history of the development of information wars, the effectiveness of various methods of information warfare in the absence of proper control over information flows by the state. The main criterion of information is defined, as well as the need to introduce the institution of responsibility of international officials for the dissemination and use of false information, which will ensure minimal security of states at the international level.