DOI: 10.17803/1994-1471.2025.170.1.086-097

П. Г. Федоров*

Формы проявления коммерческой тайны в цифровой экономике

Аннотация. Вовлечение цифровых технологий в предпринимательскую деятельность расширяет границы, в рамках которых возможно выявление и последующее использование коммерчески значимой информации. Цифровая экономика, с одной стороны, формирует среду, в которой бизнес способен шире реализовать действительную или потенциальную ценность сведений, составляющих коммерческую тайну, а с другой — создает новые риски в информационной среде, к которым бизнес может быть не готов. Актуальными становятся поиски новых проявлений коммерческой тайны в цифровой среде. Главной целью работы выступает обоснование закономерности изменений взглядов на коммерчески значимую информацию в условиях цифровой экономики. Смежной целью выступает раскрытие возможного практического использования цифровых технологий при работе со сведениями, составляющими коммерческую тайну. Изложенные цели обусловливают задачу переосмысления самого института коммерческой тайны под давлением новых технологий. В качестве методов применены сравнение, анализ, синтез и моделирование. Исследование продемонстрировало ряд перспектив переосмысления института коммерческой тайны. Использование цифровых технологий не признается обязательным фактором функционирования коммерческой тайны в новых условиях, но вовлечение таких технологий в предпринимательскую сферу способно раздвинуть горизонты круга сведений, составляющих коммерческую тайну, а также заложить фундамент подхода к защите тайны, при котором любое умышленное действие по ее нарушению ставится вне закона. При действующем правовом регулировании и сложившейся судебной практике несовершение владельцем коммерческой тайны перечисленных в статье формальных действий может привести к выводу о том, что режим коммерческой тайны не установлен, а это легализует действия правонарушителя.

Ключевые слова: цифровые технологии; блокчейн; искусственный интеллект; большие данные; цифровизация; коммерческая тайна; режим коммерческой тайны; закрытая информация; информация; информационное общество.

Для цитирования: *Федоров П. Г.* Формы проявления коммерческой тайны в цифровой экономике // Актуальные проблемы российского права. — 2025. — Т. 20. — № 1. — С. 86–97. — DOI: 10.17803/1994-1471.2025.170.1.086-097.

Forms of Trade Secrets in the Digital Economy

Pavel G. Fedorov, Partner, *Justpro* Law Firm, Moscow, Russian Federation
fedorovpg@mail.ru

Abstract. The use of digital technologies in entrepreneurial activity expands the boundaries within which it is possible to identify and subsequently use commercially relevant information. The digital economy, on the one hand, creates an environment where businesses are able to implement the actual or potential value of information that constitutes a trade secret more widely, and, on the other hand, it creates new risks in the information environment

* *Федоров Павел Геннадьевич*, партнер юридической фирмы «ЮстПро»
Бориса Пастернака ул., д. 7, кв. 199, г. Москва, Российская Федерация, 108849
fedorovpg@mail.ru

that businesses may not be ready for. It is becoming relevant to search for new manifestations of trade secrets in the digital environment. The main purpose of the study is to substantiate the pattern of changes in views on commercially significant information in the digital economy. A secondary goal is to disclose the possible practical use of digital technologies when working with information that constitutes a trade secret. The stated goals determine the task of rethinking the very institution of trade secrets under the pressure of new technologies. Methodologically, the study is based on comparison, analysis, synthesis, and modeling. The study described a number of perspectives for rethinking the institution of trade secrets. The use of digital technologies is not recognized as an obligatory factor in the functioning of commercial secrets in the new conditions, but the involvement of such technologies in the business sphere can expand the horizons of the range of information constituting a commercial secret, as well as lay the foundation for an approach to secrecy protection in which any deliberate act of violating it is outlawed. Under the current legal regulation and established judicial practice, failure by the owner of the trade secret to perform the formal actions listed in the paper may lead to the conclusion that the trade secret regime has not been established, and this legalizes the actions of the offender.

Keywords: digital technologies; blockchain; artificial intelligence; big data; digitalization; trade secret; trade secret regime; classified information; information; information society.

Cite as: Fedorov PG. Forms of Trade Secrets in the Digital Economy. *Aktual'nye problemy rossijskogo prava*. 2025;20(1):86-97. (In Russ.). DOI: 10.17803/1994-1471.2025.170.1.086-097.

Осуществление предпринимательской деятельности в условиях цифровой экономики сопровождается использованием цифровых технологий, которые повышают возможности компании в целом. Реализация таких возможностей зависит от удовлетворения ключевого требования к новым технологиям, заключающегося в их способности обеспечивать сбор, агрегацию и обработку большого массива данных[1]. Именно через данные Ю. А. Тихомиров и Э. В. Талапина определяют цифровую экономику: для них это экономика данных[2]. В. А. Вайпан видит цифровую экономику в качестве системы экономических отношений, в которой ключевым фактором производства являются данные в цифровой форме[3].

В становлении и развитии цифровой экономики в нашей стране большую заинтересованность демонстрирует государство. Так, в целях решения задачи по обеспечению ускоренного внедрения цифровых технологий в экономике и социальной сфере Правительством РФ была сформирована национальная программа «Цифровая экономика Российской Федерации»[4]. В состав данной программы были включены следующие федеральные проекты: нормативное регулирование цифровой среды; кадры для цифровой экономики; информационная инфраструктура; информационная безопасность; цифровые технологии; цифровое государственное управление; искусственный интеллект; обеспечение доступа в Интернет за счет развития спутниковой связи; развитие кадрового потенциала ИТ-отрасли.

Указанная программа рассчитана на период до 2024 г. включительно и в связи с окончанием ее действия имеются планы по утверждению до июня 2024 г. новой программы «Экономика данных» с периодом действия до 2030 г.[5]

---

1 *Сибел Т.* Цифровая трансформация. Как выжить и преуспеть в новую эпоху / пер. с англ. Ю. Гиматова ; науч. ред. М. Савицкий, К. Щеглова, К. Пахорукова. М. : Манн, Иванов и Фербер, 2021. С. 50.

2 *Семякин М. Н.* Гражданско-правовой договор в сфере цифровой экономики: теоретический и практический аспекты исследования // Экономическое правосудие в Уральском округе. 2020. № 1. С. 98–114.

3 *Вайпан В. А.* Правовое регулирование цифровой экономики // Предпринимательское право. Приложение «Право и бизнес». 2018. № 1.

4 Утверждена протоколом заседания президиума Совета при Президенте РФ по стратегическому развитию и национальным проектам от 04.06.2019 № 7 // URL: https://digital.gov.ru. 09.07.2019.

5 Параметры нацпроекта «Экономика данных» утвердят до июня 2024 года // URL: https://www.interfax.ru/russia/925139 (дата обращения: 27.02.2024).

Минцифры России поясняет, что новый национальный проект коснется всех этапов и уровней работы с данными. На первом этапе предусматривается сбор данных, в частности, за счет высокочувствительных датчиков, в том числе повышающих точность позиционирования объектов квантовых сенсоров. На втором этапе планируется передача данных и развитие систем связи.

В рамках нового национального проекта Минцифры России выделяет следующие значимые направления: обеспечение хранения (развитие центров обработки данных) и безопасности данных (технологии квантовых коммуникаций и квантового шифрования), развитие стандартов и протоколов работы с данными (особенно в части хранения персональных данных граждан), а также обработку и анализ данных, создание репозитория открытого кода. При этом алгоритмы анализа данных должны основываться на технологиях искусственного интеллекта с задействованием российского программного обеспечения[6].

По утверждению руководителя Минцифры России, новая программа будет решать как прикладные, так и научные задачи. Прикладные задачи составляет всё то, что связано с инфраструктурой: беспилотники, «умный» транспорт, видеонаблюдение. К числу научных, к примеру, можно отнести квантовые вычисления[7].

Вновь разрабатываемая программа предположительно даст мощный толчок развитию технологии big data, позволяющей обрабатывать большие массивы данных, объем которых постоянно увеличивается[8]. Без обработки таких данных их ценность компания не сможет выявить и потребить. В этой связи Томас Сибел в качестве главной сложности видит комплексное применение цифровых технологий (облачных вычислений, больших данных, Интернета вещей (IoT) и искусственного интеллекта) в целях создания значительной ценности[9].

Применение цифровых технологий имеет в первую очередь прикладную задачу. Вовлечение таких технологий в осуществление предпринимательской деятельности в условиях конкуренции позволяет после апробации и адаптации выявить особенности взаимодействия их между собой и предоставить компании потенциал роста.

Взаимодействие цифровых технологий может быть представлено следующим образом. Технологии big data и IoT обеспечивают накопление данных соответствующей направленности. Технология искусственного интеллекта производит обработку этих данных по заранее заданным алгоритмам. А в силу большого объема сведений их накопление и обработка производятся в облачных сервисах.

Архитектура выстраиваемого взаимодействия между цифровыми технологиями может потребовать перестроения бизнес-процессов, к чему руководство компании должно быть готово и не воспринимать это в качестве угрозы. Напротив, вовлечение технологии big data, позволяющей накопить большие массивы данных, в отсутствие возможной трансформации бизнес-процессов приведет к бессмысленности инвестиций в такую технологию, а возможно, и к осложнению действующих бизнес-процессов с возложением на сотрудников дополнительных обязанностей, что способно повлечь совершение ими ошибок.

К тому же необходимо учитывать, что извлечение действительной выгоды от использования технологии big data обеспечивается при условии понимания не только самих данных и поддерживающей ИТ-инфраструктуры, но и способности использовать полученную и обработанную

---

[6] Значимые направления нацпроекта «Экономика данных» // URL: https://www.kommersant.ru/doc/6380045 (дата обращения: 27.02.2024).

[7] Нацпроект «Экономика данных» будет решать прикладные и научные задачи // URL: https://www.cnews.ru/news/top/2023-11-01_mintsifry_programmu_natsionalnaya (дата обращения: 27.02.2024).

[8] Риски цифровизации: виды, характеристика, уголовно-правовая оценка : монография / отв. ред. Ю. В. Грачева. М. : Проспект, 2022. С. 28.

[9] *Сибел Т.* Указ. соч. С. 51.

информацию в предпринимательской деятельности[10].

В процессе задействования цифровых технологий компания сталкивается с необходимостью обработки полученных сведений, объем накопления которых увеличивается. В. А. Северин отмечает тенденцию накопления за последние 20 лет в стране объемов секретной информации в первую очередь частными компаниями[11]. Можно обозначить свойственную росту объемов информации закономерность в виде увеличения за период с 2008 по 2018 г. случаев утечки сведений, представляющих коммерческую тайну, в восемь раз, что в первую очередь обусловливается использованием информационных технологий[12].

Указанная тенденция сохраняется. Согласно представленной компанией «InfoWatch» информации, которая была разбита согласно группам стран, доля утечек коммерческой тайны из компаний в таких странах, как США, Великобритания, Германия, Испания, Италия и Канада, в 2022 г. выросла в два раза по сравнению с 2021 г. — в среднем с 10,2 % до 19,4 %. Скромнее показатели утечек коммерческой тайны в таких странах, как Китай, Аргентина, Белоруссия, Бразилия, Вьетнам и Индия: рост с 5,1 % в 2021 г. до 8,9 % в 2022 г. В России случаи кражи коммерческой тайны тоже участились: по состоянию на лето 2022 г. доля утечек коммерческой тайны в общем массиве раскрытых данных увеличилась до 13,7 %, притом что в 2021 г. указанный показатель составлял 5,4 %[13].

Описанные тенденции уловило ПАО «Сбербанк», которое предпринимает попытки задействовать технологии искусственного интеллекта при построении режима коммерческой тайны. Среди заявленных выгод от внедрения разрабатываемого им сервиса можно выделить:

— значительное повышение эффективности защиты от утечек сведений, составляющий коммерческую тайну, за счет существенного повышения точности их выявления;

— кратное снижение трудозатрат на поддержание режима коммерческой тайны в актуальном состоянии;

— значительное снижение субъективизма и человеческого фактора в процессе сбора информации, что гарантирует релевантность и актуальность перечня сведений, составляющих коммерческую тайну;

— повышение прозрачности процесса сбора информации и обеспечение более высокого уровня ее защищенности[14].

В целом можно говорить о том, что цифровые технологии способствуют выявлению сведений, имеющих коммерческую ценность для компании. Разумно предположить, что объем данной информации со временем будет увеличиваться. В этой связи имеет смысл обозначить две взаимосвязанные закономерности: переосмысление закрепленного в законодательстве понятия сведений, составляющих коммерческую тайну, и формирование рынка таких сведений.

В предложенной законодателем формулировке сведения, составляющие коммерческую тайну, определяются через их потенциальную и действительную ценность. Такой подход подвергается критике, базирующейся на том, что отсутствие разъяснений указанных параметров исключает практическую пользу соответ-

[10] *Сибел Т.* Указ. соч. С. 95.

[11] *Северин В. А.* Правовая работа в организациях высокотехнологичного комплекса. М. : Ленанд, 2022. С. 191. (Основы защиты информации. № 21.)

[12] *Акмаров П. Б.*, *Газетдинов М. Х.*, *Третьякова Е. С.* Проблемы защиты коммерческой информации в условиях цифровизации экономики // Вестник Казанского государственного аграрного университета. 2020. Т. 15. № 2. С. 133–138.

[13] Доля утечек коммерческой тайны в 2022 г. увеличилась по сравнению с 2021 г. // URL: https://www.kommersant.ru/doc/5925219 (дата обращения: 27.02.2024).

[14] Использование технологий ИИ в построении режима коммерческой тайны на предприятии // URL: https://www.sberbank.ru/ru/person/kibrary/articles/tehnologiy_iskusstvennogo_intellekta_v_postroenii_rezhima_kommercheskoy_tayny (дата обращения: 11.02.2024).

ствующих законоположений, поскольку произвольность оценки данных параметров может породить злоупотребления при установлении режима коммерческой тайны[15].

Вопрос использования термина «ценность» применительно к коммерческим секретам фундаментально обусловлен тем, что главным ресурсом постиндустриального общества является информация, где данные превращаются в валюту[16]. Поэтому информация представляет собой товар, который имеет определенную стоимость, что и порождает необходимость решения разного рода правовых вопросов[17].

В контексте коммерческой тайны обращает на себя внимание определение параметров потенциальной и действительной ценности через неизвестность информации для третьих лиц. Указанная ценность формируется по мнению владельца информации, который предполагает интерес к ней третьих лиц и поэтому стремится сохранить ее в тайне. При этом закон использует понятие «ценность» как собирательную категорию, которая предоставляет конкретному владельцу коммерческих секретов право предъявлять имущественные требования, подлежащие оценке.

Предположение об интересе третьего лица к тем или иным сведениям базируется на представлении их владельца, что автоматически не означает действительного интереса третьего лица. Можно допустить, что свидетельством такого интереса может являться попытка получения секретных сведений (удачная или неудачная). Но третье лицо может неумышленно получить данные сведения (например, вследствие ошибочного раскрытия их сотрудником обладателя сведений), что не должно говорить о наличии интереса к ним у третьего лица, хотя обладатель сведений может рассматривать их в качестве экономического ресурса бизнеса. Г. Ю. Хачатурян, например, допускает, что к таким сведениям могут относиться алгоритмы и способы ведения предпринимательства[18], которые могут различаться в зависимости от условий ведения бизнеса и не представлять интереса для рынка априори.

Безусловно, обладатель сведений использует защитные меры, чтобы предотвратить попадание соответствующих данных к третьим лицам, что позволяет определять коммерчески значимую информацию через введение режима коммерческой тайны: раз обладатель применяет защитные меры, значит, он защищает соответствующие сведения. Но законодатель то ли умышленно, то ли из-за желания продемонстрировать значимость сведений, составляющих коммерческую тайну, предусмотрел ценностные характеристики. И поскольку обладателем таких сведений может быть коммерческий субъект, для которого ценность воспринимается в плоскости выгоды, то использование понятия «потенциальная и действительная ценность» можно рассматривать с позиций информационного общества, расширяющего горизонты обладания информацией.

Защита информации заключается в обеспечении конфиденциальности той ее части, которая при определенных обстоятельствах предоставляет обладателю информации возможность увеличения дохода, сохранения положения на рынке или получения иного коммерческого преимущества[19]. Такая возможность находится в плоскости извлечения выгоды, что облегчает задачу объяснения параметров действительной и потенциальной ценности.

---

[15] *Мансуров Г. З.* Коммерческая тайна как разновидность конфиденциальной информации // Проблемы современной науки и образования. 2014. № 4 (22). С. 69–71.

[16] *Сибел Т.* Указ. соч. С. 14.

[17] *Ганиева И. А.*, *Бобров Н. Е.* Цифровые платформы в сельском хозяйстве России: правовой аспект внедрения // Достижения науки и техники АПК. 2019. Т. 33. № 9. С. 83–86.

[18] *Хачатурян Г. Ю.* Институциональные основы экономической безопасности банковской деятельности в современной экономике // Вестник Университета. 2015. № 21. С. 15–22.

[19] *Езангина И. А.* Проблемы и тенденции развития инфраструктуры кредитных рынков в России // Экономическая безопасность России и стратегии развития ее регионов в современных условиях : сб. науч. трудов Междунар. научно-практ. конференции. Волгоград : Волгоград. гос. тех. ун-т, 2015. С. 67–70.

Цифровые технологии позволяют повысить ценность получаемых сведений с перспективой формирования рынка коммерчески значимой информации. Поскольку сведения, в отношении которых их обладатель установил режим коммерческой тайны, обладают действительной и потенциальной ценностью, а также вызывают интерес со стороны третьих лиц, то такие сведения могут быть предметом сделок по отчуждению. Определяемая по факту отсутствия доступа к сведениям со стороны третьих лиц ценность не перестает существовать при совершении с ними сделки. Ценность закрытых сведений переходит к новому обладателю, а старый обязуется не раскрывать их третьим лицам.

На данный момент можно говорить о наличии рынка продажи массивов данных[20], стоимость которых определяется пользой полученных после их переработки результатов для принятия разного рода решений[21]. Кроме того, благодаря технологиям big data и искусственного интеллекта со временем произойдет не только увеличение таких данных, но и рост объема сведений, в отношении которых будет установлен режим секретности. Тем самым субъекты предпринимательской деятельности могут стать не просто обладателями большого информационного продукта в виде массива данных, но и получат в управление особо ценный объект в больших объемах, который будет скрыт от третьих лиц.

Накопленные сведения будут подлежать сортировке по степени значимости для бизнеса компании и уровню их вовлеченности в ее деятельность. В определенный момент та или иная компания может столкнуться с необходимостью более качественного управления закрытой информацией, что может вызвать понижение значимости информации, ранее ценной для бизнеса, но при этом сохраняющей ту или иную ценность для рынка. Это может привести к целесообразному решению по продаже такой информации. И подобная тенденция будет усиливаться по мере развития цифровых технологий, что может привести к формированию рынка коммерчески значимой информации. В литературе уже закрепилось мнение о том, что информация в информационном обществе является новой нефтью[22].

Становление такого рынка потребует разрешения конфликтных ситуаций, в первую очередь обусловленных подтверждением прав на закрытую информацию за соответствующим владельцем. Его поддержание будет предполагать введение санкций за нарушение прав на закрытую информацию, механизм применения которых должен быть удобным и прозрачным. Описанные задачи могут быть решены аналогично правам на патенты, но без внедрения системы регистрации при помощи государственного органа. Реализация соответствующих решений возможна на базе технологии блокчейн.

Блокчейн представляет собой тип электронного регистра для записи данных о транзакциях, для которых большое значение имеют постоянное хранение и защита от несанкционированного доступа и изменений. Уже сейчас технология блокчейн получила распространение в разных сферах деятельности: логистике, патентовании, кибербезопасности, банковской сфере. Защита записей производится при помощи криптографических механизмов, которые позволяют ограничить доступ к сведениям и контролировать их целостность. Выделяемыми в литературе преимуществами технологии блокчейн по сравнению с другими технологиями являются:

— децентрализация (записи одновременно хранятся у каждого участника схемы, что исключает возможность уничтожения их цепочки);

— прозрачность (все транзакции может отследить любой участник системы);

— конфиденциальность;

— надежность (санкционированное изменение требует специального уникального кода, который выдается и подтверждается системой);

[20] Риски цифровизации: виды, характеристика, уголовно-правовая оценка. С. 45.

[21] *Вайгенд А.* Big data. Вся информация в одной книге / пер. с англ. С. Богданова. М. : Эксмо, 2021. С. 41.

[22] *Талапина Э. В.* Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. С. 5–17.

— достоверность (добавляемые в систему данные проверяются ее участниками)[23].

Предполагается, что продавец является обладателем коммерчески значимой информации, что позволяет ему предоставить гарантии в достоверности сведений и надлежащем обладателе, а также отсутствии фактов ее раскрытия таким обладателем. Покупатель, приобретая закрытую информацию, вносит сведения о ней в систему блокчейн, тем самым устанавливая свое право на информацию, если это не сделал продавец.

При очередной продаже новый обладатель, который выступает продавцом, предоставляет доступ к сведениям системы блокчейн, которые подтверждают его право на информацию. В дальнейшем цепочка записей увеличивается по мере смены обладателя.

Данный подход позволит в любой момент не только подтвердить свое право на закрытую информацию, но и доказать, что она получена на законных основаниях, если иное лицо уже обладает такой информацией. Если же иной субъект не опровергнет разумных сомнений в законности прав зарегистрированного обладателя, то приоритет в защите прав на закрытую информацию целесообразно отдать тому субъекту, права которого были внесены в систему блокчейн.

В настоящий момент можно говорить о том, что действие по получению закрытой информации не признается нарушающим права ее обладателя, если он не принял всех предусмотренных законом мер защиты. Депонирование коммерчески значимой информации позволит отойти от строго формального подхода, если соответствующее лицо докажет, что оно является обладателем такой информации, обозначило ее, не совершало действий по ее раскрытию, а третье лицо незаконным способом получило ее. Иными словами, любое получение коммерчески значимой информации, совершенное с умыслом, можно квалифицировать как действие, совершенное вне закона. Сходным образом можно поступить и с получением такой информации без умысла, когда лицо извлекает выгоду после того, как оно узнало или должно было узнать о ее извлечении за счет иного лица.

Технология блокчейн может позволить оптимизировать защитные мероприятия. Если действие по получению закрытой информации априори является противозаконным, то депонирование закрытых сведений при помощи блокчейн в любой момент позволит подтвердить права на такие сведения. Данный подход не устраняет обязанности обладателя обеспечивать защиту закрытых сведений, в чем он, разумеется, заинтересован.

Калькуляция убытков при раскрытии закрытой информации представляется достаточно сложной задачей[24], в особенности если речь идет о потенциальной ценности. Следовательно, обладатель коммерческих секретов в максимальной степени заинтересован обеспечить их защиту. Но судебная практика периодически демонстрирует в некотором роде формальный подход к пренебрежению обладателем мерами по защите коммерчески значимой информации.

В судебной практике можно найти примеры отказа во взыскании денежных средств за разглашение коммерческой тайны в случае неподтверждения факта внедрения режима коммерческой тайны[25]. Включение в договор общих параметров закрытой информации в виде сведений о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления не говорит о внедрении режима коммерческой тайны[26]. Формулировка «все условия договора являются коммерческой тайной» не только не подразумевает введение режима коммерческой тайны, но и может привести к признанию незаключенным положения договора о неразглашении конфиденциальной информации[27].

[23] Риски цифровизации: виды, характеристика, уголовно-правовая оценка. С. 46–48.

[24] Апелляционное определение Липецкого областного суда от 29.01.2020 по делу № 33-135/2020.

[25] Постановление Арбитражного суда Поволжского округа от 10.07.2012 по делу № А57-11021/2011.

[26] Постановление Арбитражного суда Северо-Западного округа от 29.10.2015 по делу № А56-72074/2014.

[27] Постановление ФАС Поволжского округа от 29.07.2013 по делу № А65-9864/2012.

При депонировании закрытой информации можно допустить общее информирование контрагента о введении режима коммерческой тайны, — вступая в договорную связь, он будет обязан воздержаться от действий по разглашению сведений, связанных с договором. Напротив, самим договором можно предусмотреть категории сведений, которые могут быть раскрыты. Такой подход не представляется затруднительным реализовать на практике, поскольку договор заключается между конкретными субъектами и, как правило, касается только их.

Депонирование сведений, составляющих режим коммерческой тайны, можно предусмотреть тогда в качестве обязательного действия, которое свидетельствует о введении такого режима. Иные предусмотренные законом мероприятия, направленные на информирование лиц, работающих с коммерческой тайной, исключать нецелесообразно.

Работники в любом случае должны иметь представление, что они допущены к сведениям, составляющим коммерческую тайну, а также должны понимать, что тот или иной документ составляет коммерческую тайну. Так, при рассмотрении одного из дел суд пришел к выводу, что режим коммерческой тайны не был установлен по двум причинам: отсутствие учета лиц, получивших доступ к коммерческим секретам; отсутствие грифа «Коммерческая тайна» на документах[28].

Но можно также допустить рассуждения о чрезмерности грифа «Коммерческая тайна» как элемента, являющегося обязательным для подтверждения факта введения режима коммерческой тайны. Если работник осведомлен о наличии секретной информации и получил допуск к ней, то он не вправе разглашать такую информацию. К тому же обладателем секретной информации является работодатель, и, соответственно, ее разглашение работником свидетельствует о распоряжении чужой информацией. Отсутствие грифа «Коммерческая тайна» не должно легализовывать такое незаконное распоряжение.

Указание на внесение сведений о секретной информации в систему блокчейн можно будет включить в трудовой договор или соглашение с работником как обязательный элемент режима коммерческой тайны. В качестве момента внедрения режима коммерческой тайны можно определить дату внесения соответствующих сведений в систему блокчейн. Можно допустить условную аналогию с патентными правами, когда объекты патентного права приобретают такой статус после получения охранного документа[29], выдаваемого по факту регистрации.

Действующее законодательство не содержит упоминания о конкретном моменте внедрения режима коммерческой тайны, приурочивая его к выполнению установленных законом мероприятий. В случае с регистрацией в системе блокчейн такой момент может быть определен, конечно, при условии выполнения иных мероприятий. Размышления об открытости параметров закрытых сведений в целях информирования третьих лиц выглядят на данном этапе развития законодательства революционными и без создания соответствующей инфраструктуры невыполнимыми.

Но такой подход в перспективе может развернуть законодательство о коммерческой тайне в сторону свидетельствования противозаконности любых действий по получению закрытых сведений в случае, если их обладатель проинформировал о введении режима коммерческой тайны, сообщив об этом работнику, контрагенту и внеся соответствующую запись в систему блокчейн. Так более наглядно раскрывается специфическая особенность права на сведения, составляющие коммерческую тайну, — фактическая монополия их обладателя на некоторую совокупность знаний[30]. Предлагаемая же законом в настоящий момент конструкция защиты позволяет

[28] Кассационное определение Верховного суда Удмуртской Республики от 25.05.2011 по делу № 33-1796/2011.

[29] *Судариков С. А.* Право интеллектуальной собственности : учебник. М. : Проспект, 2009. С. 141.

[30] *Сергеев А. П.* Право интеллектуальной собственности в Российской Федерации : учебник. 2-е изд., перераб. и доп. М. : ТК Велби, Проспект, 2004. С. 676.

нарушителю избежать ответственности, если он докажет, что обладатель информации не ввел в отношении нее режим коммерческой тайны, несмотря на то что любое умышленное действие третьего лица по получению такой информации уже образует правонарушение.

Описываемое широкое использование системы блокчейн может войти в конфликт со свободой получения информации и свободной конкуренцией. Но поскольку речь идет о закрытых сведениях, то сам обладатель должен быть заинтересован в их сохранности. Запись в системе блокчейн носит информационный характер, но не гарантирует защиту. Например, конкуренты, производящие сбор информации относительно обладателя закрытых сведений, благодаря записи в системе блокчейн будут считаться осведомленными о введении режима коммерческой тайны, и, соответственно, совершение умышленных действий в отношении тех или иных категорий сведений будет рассматриваться в качестве правонарушения.

В случае произведения записи в системе блокчейн сам по себе гриф «Коммерческая тайна» может выступать информирующим элементом, который позволяет сотрудникам и третьим лицам проявлять бóльшую бдительность и осторожность. Данная мера в большей степени направлена на помощь сотруднику. Но поскольку обладатель информации наиболее заинтересован в сохранении секретности, то он по своему выбору может внедрять элементы информирования и не только через описанный гриф. При этом в силу заинтересованности обладателя в сохранении секретности сложно представить его стремление спровоцировать сотрудника на разглашение отсутствием грифа «Коммерческая тайна».

В литературе встречается мнение, основанное на судебной практике, о том, что неразумная политика в отношении информационной безопасности может быть основанием отказа в защите прав обладателя в силу того, что он не проявил должной осмотрительности[31]. С другой стороны, закон[32] содержит требование о принятии разумно достаточных мер, называя ряд соответствующих параметров:

— исключение доступа к информации, составляющей коммерческую тайну, для любых лиц без согласия ее обладателя;

— обеспечение возможности использования указанной информации работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

Указанные параметры согласуются с требованием к работодателю о создании работнику необходимых условий для соблюдения им установленного режима коммерческой тайны, которое, в свою очередь, охватывается более широкой обязанностью работодателя по созданию работнику необходимых условий для сохранения имущества работодателя, нарушение которой служит основанием отказа в удовлетворении требований работодателя, если это явилось причиной возникновения ущерба[33].

Маневрирование работодателя между определенностью некоторых формальных процедур, которые подтверждают введение режима коммерческой тайны, и принятием разумно достаточных мер может быть сопряжено с недовольством, высказываемым сотрудниками, а иногда и акционерами относительно избыточного урегулирования и усложнения бизнес-процессов. Это всё влияет на мобильность бизнеса и замедляет его работу. К тому же создание чрезмерных барьеров может подтолкнуть работника к инициированию спора о признании незаконным установления режима коммерческой тайны по причине неразумных ограничений[34], в том числе при защите от требований работодателя.

---

[31] *Коровяковский Д. Г.* Защита коммерческой тайны предприятия: теоретические и практические аспекты // Юридический комментарий. 2006. № 3. С. 71–77.

[32] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 2004. № 32 Ст. 3283.

[33] Постановление Пленума Верховного Суда РФ от 16.11.2006 № 52 «О применении судами законодательства, регулирующего материальную ответственность работников за ущерб, причиненный работодателю» // Бюллетень Верховного Суда РФ. 2007. № 1.

[34] *Северин В. А.* Коммерческая тайна в России. 2-е изд., перераб. и доп. М. : Зерцало-М, 2009. С. 154–155.

При правовом регулировании резонно оттолкнуться от заинтересованности в сохранении коммерчески значимой информации, предусмотрев минимально необходимые мероприятия, свидетельствующие о режиме коммерческой тайны. Поскольку обладатель информации в принципе заинтересован в ее защите, то он должен самостоятельно разрабатывать мероприятия, которые позволят это осуществить. На первом месте должны стоять разъяснительная работа с сотрудниками и контрольные мероприятия, препятствующие разглашению коммерческой тайны.

Нанесение грифа «Коммерческая тайна» на материальные носители со временем будет утрачивать актуальность благодаря цифровизации, предусматривающей повсеместное внедрение электронного документооборота, что позволяет в структуру электронного документа включать упоминание о коммерческой тайне.

Цифровизация оказывает сильное влияние на условия ведения компаниями своей деятельности. Помимо удобства общения с органами власти в электроном виде, облегчения обмена документами с контрагентами, цифровизация выводит отношения между работодателем и работником на новый уровень. Работник может исполнять свою трудовую функцию вне места работы и рабочего места — не только дома, но и на любом месте. В итоге повышаются ожидания работодателя от работника в вопросе его более широкой доступности[35].

Цифровизация обостряет проблему защиты коммерческой тайны в особенности в отношениях с работниками. В литературе предлагается включать в трудовые договоры условия, определяющие порядок дистанционного взаимодействия сторон трудовых отношений[36]. При этом обеспечить надлежащую защиту коммерческой тайны при таком типе взаимодействия крайне проблематично, поскольку в отсутствие контроля работодателя к компьютеру работника может иметь доступ неограниченное число лиц. Выход в такой ситуации видится в комбинировании дистанционной работы с исполнением трудовой функции при работе с коммерческой тайной непосредственно в месте нахождения работодателя.

Проходящие процессы становления цифровой экономики позволяют сделать предположение о том, что в ближайшей временно́й перспективе можно будет увидеть своего рода переходный период. По мнению Томаса Сибела, организации не хотят отказываться от проверенных инструментов в пользу чего-то сомнительного и неопробованного и не внедряют новшества[37]. Но поскольку цифровые технологии всё больше и больше вовлекаются в предпринимательские отношения, то компании вынуждены будут задействовать их в своей деятельности в первую очередь в целях сохранения или улучшения конкурентных преимуществ.

Что касается коммерчески значимой информации, то можно ожидать не только увеличения ее объема, но и уточнение самих данных. Обладатель такой информации получит в свои руки значимые ресурсы, которые могут выступить также и в качестве товара по договору отчуждения. Участившиеся случаи вовлечения в оборот этой информации сформируют движение в направлении становления рынка закрытой информации, что потребует адекватной системы учета, например, на базе блокчейн.

Поступательное развитие цифровых технологий может создать предпосылки для пересмотра законодательного понимания коммерческой тайны. В любом случае благодаря данным технологиям институт коммерческой тайны получает стимулы для своего последующего развития с возможной переоценкой места в российском законодательстве.

Следует отметить значительный интерес государства в становлении цифровой экономики в нашей стране. Разрабатываемая им программа

[35] *Чесалина О. В.* Работа на основе интернет-платформ (crowdwork и work on demand via apps) как вызов трудовому и социальному праву // Трудовое право в России и за рубежом. 2017. № 1. С. 52–55.

[36] *Закалюжная Н. В.* Новая концепция занятости и развитие трудовых отношений в цифровую эпоху // Право. Журнал Высшей школы экономики. 2023. Т. 16. № 2. С. 139–164.

[37] *Сибел Т.* Указ. соч. С. 35.

«Экономика данных» ожидаемо предоставит действенные стимулы развития цифровой экономики, в основание которой будут заложены данные в большом объеме. Формирование новых экономических условий, с одной стороны, будет способствовать обнаружению коммерческими организациями конкурентных преимуществ, а с другой — может повлечь возможное увеличение числа случаев утечек коммерчески значимой информации. Последнее обусловлено ростом объема обрабатываемых данных, допускаемыми сотрудниками ошибками при работе с конфиденциальной информацией и совершенствованием методов кражи данных. Но увеличение количества утечек спровоцирует и без того высокий спрос на качественные решения по обеспечению информационной безопасности, а также на соответствующий персонал.

БИБЛИОГРАФИЯ

1. *Акмаров П. Б.*, *Газетдинов М. Х.*, *Третьякова Е. С.* Проблемы защиты коммерческой информации в условиях цифровизации экономики // Вестник Казанского государственного аграрного университета. — 2020. — Т. 15. — № 2. — С. 133–138.
2. *Вайгенд А.* Big data. Вся информация в одной книге / пер. с англ. С. Богданова. — М. : Эксмо, 2021. — 384 с.
3. *Вайпан В. А.* Правовое регулирование цифровой экономики // Предпринимательское право. Приложение «Право и бизнес». — 2018. — № 1.
4. *Ганиева И. А.*, *Бобров Н. Е.* Цифровые платформы в сельском хозяйстве России: правовой аспект внедрения // Достижения науки и техники АПК. — 2019. — Т. 33. — № 9. — С. 83–86.
5. *Езангина И. А.* Проблемы и тенденции развития инфраструктуры кредитных рынков в России // Экономическая безопасность России и стратегии развития ее регионов в современных условиях : сборник научных трудов Международной научно-практической конференции // Волгоград : Волгоградский государственный технический университет, 2015. — С. 67–70.
6. *Закалюжная Н. В.* Новая концепция занятости и развитие трудовых отношений в цифровую эпоху // Право. Журнал Высшей школы экономики. — 2023. — Т. 16. — № 2. — С. 139–164.
7. *Коровяковский Д. Г.* Защита коммерческой тайны предприятия: теоретические и практические аспекты // Юридический комментарий. — 2006. — № 3. — С. 71–77.
8. *Мансуров Г. З.* Коммерческая тайна как разновидность конфиденциальной информации // Проблемы современной науки и образования. — 2014. — № 4 (22). — С. 69–71.
9. Риски цифровизации: виды, характеристика, уголовно-правовая оценка : монография / отв. ред. Ю. В. Грачева. — М. : Проспект, 2022. — 272 с.
10. *Северин В. А.* Коммерческая тайна в России. — 2-е изд., перераб. и доп. — М. : Зерцало-М, 2009. — 472 с.
11. *Северин В. А.* Правовая работа в организациях высокотехнологичного комплекса. — М. : Ленанд, 2022. — 264 с. (Основы защиты информации. № 21.)
12. *Семякин М. Н.* Гражданско-правовой договор в сфере цифровой экономики: теоретический и практический аспекты исследования // Экономическое правосудие в Уральском округе. — 2020. — № 1. — С. 98–114.
13. *Сергеев А. П.* Право интеллектуальной собственности в Российской Федерации : учебник. — 2-е изд., перераб. и доп. — М. : ТК Велби, Проспект, 2004. — 752 с.
14. *Сибел Т.* Цифровая трансформация. Как выжить и преуспеть в новую эпоху / пер. с англ. Ю. Гиматова ; науч. ред. М. Савицкий, К. Щеглова, К. Пахорукова. — М. : Манн, Иванов и Фербер, 2021. — 256 с.
15. *Судариков С. А.* Право интеллектуальной собственности : учебник. — М. : Проспект, 2009. — 368 с.
16. *Талапина Э. В.* Право и цифровизация: новые вызовы и перспективы // Журнал российского права. — 2018. — № 2. — С. 5–17.

17. *Хачатурян Г. Ю.* Институциональные основы экономической безопасности банковской деятельности в современной экономике // Вестник Университета. — 2015. — № 21. — С. 15–22.
18. *Чесалина О. В.* Работа на основе интернет-платформ (crowdwork и work on demand via apps) как вызов трудовому и социальному праву // Трудовое право в России и за рубежом. — 2017. — № 1. — С. 52–55.

Материал поступил в редакцию 20 февраля 2024 г.

REFERENCES (TRANSLITERATION)

1. Akmarov P. B., Gazetdinov M. Kh., Tretyakova E. S. Problemy zashchity kommercheskoy informatsii v usloviyakh tsifrovizatsii ekonomiki // Vestnik Kazanskogo gosudarstvennogo agrarnogo universiteta. — 2020. — T. 15. — № 2. — S. 133–138.
2. Vaygend A. Big data. Vsya informatsiya v odnoy knige / per. s angl. S. Bogdanova. — M.: Eksmo, 2021. — 384 s.
3. Vaypan V. A. Pravovoe regulirovanie tsifrovoy ekonomiki // Predprinimatelskoe pravo. Prilozhenie «Pravo i biznes». — 2018. — № 1.
4. Ganieva I. A., Bobrov N. E. Tsifrovye platformy v selskom khozyaystve Rossii: pravovoy aspekt vnedreniya // Dostizheniya nauki i tekhniki APK. — 2019. — T. 33. — № 9. — S. 83–86.
5. Ezangina I. A. Problemy i tendentsii razvitiya infrastruktury kreditnykh rynkov v Rossii // Ekonomicheskaya bezopasnost Rossii i strategii razvitiya ee regionov v sovremennykh usloviyakh: sbornik nauchnykh trudov Mezhdunarodnoy nauchno-prakticheskoy konferentsii // Volgograd: Volgogradskiy gosudarstvennyy tekhnicheskiy universitet, 2015. — S. 67–70.
6. Zakalyuzhnaya N. V. Novaya kontseptsiya zanyatosti i razvitie trudovykh otnosheniy v tsifrovuyu epokhu // Pravo. Zhurnal Vysshey shkoly ekonomiki. — 2023. — T. 16. — № 2. — S. 139–164.
7. Korovyakovskiy D. G. Zashchita kommercheskoy tayny predpriyatiya: teoreticheskie i prakticheskie aspekty // Yuridicheskiy kommentariy. — 2006. — № 3. — S. 71–77.
8. Mansurov G. Z. Kommercheskaya tayna kak raznovidnost konfidentsialnoy informatsii // Problemy sovremennoy nauki i obrazovaniya. — 2014. — № 4 (22). — S. 69–71.
9. Riski tsifrovizatsii: vidy, kharakteristika, ugolovno-pravovaya otsenka: monografiya / otv. red. Yu. V. Gracheva. — M.: Prospekt, 2022. — 272 s.
10. Severin V. A. Kommercheskaya tayna v Rossii. — 2-e izd., pererab. i dop. — M.: Zertsalo-M, 2009. — 472 s.
11. Severin V. A. Pravovaya rabota v organizatsiyakh vysokotekhnologichnogo kompleksa. — M.: Lenand, 2022. — 264 s. (Osnovy zashchity informatsii. № 21.)
12. Semyakin M. N. Grazhdansko-pravovoy dogovor v sfere tsifrovoy ekonomiki: teoreticheskiy i prakticheskiy aspekty issledovaniya // Ekonomicheskoe pravosudie v Uralskom okruge. — 2020. — № 1. — S. 98–114.
13. Sergeev A. P. Pravo intellektualnoy sobstvennosti v Rossiyskoy Federatsii: uchebnik. — 2-e izd., pererab. i dop. — M.: TK Velbi, Prospekt, 2004. — 752 s.
14. Sibel T. Tsifrovaya transformatsiya. Kak vyzhit i preuspet v novuyu epokhu / per. s angl. Yu. Gimatova; nauch. red. M. Savitskiy, K. Shcheglova, K. Pakhorukova. — M.: Mann, Ivanov i Ferber, 2021. — 256 s.
15. Sudarikov S. A. Pravo intellektualnoy sobstvennosti: uchebnik. — M.: Prospekt, 2009. — 368 s.
16. Talapina E. V. Pravo i tsifrovizatsiya: novye vyzovy i perspektivy // Zhurnal rossiyskogo prava. — 2018. — № 2. — S. 5–17.
17. Khachaturyan G. Yu. Institutsionalnye osnovy ekonomicheskoy bezopasnosti bankovskoy deyatelnosti v sovremennoy ekonomike // Vestnik Universiteta. — 2015. — № 21. — S. 15–22.
18. Chesalina O. V. Rabota na osnove internet-platform (crowdwork i work on demand via apps) kak vyzov trudovomu i sotsialnomu pravu // Trudovoe pravo v Rossii i za rubezhom. — 2017. — № 1. — S. 52–55.