

ПРОБЛЕМЫ ПРАВОВОЙ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ БИЗНЕСА



И. А. Дюсов, студент
E-mail: dyusov.ilya@inbox.ru
ФГБОУ ВО «Северо-Восточный государственный университет»

А. Р. Баласанян, к. ю. н., доц.
E-mail: balasakan@mail.ru
ФГБОУ ВО «Северо-Восточный государственный университет»

В настоящей статье рассматриваются актуальные проблемы правоприменения и защиты коммерческой тайны в контексте стремительной цифровизации бизнес-процессов. Особое внимание уделено вызовам, с которыми сталкиваются компании при обеспечении конфиденциальности данных в условиях широкого распространения цифровых технологий, включая инсайдерские угрозы и усложнение процесса доказывания фактов разглашения. Проанализированы существующие пробелы в законодательстве Российской Федерации и предложены направления его совершенствования, в том числе с учетом международного опыта. Рассмотрены аспекты, связанные с необходимостью развития правовых механизмов сбора и оценки цифровых доказательств, а также важностью формирования комплексных мер безопасности внутри организаций, включающих технические, организационные и правовые компоненты. Приведены примеры из судебной практики, иллюстрирующие сложности в защите коммерческой тайны в цифровой среде, и обозначены пути решения выявленных проблем для обеспечения устойчивого развития бизнеса.

Ключевые слова: *коммерческая тайна, цифровая трансформация, защита информации, конфиденциальность, правовое регулирование, цифровые доказательства, инсайдерские угрозы, законодательство, информационная безопасность, утечка данных.*

ВВЕДЕНИЕ

В наш век стремительного развития информационных технологий, когда каждое предприятие стремится к цифровой трансформации, вопросы защиты коммерческой тайны приобретают особую остроту. Автоматизация, перевод информации в электронный формат, облачные технологии – все это, несомненно, повышает эффективность бизнеса, но и создает новые лазейки для тех, кто стремится завладеть ценными сведениями. Коммерческая тайна, будучи невидимым, но ценнейшим активом, сегодня подвергается беспрецедентным угрозам. Традиционные подходы к ее защите зачастую оказываются неэффективными перед лицом цифровых вызовов. Правовая система сталкивается с необходимостью не только адаптировать существующие нормы, но и разрабатывать новые, более совершенные механизмы охраны. Данная статья посвящена анализу актуальных проблем, возникающих при обеспечении правовой защиты коммерческой тайны в условиях повсеместной цифровизации бизнес-процессов, и поиску путей их решения.

ОБЪЕКТ ИССЛЕДОВАНИЯ

Объектом данной статьи выступают общественные отношения, возникающие в процессе формирования, использования и защиты коммерческой тайны в условиях активного внедрения цифровых технологий в предпринимательскую деятельность. Кроме того, анали-

зируются правовые нормы, призванные регулировать эти отношения, и их адекватность современным требованиям.

ЦЕЛЬ И ЗАДАЧИ ИССЛЕДОВАНИЯ

Основная цель настоящей статьи – всесторонне проанализировать ключевые правовые барьеры и предложить практические пути их преодоления для обеспечения надежной защиты коммерческой тайны в условиях цифровой трансформации бизнеса. Для достижения этой цели были поставлены следующие задачи:

- Определить специфику коммерческой тайны как объекта правовой защиты в контексте повсеместного использования цифровых технологий.
- Проанализировать действующее российское законодательство, регулирующее вопросы коммерческой тайны, на предмет его соответствия современным реалиям.
- Выявить основные угрозы и риски, связанные с несанкционированным доступом к коммерческой тайне и ее разглашением в цифровой среде.
- Исследовать сложности, возникающие при фиксации фактов нарушения режима коммерческой тайны и оценке причиненного ущерба в цифровом пространстве.
- Оценить роль инсайдерских угроз в общем контексте защиты коммерческой тайны в условиях повсеместной цифровизации.
- Изучить международный опыт правового регулирования защиты коммерческой тайны и возможности его применения в Российской Федерации.
- Сформулировать ряд рекомендаций, направленных на повышение эффективности правовой защиты коммерческой тайны в условиях растущей цифровизации.

В результате проведенного анализа было показано, что цифровая трансформация бизнеса, подразумевающая повсеместное внедрение информационных технологий, несет в себе как значительные преимущества, так и новые, куда более сложные вызовы для обеспечения конфиденциальности ценной информации. Если раньше основные угрозы исходили от физического проникновения или подкупа сотрудников, то сегодня на первый план выходят кибератаки, утечки через цифровые каналы и несанкционированный доступ к данным [10, 12].

МЕТОДЫ ИССЛЕДОВАНИЯ

Для достижения поставленных целей и решения обозначенных задач в данной статье были задействованы общенаучные методы познания, а также специфические подходы, применимые к юридической науке. Ими являлись анализ и синтез, использованные для изучения обширного пласта нормативных правовых актов, научной литературы, материалов судебной практики, а также для выявления взаимосвязей между различными аспектами рассматриваемой проблемы. Сравнительно-правовой метод позволил сопоставить российское законодательство с зарубежными аналогами, выявив наиболее эффективные решения. Системный подход способствовал рассмотрению проблемы в ее комплексности, принимая во внимание взаимосвязь правовых, технических и организационных аспектов. Формально-юридический метод был применен для точного толкования норм действующего законодательства. Отдельные аспекты были проанализированы с использованием статистических данных, помогающих оценить масштабы проблемы и наметить тенденции.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Цифровизация бизнеса, как активно развивающийся процесс, несомненно, открывает новые горизонты для оптимизации и роста, но вместе с тем порождает и целый комплекс проблем, связанных с защитой сведений, составляющих коммерческую тайну. Если ранее основным инструментом злоумышленников были кражи физических носителей информации или подкуп сотрудников, то сегодня главный удар приходится из киберпространства [10]. Основные угрозы проявляются в виде сложных кибератак, инсайдерских утечек через разнообразные цифровые каналы, а также несанкционированного доступа к информации, зачастую осуществляемого с использованием анонимных инструментов [8].

Одной из ключевых проблем на сегодняшний день является определенная неадекватность действующего законодательства современным реалиям. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», будучи краеугольным камнем в этой области, зачастую содержит слишком общие положения, которые не всегда позволяют эффективно разрешать специфические проблемы, присущие цифровой среде. Например, понятие «конфиденциальность информации» трактуется достаточно широко, что создает трудности с его доказыванием, особенно в тех случаях, когда информация, находясь в открытом доступе в сети Интернет, требует выполнения определенных условий для получения доступа [1, 7].

Сложности возникают и на этапе выявления самого факта нарушения режима коммерческой тайны. В цифровом пространстве информация может быть моментально скопирована, изменена или даже уничтожена, зачастую оставаясь незамеченной для владельца. Определение личности злоумышленника, особенно при его анонимной деятельности или использовании внешних, зачастую зарубежных, серверов, становится весьма затруднительной задачей. Это, в свою очередь, усложняет процесс установления размера причиненного ущерба. Классические методы оценки убытков, такие как упущенная выгода или прямые потери, не всегда применимы в ситуациях, когда, например, конкуренты получают доступ к уникальному технологическому процессу или инновационной разработке [12].

Инсайдерские угрозы продолжают оставаться одними из наиболее опасных рисков. Сотрудники, имеющие законный доступ к конфиденциальной информации, могут намеренно или по неосторожности разгласить ее заинтересованным третьим лицам. С развитием мобильных технологий, облачных сервисов и различных мессенджеров возможности для такого рода утечек значительно расширились. По данным ряда экспертов, до 70 % всех утечек конфиденциальной информации происходят именно по вине инсайдеров [10]. Важно отметить, что даже случайная неосторожность, например, оставленная без присмотра включенная рабочая станция, может привести к компрометации ценных данных.

Технические аспекты защиты информации приобретают первостепенное значение. Шифрование данных, строгое управление доступом, своевременное обновление программного обеспечения, использование антивирусных систем и межсетевых экранов – это базовые кирпичики надежной обороны. Особое место в этой системе занимают системы предотвращения утечек данных (DLP – Data Loss Prevention), которые становятся неотъемлемой частью арсенала компаний, серьезно относящихся к контролю над перемещением конфиденциальной информации [2]. Современные DLP-системы позволяют не только блокировать передачу данных по запрещенным каналам, но и анализировать контент, выявляя попытки несанкционированного копирования или передачи [8].

Международный опыт показывает, что многие юрисдикции активно работают над обновлением своего законодательства с учетом цифровых реалий. Так, Директива (ЕС) 2016/943 Европейского парламента и Совета направлена на гармонизацию правовых норм в области защиты коммерческой тайны в Европейском союзе, предлагая более четкие определения и совершенствуя механизмы защиты [2]. Отдельные положения данной директивы, в частности касающиеся определения коммерческой тайны и мер ответственности за ее разглашение, могли бы стать ценным ориентиром для российских законодателей [6].

Судебная практика в России демонстрирует определенную, хотя и не всегда последовательную динамику в решении вопросов, связанных с цифровыми доказательствами. В одном из дел, которое детально рассматривалось в судебных инстанциях, предметом спора стало незаконное использование производственной схемы, полученной путем копирования данных с корпоративного сервера. В качестве доказательств были представлены логи доступа к серверу, записи с камер видеонаблюдения, а также заключение эксперта в области компьютерной криминалистики, которое подтвердило факт несанкционированного копирования. Суд, признав представленные доказательства достаточными для установления вины, привлек ответственное лицо к установленной законом ответственности [4].

Несмотря на положительные примеры, существует множество случаев, когда отсутствие четких правил сбора и оценки цифровых доказательств, а также недостаточная квали-

фикация экспертов, выступающих в суде, существенно затрудняют вынесение справедливого и обоснованного решения [5].

Приведем еще один показательный пример. В одной из фармацевтических компаний произошла утечка конфиденциальной информации, касающейся формулы нового, еще не запатентованного лекарственного препарата. Это событие привело к появлению на рынке большого количества контрафактной продукции, что нанесло компании серьезный ущерб. В ходе расследования выяснилось, что утечка произошла через личный аккаунт электронной почты одного из научных сотрудников, куда им были скопированы отдельные фрагменты исследовательской документации. Несмотря на очевидность факта утечки, установить точный момент ее совершения, а также полный объем разглашенной информации, не говоря уже о прямой выгоде, полученной конкурентами, оказалось крайне затруднительно. Это обстоятельство существенно повлияло на размер взыскиваемой судом компенсации [2, 4, 9].

В условиях стремительно развивающихся цифровых технологий разглашение коммерческой тайны может происходить практически мгновенно и иметь глобальный охват. Это требует от бизнес-сообщества и государственных органов не только превентивных мер, но и способности к быстрой и адекватной реакции. Осознание существующих рисков и формирование внутри компании внутренней культуры информационной безопасности становится не менее важным, чем внедрение передовых технических средств защиты [2, 5]. Это включает в себя регулярное проведение аудитов безопасности, тренингов для сотрудников по вопросам защиты конфиденциальной информации, а также разработку четких регламентов и инструкций по работе с чувствительными данными [3]. Вследствие этого для эффективного противодействия цифровым угрозам компаниям необходимо иметь комплексную стратегию безопасности. Эта стратегия должна включать в себя:

- Технические средства защиты, такие как современные системы шифрования, межсетевые экраны, DLP-системы.
- Организационные меры, включая разработку и внедрение политик конфиденциальности, обучение персонала, проведение регулярных внутренних проверок.
- Правовые механизмы, обеспечивающие возможность защиты прав в случае нарушения режима коммерческой тайны, включая грамотно составленные договоры с сотрудниками и контрагентами.

Важным аспектом является также развитие законодательства в области цифровых доказательств. Принятие специальных законов или внесение изменений в действующие процессуальные кодексы, определяющих порядок сбора, фиксации и оценки цифровых доказательств, могло бы существенно упростить доказывание фактов нарушения режима коммерческой тайны в суде.

ЗАКЛЮЧЕНИЕ

Цифровизация бизнес-процессов, несомненно, является прогрессивным трендом, открывающим для компаний беспрецедентные возможности для развития и оптимизации. Однако эта трансформация одновременно порождает новые, зачастую весьма сложные вызовы для обеспечения конфиденциальности ценнейших активов, среди которых коммерческая тайна занимает одно из ведущих мест. В условиях растущей цифровой уязвимости этот актив постоянно подвергается разнообразным угрозам.

Проведенный анализ показал, что действующая в Российской Федерации правовая база, хотя и закладывает необходимый фундамент для защиты коммерческой тайны, все же требует существенной доработки и адаптации с учетом специфики и стремительного развития цифровых технологий. Проблематика, связанная с идентификацией нарушений, точным доказыванием факта разглашения и корректной оценкой размера причиненного ущерба в цифровом пространстве, остается одной из наиболее острых. Инсайдерские угрозы, многократно усиленные доступностью современных средств коммуникации, продолжают представлять серьезную опасность для конфиденциальности информации.

В итоге для обеспечения адекватной защиты коммерческой тайны в современной цифровой среде, необходим комплексный, многоуровневый подход. Прежде всего актуальной задачей является дальнейшее совершенствование законодательства. Это должно включать в себя более детальное регулирование норм, касающихся защиты данных в цифровых системах, а также расширение перечня мер ответственности, применяемых к нарушителям. Изучение и, при целесообразности, адаптация успешных международных практик, таких как положения европейской Директивы 2016/943, могут стать ценным ориентиром в этом процессе [2, 6].

Кроме того, ключевая роль в обеспечении защиты принадлежит самим компаниям. Инвестиции должны направляться не только в передовые технические средства защиты – современные DLP-системы, надежное шифрование, но и в разработку, а главное, в строгое соблюдение внутренних политик конфиденциальности. Не менее важно регулярное обучение персонала, формирование устойчивой культуры строгой конфиденциальности.

Судебные и правоохранительные органы также нуждаются в адаптации к новым реалиям, развитии специализированной экспертизы в области компьютерной криминалистики и совершенствовании методов сбора и оценки цифровых доказательств. Работа с цифровыми уликами требует не только технических знаний, но и понимания специфики правового регулирования.

Следовательно, только синергия адекватного правового регулирования, внедрения современных технологических решений и формирования внутри компаний глубокой культуры строгой конфиденциальности позволит минимизировать риски, связанные с разглашением коммерческой тайны, и обеспечить устойчивое развитие бизнеса в динамично меняющемся цифровом мире.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (с послед. изм.) // СПС «КонсультантПлюс».
2. Директива (ЕС) 2016/943 Европейского парламента и Совета от 8 июня 2016 г. «О защите нераскрытых ноу-хау и деловой информации (коммерческой тайны)» // Официальный журнал Европейского Союза, L 157, 15 июня 2016 г. – С. 1–18.
3. Емельянов, С. В. Проблемы правового регулирования ответственности за использование коммерческой тайны / С. В. Емельянов // Хозяйство и право. – 2018. – № 9. – С. 56–62.
4. Малиновский, А. А. Гражданско-правовая охрана способов производства и коммерческой тайны / А. А. Малиновский. – Москва: Статут, 2019. – 304 с.
5. Новиков, А. С. Актуальные проблемы защиты коммерческой тайны в России / А. С. Новиков // Вестник Московского университета. Серия 11: Право. – 2019. – № 3. – С. 88–95.
6. Петров, А. Н. Инсайдерские угрозы и защита коммерческой тайны в современных условиях / А. Н. Петров // Право и бизнес. – 2020. – № 2. – С. 45–50.
7. Попов, И. В. Правовые режимы конфиденциальной информации / И. В. Попов. – Москва: Инфра-М, 2021. – 240 с.
8. Румак, А. А. Киберпреступность и методы борьбы с ней / А. А. Румак, И. П. Иванов. – Москва: Юнити-Дана, 2018. – 320 с.
9. Свердлов, А. А. Ответственность за разглашение коммерческой тайны / А. А. Свердлов // Российский судья. – 2019. – № 6. – С. 30–34.
10. Сидоров, А. В. Цифровизация бизнеса: новые вызовы для правовой защиты / А. В. Сидоров // Экономика и право. – 2022. – № 1. – С. 100–105.
11. Соколов, А. А. Коммерческая тайна в Российской Федерации: понятие, содержание, правовая охрана / А. А. Соколов. – Москва: Волтерс Клувер, 2016. – 320 с.
12. Цифровое право: учебник / под ред. Б. Н. Гонгалло. – Москва: Статут, 2020. – 784 с.

LEGAL PROTECTION OF BUSINESS SECRETS IN CONDITIONS OF DIGITALIZATION OF BUSINESS

I. A. Dyusov, student
E-mail: dyusov.ilya@inbox.ru
North-Eastern State University

A. R. Balasanyan, Candidate of Science (Law), Associate Professor
E-mail: balasakan@mail.ru
North-Eastern State University

This article discusses current issues of law enforcement and protection of commercial secrets in the context of the rapid digitalization of business processes. Special attention is paid to the challenges faced by companies in ensuring data confidentiality in the context of the widespread use of digital technologies, including insider threats and the complexity of proving the facts of disclosure. The article analyzes the existing gaps in the legislation of the Russian Federation and proposes some ways to improve it, taking into account international experience. It also discusses aspects related to the need to develop legal mechanisms for collecting and evaluating digital evidence, as well as to the importance of implementing comprehensive security measures within organizations, which include technical, organizational, and legal components. It provides examples from judicial practice that illustrate the challenges in protecting commercial secrets in the digital environment, and suggests solutions to address these issues in order to ensure sustainable business development.

Keywords: *commercial secrets, digital transformation, information protection, confidentiality, legal regulation, digital evidence, insider threats, legislation, information security, and data leakage.*