МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»
Институт права
(наименование института полностью)

Кафедра «Предпринимательское и трудовое право»
(наименование)

40.04.01 Юриспруденция
(код и наименование направления подготовки)

Правовое обеспечение предпринимательской деятельности
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему Информация с ограниченным доступом в предпринимательской деятельности: правовой аспект

Студент Д.Н. Игнатова
(И.О. Фамилия) (личная подпись)

Научный руководитель кандидат педагогических наук, доцент О.А. Воробьёва
(ученая степень, звание, И.О. Фамилия)

Тольятти 2021

Оглавление

Введение

В связи с развитием технологий, в последние двадцать лет, многие жители планеты, а также граждане Российской Федерации, стали активно использовать современные технологии в процессе жизнедеятельности.

Основным объектом использования информационных технологий, является информация.

Информации в современном мире существует огромное количество, и чаще всего она связана с передачей через технические каналы связи. Неисчисляемый оборот информации в современном мире, установил необходимость правового регулирования данной сферы деятельности.

Развитие социальных сетей, различных сайтов, а также технологическое изменение предоставления различных государственных и муниципальных услуг, обязывают государство обеспечить охрану и защиту персональных данных, как обособленной разновидности информации, которая чаще всего может стать объектом преступного умысла, либо иных действий направленных против его владельца.

Глобализационные и интеграционные процессы XXI века существенно повлияли на использование информационных технологий в процессе реализации коммерческих отношений.

В цивилизованном обществе любая отрасль деятельности нуждается в правовом регулировании.

В России для информационной сферы в настоящее время базовым выступает Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [12]. Статьей 2 данного закона информация определяется как сведения (сообщения, данные) независимо от формы их представления.

Несмотря на неограниченный оборот информации в рамках существующих общественных отношений, действующее российское

законодательство определило круг информации, которая имеет ограниченный доступ.

В сфере предпринимательской деятельности, также существует информация, которая может быть ограничена участниками такой деятельности в целях сохранения и повышения эффективности используемой бизнес модели. В условиях рыночной конкуренции, получение информации конкурентами может способствовать неблагоприятному положению компании на рынке, что может вовсе привести такую компанию к краху.

Информация, ограниченная в доступе, которая используется в коммерческой деятельности, способствует тому, чтобы третьи лица не могли без согласия владельца информации осуществлять её передачу, хранение, распространение и иные действия, которые будут способствовать нарушению режима коммерческой тайны.

Помимо коммерческой тайны, в рамках предпринимательской деятельности существуют иные режимы ограничения информации, которые чаще всего связаны со щепетильностью такого рода информации, в случае её распространения. Наиболее часто встречаемыми видами такой информации является налоговая информация и банковская информация, для охраны которой также существует специальный режим ограничения, установленный законом.

Актуальность работы заключается в том, что в эпоху информационных технологий, использование информации в процессе предпринимательской деятельности является в некоторых случаях сопутствующим, либо основным фактором получения прибыли, что определяет необходимость ограниченного использования некоторых сведений в предпринимательской деятельности.

Степень разработанности темы исследования является достаточно высокой и встречается в работах таких авторов как С.С. Алексеева; И.А. Близнеца, М.М. Богуславского, В.В. Витрянского, А.В. Власовой, Э.П. Гаврилова', В.П. Грибанова, В.А. Дозорцева, И.А. Зенина, В.И. Еременко,

О.С. Иоффе, В.М. Каневского, В.О. Калятина, А.В. Коломийца, А.Я. Курбатова, В.А. Лапача, М.Н. Малеиной, Д.И. Мейера, К.П. Победоносцева.

Объект исследования общественные отношения в сфере ограниченного оборота информации.

Предмет исследования общественные отношения в сфере правового регулирования информации, с ограниченным доступом используемой в предпринимательской деятельности.

Цель исследования изучить правовой аспект регулирования информации, с ограниченным доступом используемой в предпринимательской деятельности.

Задачи исследования:

- определить понятие и значение информации;

- изучить право человека на информацию: содержание, соотношение с правом на доступ к информации;

- определить понятие «информации с ограниченным доступом» и её значением в регулировании общественных отношений;

- определить правовое регулирование информации с ограниченным доступом;

- изучить понятие и значение банковской, налоговой и коммерческой тайны;

- определить порядок предоставления доступа к сведениям, составляющим, банковскую, налоговую и коммерческую тайны;

- изучить порядок охраны сведений, составляющих банковскую, налоговую и коммерческую тайны.

Методологическая основа исследования составляют общенаучные методы познания (диалектический метод, методы индукции, дедукции, анализа,, синтеза) и частнонаучные методы познания (системный, логический, исторический, и формально-юридический методы).

Нормативно-правовая основа исследования состоит из Конституции РФ, Гражданского кодекса РФ, Налогового кодекса РФ, ФЗ «Об информации,

информационных технологиях и о защите информации», ФЗ «О коммерческой тайне» и других нормативных правовых актов в сфере оборота информации связанной с предпринимательской деятельностью.

Теоретическими основами исследования являются работы, в которых рассмотрены аспекты гражданско-правового режима информации (В.М. Богданов, М.С. Зельцер, А.Г. Картяшян, В.А. Северин, И.И. Салихов), а также к диссертационным исследованиям, посвященным непосредственно информации с ограниченным доступом З.Ф. Гайнуллиной, О.В. Добрынина, И.В. Строганова, А.А. Клишина, И.Ю. Мирских, Е.В. Шишмаревой.

Научная новизна исследования заключается в том, что автором было проведено подробное исследование проблематики оборота информации ограниченного доступа, которая используется в предпринимательской деятельности.

Положения, выносимые на защиту:

- Информация ограниченного доступа в первую очередь закрепляется в различных нормативных правовых актов. Условия ограничения доступа к таким сведениям определяется в зависимости от конкретного вида правоотношений. Следует отметить, что в различных правоотношениях могут встречаться смешенные виды тайн, которые могут находиться на стыке различных нормативных актов. В предпринимательской деятельности, ограничение информации осуществляется в целях сохранения определенных позиций на рынке для недопущения потери конкурентного преимущества, что способствует развитию и процветанию субъектов предпринимательской деятельности.

- Административный контроль, который в большей степени не является оправданным, также не способствует развитию информационного обеспечения компаний, что также заставляет владельцев и управляющий корпораций принимать меры по защите информации, вне существующих правовых концепций,

- Предусмотренный подход законодателя в Гражданском кодексе РФ, по вопросу того, что информация с ограниченным доступом, составляющая коммерческую тайну, выступает объектом единого исключительного права, считаем, является неверным. Поскольку происходит необоснованное смешение исключительного права и права, гарантирующего обладателю такой информацией, защиту от третьих лиц (право на конфиденциальность информации), которое необходимо рассматривать в качестве самостоятельного интеллектуального права,

- «Деловая конфиденциальная информация» в отличие от «секрета производства» не должна признаваться объектом исключительных прав. За обладателем такой информации должно закрепляться только право на конфиденциальность информации,

- Предлагается законодательное закрепление применения гражданско-правовой ответственности к нарушителю права на коммерческую тайну путем возложения на нарушителя — обязанности по выплате денежной компенсации обладателю информации, составляющей коммерческую тайну. Кроме того, законодательно внести пределы такой денежной компенсации для определения судом размера выплаты в случае невозможности точной оценки объема причиненных обладателю такой информации убытков.

Структура работы состоит из введения, трех глав, восьми параграфов, заключения и списка используемой литературы и используемых источников.

Глава 1. Общая характеристика информации

1.1 Понятие и значение информации

Право на информацию появилось относительно недавно, по отношению с иными видами прав человека. В первую очередь появление права на информацию, связано с существенным увеличением объемов различной информации в рамках общественных отношений, что вызвало последующую необходимость их правового регулирования, как в рамках национальных правовых систем, так и в рамках международного права.

Основным объектом отношений в сфере права на информацию, является информация, которая в зависимости от точек зрения и формулировок имеет разное значение.

Информацию следует рассматривать в качестве разрешения вопросов неопределенности. Информация формируется в обществе путем наделения определенных сущностей и явлений соответствующими характеристиками, которые проистекают из рамок восприятия окружающего мира.

Понятие информации имеет разное значение в разных контекстах.

«Информация связана с данными, поскольку данные представляют собой значения, приписываемые параметрам, а информация - это данные в контексте и со смыслом. Информация также относится к знаниям, поскольку знание означает понимание абстрактного или конкретного понятия» [3].

«С точки зрения коммуникации информация выражается либо в виде содержания сообщения, либо посредством прямого или косвенного наблюдения. То, что воспринимается, может быть истолковано как сообщение само по себе, и в этом смысле информация всегда передается как содержание сообщения» [3].

Человек, будучи существом, исключительно субъективного восприятия любой окружающей действительности, волен интерпретировать эту действительность, исключительно в рамках своего уровня понимания

происходящих событий. В момент приема, обработки, хранения и последующей передачи определенных наборов данных, формируется конкретный объем информации об объекте, предмете, явлениях, категориях, которые до этого были объектом изучения человека.

То есть в данном случае интерпретирует, как сам носитель образа, так и те люди которые воспринимают его поведение. И в том и другом случае результаты такого восприятия, а также оценка поведения субъекта, будут являться индивидуальными.

Любые формы объективного толкования окружающей действительности, связаны с призмой субъективной оценки такой действительности. А формирование субъективных черт осмысления, связано с воздействием объективных факторов. Информация является в данном случае результатом соприкосновения объективного и субъективного, то что позволяет обеспечить взаимодействие между субъектом и окружающим его миром.

Каждый из нас, будучи наблюдателем происходящих вокруг событий, а порою и участником таких событий, склонен оценивать такие события не с позиции того что происходит, либо произошло, а с позиции того, как он это видит.

Информация, полученная таким образом, формируется в рамках представлений и системы оценки именно конкретного человека. Дальнейшая интерпретация, также происходит исходя из субъективных представлений человека [40].

Психика человека, будучи абсолютно индивидуальной, не может сформировать обобщенного подхода к одинаковой оценки окружающей реальности. Поэтому различность, многообразие количества информации зависит от того, сколько человек осуществляют обработку этой информации.

Любое осмысление предполагает набор определенных характеристик. Мозг, в данном случае можно сравнить с компьютером. Если у компьютера, не достаточные технические характеристики, то некоторые процессы,

которые хотелось бы на нем произвести, становятся просто не доступными для этого. Аналогично и с осмыслением, если интеллектуальный, образовательный, житейский уровень не позволяет человеку произвести наиболее приближенную оценку своих действий и окружающей обстановки, то следует говорить о том, что такая оценка является ошибочной и не верной, с позиции общепризнанности.

Информация, является таковой только тогда, когда она общепризнанна в рамках общества. Для этого, любой информационный элемент, общество структурирует, осмысливает, теоретически оформляет и практически использует.

При условии повышенного потока информации – менее усваивается при индивидуальном восприятии того или иного события. Будучи образом, человек осуществляющий жизнедеятельность, склонен оценивать все с позиции своего собственного опыта. Образ, будучи создан в качестве художественного, идеализированного произведения, весьма проблематичен для восприятия, в тех ситуациях, когда человек (субъект восприятия) контактирует с объектом образа в реальности.

Образ, сам по себе, это проекция той информации, которая формулируется в рамках человеческого восприятия. Соответственно, информация категория динамическая.

Информация может быть закодирована в различных формах для передачи и интерпретации (например, информация может быть закодирована в последовательности из признаков, или передается через сигнал). Она также может быть зашифрован для безопасного хранения и связи.

Неопределенность события измеряется вероятностью его возникновения и обратно пропорциональна ей. Чем более неопределенным является событие, тем больше информации требуется для разрешения неопределенности этого события.

«Информация может относиться, к изменению внешнего мира, и в этом случае она была определена как «различие, которое имеет значение», то есть

оперативное изменение, вызванное внешним миром в системе наблюдения» [50].

«Это может также относиться, инвертируя порядок этого отношения, к процессу нахождения различий - информации как различия, которое находит различие - и в этом случае система стимулируется различием во внешнем мире» [50].

С одной стороны, информация - это вещь, с другой - психическая конструкция. Информация как различие в реальности - как нечто существующее независимо от наблюдателя - кажется, это точка зрения на информацию в инженерии и естественных науках, хотя, как мы видели, это не всегда так. Это было одним из следствий исключения Шенноном семантических и прагматических аспектов повседневного использования слова « информация».

«Существующая в гуманитарных науках понятие «информации» сохраняет основной аспект современной концепции информации в смысле передачи знаний, а именно отбор. Имея дело со смыслом сообщения, человек обсуждает интерпретацию - то есть выбор между семантическими и прагматическими возможностями» [34].

Интерпретировать сообщение означает, другими словами, ввести перспективу приемника - убеждения и желания, сделать получателя информации активным партнером в информационном процессе.

«Бар-Гиллель указал на «семантические ловушки» терминологии Шеннона, особенно в отношении аналогий между психологической и инженерной полями. Бар-Хиллель и Карнап разработали семантическую теорию информации, в которой они проводят различие между информацией и объемом информации в рамках лингвистической структуры. Теория семантической информации Дрецке основана на различении информации и значения. Информация не требует интерпретирующего процесса, хотя это необходимое условие для получения знаний» [34].

Активная фиксация информации различного рода начала происходить с XIX века, когда в период индустриальной революции возникли первые средства фиксации визуальной и звуковой информации [51].

«Первые разработки для хранения данных были первоначально основаны на фотографиях, начиная с микрофотографии в 1851 году, а затем с микроформ в 1920-х годах, с возможностью хранения документов на пленке, что сделало их намного более компактными. Ранняя теория информации и коды Хэмминга были разработаны примерно в 1950 году, но ожидали, что технические инновации в передаче и хранении данных будут использованы в полной мере» [49].

В процессе расширения применения и оборота информации, люди стали регулировать её оборот в рамках систем правового регулирования.

Информация, в качестве объекта информационных правоотношений, обладает рядом специфических черт и свойств. Хотя закон и устанавливает четкое определение «информации», необходимо понимать, что данное в законе определение не может раскрыть всю сущность данного явления.

Информационные правоотношения не могут быть выражены в чистом виде. Они взаимосвязаны с различными иными правоотношениями, соответственно данная позиция является доводом к тому, что информационное право по своей сути, является комплексной отраслью права, и существует лишь при реализации иных правоотношений, в которых в качестве объекта фигурирует информация.

Исходя из всего выше сказанного, информация как понятие имеет много значений. Концепция информации тесно связана с понятиями ограничения, коммуникации, контроля, данных, формы, инструкции, знания, значения, умственного стимула, паттерна, восприятия и представления. В самом ограниченном техническом смысле информация - это упорядоченная последовательность символов.

Каждое живое существо обрабатывает информацию постольку, поскольку оно использует (внутренние или внешние) датчики для

обнаружения своего состояния или окружающей среды, и использует результаты этого процесса обнаружения либо сразу, либо после дальнейшей обработки информации для выбора из поведенческого репертуара, в котором поведение может быть внешне видимое физическое поведение или обработка новой информации. В процессе использования информации он также расходует накопленную энергию, поэтому ему также необходимо использовать информацию для получения большего количества энергии.

Существуют огромные различия между различными способами использования информации организмами, включая растения, одноклеточные организмы и все остальное.

В национальной правовой доктрине «информация» имеет более практическое значение, так как основное применение данного термина требуется в рамках регулируемых правоотношений.

Информация представляет собой, определенный объем данных, который передается между субъектами. Определение информации имеет нормативное закрепление, которое является очень важным для правоотношений связанных с информацией.

В соответствии с пунктом 1 статьи 2 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации» (далее – ФЗ № 149-ФЗ), под информацией понимается, сведения (сообщения, данные) независимо от формы их представления.

Информация на сегодняшнем этапе технического развития, может быть выражена в абсолютно любой форме, а следовательно её правовое регулирование, а также теоретические и научные разработки в сфере правового регулирования информационных правоотношений, должны соответствовать техническим новшествам и разработкам.

Таким образом, понятие «информации» является всеобъемлющим и в зависимости от конкретной ситуации и интерпретации может иметь разное значение. В аспекте правового регулирования, отношений содержащих

информационные аспекты, следует прибегать к нормативному толкованию данного термина, так как в национальной правовой системе понятие «информации» имеет правовое закрепление.

Основное значение информации заключается в передачи между субъектами информационного взаимодействия различных сведений, которые могут быть абсолютно любыми. Право на получение информации, обязанности по предоставлению той или иной информации, ограничения оборота какой-либо информации являются определенной формой отношений с конкретными видами информации и в зависимости от требований закона подлежат определенной правовой форме регулирования.

1.2 Право человека на информацию: содержание, соотношение с правом на доступ к информации

Право на информацию, как основная категория, формулирующая основы правоотношений, в рамках которых существует информация, в первую очередь связано с тем, что субъект имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

Нормативные правовые акты, которые являются источником права для иных отраслей права, устанавливают необходимость предоставления информации в определенных законом случаях. Так для регистрации юридического лица, учредители должны предоставить некоторое количество информации о себе, об организации, а также о видах деятельности, которые создаваемая организация планирует осуществлять. В данном случае в рамках административных правоотношений, информация является обязательным условием их реализации и не создает каких-либо информационных правоотношений.

Процессы информатизации в рамках различных правоотношений, приводят к тому, что отношения в сфере использования информации,

составляют предмет информационного права и регулируются нормами информационного законодательства.

Определить содержание создаваемых правоотношений можно лишь постепенно, с учетом объективных факторов, которые влияют на создаваемые процессы.

Право информации базируется на такой категории, как свобода информации.

Под свободой информации, следует понимать свободу человека или людей публиковать и потреблять информацию.

В некоторых государствах (например Великобритания) свобода информации является расширенной производной от свободы слово, которое относится к фундаментальным правам человека.

Право на информацию связано со свободой выражения мнений, которая может применяться к любым средствам массовой информации, будь то устные, письменные, печатные, электронные или художественные формы.

Помимо этого, человек имеет право потреблять все возможную информацию, которая есть в открытом доступе и на которую не наложены ограничения закона.

Свобода информации - это отдельное понятие, которое иногда вступает в противоречие с правом на неприкосновенность частной жизни в контексте использования Интернета и информационных технологий.

Как и право на свободу выражения мнения, право на неприкосновенность частной жизни является признанным правом человека, и свободу информации, также можно рассматривать с позиции расширения этого правомочия по своему объему.

Свобода информации (или свобода информации) также относится к защите права на свободу выражения мнения в отношении Интернета и информационных технологий.

Свобода информации также может касаться цензуры в контексте информационных технологий, то есть возможности доступа к веб-контенту без цензуры или ограничений.

Право на доступ к информации основывается на принципе, согласно которому общественность имеет право знать, как осуществляется власть и расходуются государственные деньги, учитывая, что государственные органы избираются людьми и поддерживаются налогоплательщиками.

«Доступ к публичной информации является предварительным условием подотчетности правительств и государственных должностных лиц и позволяет гражданам принимать обоснованные решения, следовательно, представляет собой фундаментальный элемент для надлежащего функционирования демократических систем» [31].

Международные стандарты и развивающаяся судебная практика подтвердили, что информация, находящаяся в распоряжении государственных органов, принадлежит общественности.

Конвенция Совета Европы о доступе к официальным документам(2009) заявляет, что «все официальные документы в принципе являются общедоступными и могут быть отказаны в предоставлении только при условии защиты других прав и законных интересов».

Более 100 стран по всему миру уже приняли национальные законы о доступе к информации, чтобы определить законный доступ граждан к информации.

В Российской Федерации, основой регулирования вопросов частной жизни, а также персональных данных является Конституция Российской Федерации [3], которая в своих положениях закрепляет, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Основой для закрепления данных положений, является Всеобщая декларация прав человека, провозглашенная Генеральной Ассамблеей Организации Объединенных Наций в 1948 г [1]. Согласно ст. 12 этого документа «никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь произвольным посягательством на его честь и репутацию». Положения Декларации получили своё дальнейшее развитие в других международно-правовых документах и документах Европейского союза, в частности в принятой 4 декабря 1950 г. Европейской конвенции о защите прав человека и основных свобод [2].

Основным нормативно-правовым актом, регулирующим использование и охрану персональных данных, является Федеральный закон «О персональных данных».

Данное положение, подтверждает, статья 4 Федерального закона «О персональных данных», законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из настоящего Федерального закона и других определяющих случаи и особенности обработки персональных данных федеральных законов.

На основании и во исполнение федеральных законов государственные органы в пределах своих полномочий могут принимать нормативные правовые акты по отдельным вопросам, касающимся обработки персональных данных. Нормативные правовые акты по отдельным вопросам, касающимся обработки персональных данных, не могут содержать положения, ограничивающие права субъектов персональных данных. Указанные нормативные правовые акты подлежат официальному опубликованию, за исключением нормативных правовых актов или отдельных положений таких нормативных правовых актов, содержащих сведения, доступ к которым ограничен федеральными законами.

Свобода информации не гарантирует доступа к ней. Даже если бы правительства стали образцом обнародования информации с помощью

электронного управления, размещая свою информацию в сети, без средств доступа к этой информации люди не имели бы возможностей с ней ознакомиться.

Подключение к Интернету и ИТ-ресурсы стали критически важными для беспрепятственного доступа к информации. Это также верно для доступа к национальным или международным новостным ресурсам. Если отсутствие подключения или оборудования может высветить цифровой разрыв и связанный с этим разрыв в знаниях, разделяющий развивающиеся и развитые страны, группы внутри страны также могут стать еще более маргинализованными из-за их неспособности получить доступ к информации в Интернете [42].

Нельзя недооценивать важность доступа к технологиям и инфраструктуре, которых по-прежнему остро не хватает во многих частях мира. Что могут фактически означать понятия «цифровая революция» или «информационное общество» для 80% населения мира, у которого все еще нет доступа к основным средствам электросвязи, или примерно для 860 миллионов неграмотных людей, или для 2 миллиардов жителей планеты у кого еще нет электричества.

Исходя из этого, право на информацию и свободу информации следует рассматривать в качестве взаимозависимых элементов, тогда как доступ к информации, является иной категорией, основной смысл которой заключается в том, что право на доступ к информации, в первую очередь касается публичной информации неограниченного доступа государственных и международных органов власти. То есть право на информацию у субъекта есть по рождению, а вот право на доступ к информации может отсутствовать. Так, ограничен доступ к сведениям, составляющим государственную тайну государств.

Развитие социальных сетей, различных сайтов, а также технологическое изменение предоставления различных государственных и муниципальных услуг, обязывают государство обеспечить охрану и защиту

персональных данных, как обособленной разновидности информации, которая чаще всего может стать объектом преступного умысла, либо иных действий направленных против его владельца [48].

Помимо расширения достаточно большого количества информации в открытом доступе, существует некоторый вид информации, которые закрыты для большинства граждан. Такая информация является особенной не только в силу того что она скрывается, но и в силу того, что содержание этой информации имеет огромную значимость для государства и общества.

Таким образом, право на информацию – это сформулированное в национальных и международных правовых актах право человека на свободный поиск, получение, передачу, производство и распространение информации любым законным способом.

Право на доступ к информации – это право человека на получение публичной и частной информации публичного характера, в рамках требований закона государства.

1.3 Понятие информации с ограниченным доступом и её значение в регулировании общественных отношений

Несмотря на важность доступа людей к различной информации, в рамках каждой конкретной правовой системы существует «информация ограниченного доступа», основным признаком которой является ограниченность субъектов вовлеченных в оборот информации.

В контексте рассмотрения «информации с ограниченным доступом», следует разделить всю возможную информацию на два вида:

- общедоступная информация;
- информация с ограниченным доступом.

И ту и другую информацию, определяют таковой с позиции её нормативного закрепления. Например, сведения составляющая государственную тайну относится к информации ограниченного доступа,

тогда как, информация о состоянии окружающей среды является общедоступной и не может быть ограничена.

Основное различие двух этих видов информации проистекает в круге потенциальных пользователей такой информации. Общедоступная информация доступна неограниченному кругу лиц, тогда как информация ограниченного доступа может использоваться только в рамках определенной группы, которая определяет законом, договором, либо иной формой правового закрепления её оборота.

Оборот ограниченной информации регулируется не общими правилами об обороте информации, а специальными нормативными актами в сфере такой информации.

Информация ограниченного доступа обладает следующими признаками:

- сведения не доступны широкому кругу лиц и такая информация не является общеизвестной;

- сведения могут распространяться только в рамках определенных участников по правилам, которые регулируют оборот такой информации;

- владелец информации, а также пользователи обязаны принимать определенные меры для ограничения распространения информации ограниченного доступа;

- сведения ограниченного доступа обладают определенной ценностью для лиц, определяющих её таковой;

- информация ограниченного доступа, при определении её таковой, должна соответствовать требованиям законодательства определяемых для такого вида информации.

Основным требования к информации ограниченного доступа является требование, связанное с неизвестностью такой информации для широкого круга лиц.

Общеизвестная информация некоем образом не может быть ограничена, в силу объективных факторов, а ограничение ряда

общеизвестной информации может иметь негативные последствия, в виде привлечения к ответственности, лиц ответственных за ограничение общеизвестной информации.

С правовой точки зрения, общеизвестная информация квалифицируется в качестве «общедоступной информации». Так, в статье 7 ФЗ № 149-ФЗ, содержится перечень общедоступной информации, оборот которой не может быть ограничен.

К такой информации относится общеизвестная информация, и сведения доступ к которой не ограничен.

В соответствии со статьей 10 ФЗ № 149-ФЗ, к информации доступ к которой ограничить нельзя, относятся:

- нормативные правовые акты, которые затрагивают права и свободы человека и гражданина, определяющие правовой статус организаций, органов государственной и муниципальной власти;

- сведения о состоянии окружающей среды;

- сведения о деятельности государственных и муниципальных органов власти;

- сведения, составляющие культурное достояние, которые хранятся в различных культурных учреждениях и информационных системах организованных в целях предоставления этой информации неограниченному кругу лиц;

- сведения, которые в соответствии с федеральным законодательством не могут подлежать какому-либо ограничению.

Последний вид общедоступной информации определяется в рамках какой-либо специфической деятельности, в рамках которой информация не может быть ограничена в силу специфики такой деятельности, например информация о благотворительных, некоммерческих организациях и иные сведения.

Круг информации ограниченного доступа в рамках национальной правовой системы весьма обширный и составляет собой перечень сведений,

который формируется из различных областей регулируемых правоотношений.

Рассмотрим виды информации ограниченного доступа, более подробно.

1) Сведения, составляющие государственную тайну. Являются наиболее охраняемой информацией ограниченного доступа, распространение которой привлечет к уголовной ответственности. Правовое регулирование информации, составляющей государственную тайну закреплены в положениях Закона РФ от 21 июля 1993 г. № 5485-I «О государственной тайне».

Сведения, составляющие государственную тайну, являются сведения, которые защищаются государством в сфере военной, внешнеполитической, экономической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, распространение которых может нанести ущерб государству.

«Сведения, которые составляют государственную тайну, подразделяются на четыре блока:

- сведения в военной области;

- сведения в области экономики, науки и техники;

- сведения в области внешней политики и экономики;

- сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, в области противодействия терроризму и обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты» [27].

Данный федеральный закон, является обязательным для исполнения и соблюдения на территории России, а также за её пределами органами различных ветвей власти.

Помимо государственных органов власти, соблюдать и исполнять нормы, закрепленные в данной федеральном законе, обязаны организации, которые в соответствии с законодательством Российской Федерации

осуществляют государственное управление в установленной сфере деятельности, а также органы местного самоуправления.

Так же положения данного законы, должны соблюдать различные предприятия, учреждения и организации вне зависимости от их организационно-правовой формы и формы собственности, а также должностные лица и граждане Российской Федерации, которые взяли на себя обязательства, либо в соответствии со своим статусом, обязаны исполнять требования законодательства о государственной тайне.

В соответствии со статьей 3 ФЗ «О государственной тайне», законодательство Российской Федерации о государственной тайне основывается на следующих нормативно-правовых актах:

- Конституция Российской Федерации;

- Федеральный закон «О безопасности» [13];

- Федеральный закон «О государственной тайне»;

- Федеральный закон «Об оперативно-розыскной деятельности» [14].

- иные законодательные акты, различных государственных органов о защите государственной тайны.

2) Конфиденциальная информация. Данные виды информации ограниченного доступа перечислены в рамках Указа Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера» [24]. К конфиденциальной информации в соответствии с этим указом можно отнести:

- персональные данные;

- тайну следствия, судопроизводства и меры государственной защиты;

- сведения, составляющие служебную тайну;

- сведения, доступ к которым ограничен в связи с профессиональной тайной;

- сведения, составляющие коммерческую тайну;

- секрет производства.

Представленный перечень конфиденциальной информации является наиболее структурированным в рамках системы информации ограниченного доступа.

Помимо нормативного закрепления представленной информации в рамках Указа Президента № 188 от 06.03.1997, в нормативных правых актах содержаться положения, которые касаются иных видов тайн, которые относятся к информации ограниченного доступа.

Помимо этого важно понимать, что определенные виды тайн, могут соприкасаться друг с другом в рамках конкретных общественных отношений. Так, врачебная тайна может являться персональными данными лица, а банковская тайна относится к конфиденциальной информации коммерческой организации (в случаях предусмотренных законом).

Рассмотрим подробнее различные виды тайн, которые предусмотрены положениями нормативных актов Российской Федерации. Данная классификация является в большей степени теоретической и структура классификации зависит от автора, который её дает. Наиболее относимой к данному исследованию является классификация тайн предложенная А. Лукацким.

1) Коммерческая тайна. Коммерческая тайна регулируется Федеральным законом от 29.07.2004 № 98-ФЗ (ред. от 18.04.2018) «О коммерческой тайне». Данные сведения более всего относятся к предпринимательской деятельности и связаны с информацией, которая в рамках такой деятельности присутствует.

К коммерческой тайне, в соответствии с действующим законом, относится информация производственного, технического, экономического и организационного характера, которая имеет определенную коммерческую ценность. В данном контексте, под коммерческой ценностью, следует понимать информацию, которая способствует получению прибыли и является основой формой её генерации. Коммерческая тайна не известна третьим лицам и охраняется в рамках нормативных актов корпорации.

Оборот информации составляющей коммерческую тайну в рамках корпорации осуществляется на основании федеральных законов и внутренних нормативных актов корпораций. Однако, стоит отметить, что некоторые виды информации, которые косвенно, по первому признаку можно отнести к сведениям составляющим коммерческую тайну, к таковой могут не относится на основании иных нормативных правовых актов. Так, ФЗ «Об акционерных обществах» [16], содержит перечень информации, которая не может быть ограничена даже для третьих лиц, хотя косвенно и является некой основой связанной с деятельностью акционерных обществ.

2) Банковская тайна. Банковская тайна также относится к видам информации ограниченного доступа, использование которой регламентируется ФЗ «О банках и банковской деятельности» [17].

К банковской тайне, в соответствии с данным нормативным правовым актом, относятся сведения об операциях, счетах, вкладах клиентов кредитных организаций и корреспондентов, а также иные сведения, которые в соответствии с внутренними документами банков относятся к банковской тайне.

Помимо данного нормативного акта, правовое регулирование банковской тайны осуществляется на основании Гражданского кодекса Российской Федерации (далее – ГК РФ) [4], Таможенного кодекса ЕАЭС (далее – ТК ЕАЭС) [6].

По мнению ряда теоретиков, в число которых входит А.В. Щепотьев [55], к одной из разновидностей банковских тайн можно отнести тайну кредитных историй, которая установлена ФЗ «О кредитных историях» [20].

Информация, которая относится к тайне кредитных историй представляет собой сведения о кредитных обязательствах заемщика, которые были взяты им на основании договора займа (кредита) и храниться в бюро кредитных историй.

3) Служебная тайна. К служебной тайне относятся сведения, доступ к которым ограничен органами государственной власти Российской Федерации

в соответствии с действующим законодательством. Основным источником ограничения такой информации является ФЗ «О государственной гражданской службе в РФ» [21], Постановление Правительства РФ от 3.11.1994 г. № 1233 [25].

4) Тайна страхования. В соответствии со статьей 946 ГК РФ сведения об участниках страховых правоотношениях, о состоянии здоровья, имущественном положении застрахованных лиц относятся к тайне страхования.

5) Тайна завещания. В соответствии со статьей 1123 ГК РФ [5], является информацией, которая касается содержания завещания, а также различных действий связанных с завещанием.

6) Налоговая тайна. Налоговая тайна состоит из сведений, которые уполномоченные налоговым законодательством органы могут получать от налогоплательщика. Налоговая тайна регулируется Налоговым кодексом Российской Федерации (далее – НК РФ) [7],

6) Тайна усыновления ребенка. Данный вид тайны регулируется Семейным кодексом Российской Федерации (далее – СК РФ) [7] и заключается в неразглашении сведений полученных в процессе усыновления ребенка. Лица, которые осведомлены о процессе усыновления ребенка не имеют права разглашать эти сведения.

7) Врачебная тайна. К данному виду тайны относятся сведения, которые получены в рамках медицинской деятельности и связаны с состоянием жизни и здоровья граждан.

К врачебной тайне можно отнести следующую информацию ограниченного доступа:

- сведения о психическом здоровье человека,

- сведения об обращении гражданина в медицинскую организацию.

8) Тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Данный вид тайн является конституционным, а также повторно детализируется в ряде федеральных нормативных правовых актов.

Несмотря на это, федеральное законодательство также дает легальную возможность не исполнять данное право граждан в рамках осуществления оперативно-розыскной деятельности и расследования преступлений.

Под специальными техническими средствами для негласного получения информации (далее СТС НПИ) следует понимать технические устройства перехвата информации с иных носителей. Особую роль СТС НПИ играют в борьбе с преступность, осуществлением и соблюдением национальной безопасности в Российской Федерации.

Основными субъектами, которые используют СТС НПИ, являются правоохранительные органы, осуществляющие оперативно-розыскную деятельность,

9) Право частной жизни (личная тайна). Является фундаментальным правом человеком и регулируется рядом международных и национальных нормативных правовых актов,

10) Аудиторская тайна. Аудит, термин, который является не только юридическим, но и экономическим. С позиции юридической терминологии аудит, можно описать как некий процесс реализации определенных правоотношений, который установлены в рамках законодательного акта.

Аудит, подразумевает под собой проведение определенной проверки, процедуры проведения сверки и анализа отчетности организации.

Под аудиторской проверкой, понимается процедура независимой проверки и оценки отчетности, данных проводимого учета, а также непосредственной деятельности организации.

На практике, зачастую основным объектом аудиторской проверки, является бухгалтерская отчетность, которая в наиболее поной мере содержит информацию, касающуюся состояния хозяйственных условий организации.

Помимо этого, на сегодняшний день, существует множество различных вариантов аудиторской проверки, которая осуществляет не только в целях изучения бухгалтерской отчетности. Аудиторская проверка, может проводиться, в качестве аудита операционного управлении, аудита

технического оборудования и устройств, аудит экологической обстановки организации и иные виды аудита, которые имеют четкое целевое назначение.

Информация, полученная в результате такой проверки, является информацией ограниченного доступа.

11) Тайна судопроизводства (тайна следствия). В соответствии с рядом национальный процессуальных нормативных правовых актов, информация, полученная в рамках какого-либо судопроизводства не может подлежать разглашению. Более всего данный вид тайны относится к сведениям, которые получены в результате предварительного расследования преступлений.

12) Адвокатская тайна. Данный вид тайны тоже отчасти относится к конкретному виду судопроизводства, однако в большей степени связан с адвокатской деятельностью и регламентируются ФЗ «Об адвокатской деятельности и адвокатуре» [22]. К адвокатской тайне в соответствии с данным федеральным законом относятся любые сведении, которые связаны с оказанием адвокатом юридической помощи своему доверителю.

13) Тайна нотариальных действий. Основы законодательства о нотариате [18] закрепляют обязанность за нотариусом хранить в тайне те сведения, которые получены им в результате осуществления нотариальной деятельности. В случаях, когда в отношении нотариуса возбуждено уголовное дело, суд может освободить нотариуса от обязанности соблюдать нотариальную тайну. Помимо самих нотариусов обязанность хранить в тайне сведения, полученные в результате нотариальных действий, также лежит на помощников нотариусов, а также представителей палат нотариусов субъектов Российской Федерации.

14) Тайна исповеди. Данный вид тайны в большей степени относиться к принципу свободы совести и обязывает сотрудников религиозных организаций хранить в тайне сведения, полученные ими в результате проведения исповеди в религиозном учреждении. Порядок сохранения тайны исповеди предусмотрен ФЗ «О свободе совести и о религиозных объединениях» [19]. Также одной из разновидностей религиозных тайн,

является тайна вероисповедания, которая предоставляет человеку право не сообщать третьим лицам информацию о его религиозной принадлежности.

15) Тайна голосования. Тайна голосования является базовым принципом реализации избирательных прав граждан и предусматривает право на оставление в тайне сведений о голосовании. В частном случае, такое право реализуется в качестве несообщения третьим лицам фактах о том, за кого проголосовал избиратель. Право на тайное голосование регулируется рядом нормативных правовых актов в сфере избирательного процесса.

16) Журналистская тайна. Данный вид тайны предусмотрен ФЗ «О средствах массовой информации» [23]. В соответствии с положениями данного нормативного акта, редакция СМИ не вправе разглашать информацию, полученную в результате осуществления ими своей профессиональной деятельности, если лицо предоставившее информации, желает не сообщать о себе данных. В данном случае речь идет прежде всего о тех ситуациях, в рамках которых лицо предоставляющее информацию в СМИ желает сохранить данные о себе в тайне.

Представленные виды информации ограниченного доступа не являются окончательными. При анализе ряда нормативных правовых актов, а также отраслей российской системы права, можно обнаружить огромное количество различной информации, которая будет подлежать ограниченному доступу, как на основании закона, так и по договоренности между участниками конкретных правоотношений.

Подобное количество информации, имеющей ограниченный доступ, является необходимым условием функционирования ряда правоотношений, в рамках которой ограничение информации является основной целью субъектов отношений.

В рамках предпринимательской деятельности, из перечисленного количества информации ограниченного доступа, наиболее часто встречается коммерческая тайна, банковская тайна, налоговая тайна, а также тайны

связанные с судопроизводством, если субъект предпринимательской деятельности является и субъектом процессуальных отношений.

Таким образом, информация ограниченного доступа в первую очередь закрепляется в различных нормативных правовых актов. Условия ограничения доступа к таким сведениям определяется в зависимости от конкретного вида правоотношений. Следует отметить, что в различных правоотношениях могут встречаться смешенные виды тайн, которые могут находиться на стыке различных нормативных актов. В предпринимательской деятельности, ограничение информации осуществляется в целях сохранения определенных позиций на рынке для недопущения потери конкурентного преимущества, что способствует развитию и процветанию субъектов предпринимательской деятельности.

Глава 2. Информация с ограниченным доступом

2.1 Информация, с ограниченным доступом используемая в предпринимательской деятельности

Определив всевозможные виды тайн, а также определив, что представляет собой информация, следует исследовать вопрос о том, какая информация в рамках предпринимательской деятельности относится к ограниченной в обороте, а какая нет.

Основным видом тайны в рамках предпринимательской деятельности является коммерческая тайна, которая фактически содержит в себе информацию, способствующую осуществлению предпринимательской деятельности и получению прибыли.

Как уже было отмечено в предыдущей главе, коммерческая тайна в Российской Федерации регулируется Федеральным законом от 29.07.2004 № 98-ФЗ (ред. от 18.04.2018) «О коммерческой тайне».

Коммерческая тайна - это информация, содержащая сведения о технологии или процессах компании, которые обычно не известны за её пределами. Информация, считающаяся коммерческой тайной, дает компании рыночное преимущество перед ее конкурентами и часто является продуктом внутренних исследований и разработок.

Коммерческие тайны могут различаться в разных юрисдикциях, но имеют три общих черты: не являются публичными, предлагают некоторую экономическую выгоду и активно защищаются.

В Российской Федерации на сегодняшний день отсутствует объективный подход к защите коммерческой информации. Объективный подход означает публичный характер правового регулирования коммерческой тайны, контроль и надзор государственных органов власти за её соблюдением и охраной.

По сути, на сегодняшний день установления и последующая защита коммерческой тайны в рамках предпринимательской деятельности является инициативой самих организаций, которые устанавливают и определяют порядок доступа, оборота и охраны коммерчески важной информации.

Коммерческая тайна может принимать различные формы, такие как проприетарный процесс, инструмент, образец, дизайн, формула, рецепт, метод или практика, которые не очевидны для других и могут использоваться как средство для создания предприятия, предлагающего преимущества, по сравнению с конкурентами или обеспечивает ценность для клиентов.

В соответствии с законодательством о коммерческой тайне, в статье 5 определен перечень видов информации, которые не могут быть ограничены в рамках данного правового режима.

К информации ограничение доступа, к которой невозможно, относится:

- сведения, содержащиеся в учредительных документах юридических лиц и индивидуальных предпринимателей, которые подлежат внесению в ЕГРЮЛ и ЕГРИП;

- документы, дающие право на осуществление некоторых видов предпринимательской деятельности (в первую очередь речь идет о лицензиях, разрешениях и т.п.);

- сведения о составе имущества организаций, созданных публично-правовыми образованиями;

- сведения общественного характера, которые включают информацию об окружающей среде, пожарной безопасности, эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и иной информации, которая прямо или косвенно может влиять на жизнь и здоровье человека и гражданина;

- о численности сотрудников, условиях труда, а также о сведениях, составляющих систему охрану труда в организации;

- сведения о задолженности по выплатам заработной платы и социальных обязательств;

- информация о нарушениях законодательства Российской Федерации о фактах привлечения к различным видам ответственности;

- сведения об условиях приватизации, аукционов объем государственной и муниципальной собственности;

- сведения о размерах, структуре, имуществе, расходах, численности, вопросов оплаты труда, использования безвозмездного труда граждан некоммерческих организаций;

- сведения о лицах, которые имеют право выступать от имени юридического лица без доверенности;

- сведения ограничить доступ, к которым в соответствии с федеральным законодательством – нельзя [35].

Коммерческая тайна определяется по-разному в зависимости от юрисдикции, но все они имеют следующие общие характеристики:

- это не общедоступная информация;

- их секретность обеспечивает их владельцу экономическую выгоду;

- тайна активно охраняется.

Если владелец коммерческой тайны не может защитить тайну или если тайна независимо от принимаемых мер обнаруживается, раскрывается или становится общеизвестной, защита информации нарушается.

Как конфиденциальная информация (поскольку коммерческие секреты известны в некоторых юрисдикциях), коммерческие секреты являются «секретными документами» делового мира, точно так же, как сверхсекретные документы строго охраняются государственными органами.

Поскольку стоимость разработки определенных продуктов и процессов намного дороже, чем конкурентная разведка, у компаний есть стимул выяснить, что делает их конкурентов успешными. Для защиты своей коммерческой тайны компания может потребовать от сотрудников, обладающих информацией, подписать соглашения о недопущении конкуренции или неразглашении информации при приеме на работу.

Способ производства продукта или ингредиенты, входящие в его состав, даже списки клиентов, могут быть защищены как коммерческая тайна.

Исходные коды компьютерных программ и формула Кока-колы являются общими примерами коммерческой тайны. Важнейшее требование защиты коммерческой тайны заключается в сохранении тайны. Открытые для общественности методы или информация не могут быть защищены законом о коммерческой тайне.

Как и в случае с компьютерными преступлениями, защита коммерческих секретов и другой конфиденциальной информации во многом является делом здравого смысла. Первое, что нужно сделать, это определить свои коммерческие секреты, то есть чертить круг информации, которая дает конкурентное преимущество на рынке. Сюда входит любая информация, которую используют компании для ведения своего бизнеса, которую руководство организации считает достаточно ценной - и достаточно секретной - чтобы дать вам преимущество перед конкурентами.

После того, компания провела аудит своих коммерческих секретов, ей необходимо настроить политику для установления порядка защиты коммерческой тайны.

Следует выделить следующие этапы и подходы для установления порядка защиты коммерческой тайны:

- Следует установить ограниченный доступ к обороту информации, таким образом, чтобы её носителя знали о связанных с ней ограничениями. Следует сообщить партнерам, клиентам, поставщикам и сотрудникам, имеющим право пользования коммерческой информацией, о том, что материал является конфиденциальным.

От указанных лиц следует получить согласие на неиспользование информации против компании и не разглашать кому-либо эту информацию, без письменного разрешения руководства компании. В подобных ситуациях

составляет соглашение о конфиденциальности и не разглашении информации составляющей коммерческую тайну.

- Меры безопасности. Следует установить определенную систему безопасности, которая может позволить ограничить возможность распространения информации ограниченного пользования. Например, можно использовать идентификационные значки сотрудников и посетителей, чтобы контролировать доступ к вашему бизнесу. Установить правила, требующие от людей подписывать конфиденциальные документы и исполнять их.

Установить пароли, для использования доступа к компьютерам, копировальным аппаратам, факсимильным аппаратам и другим машинам, которые могут использоваться для копирования или передачи секретов.

Когда сотрудники покидают рабочее место, следует применить меры, направленные на то, чтобы секреты не ушли с ними [44].

Компании, располагающие обширными данными о потребителях, рецептами продуктов питания или передовыми исследованиями и анализом рынка, хотят быть уверенными, что конкуренты не получат доступ к этой информации. Этот тип конфиденциальной информации (интеллектуальная собственность) обычно не защищен патентами, товарными знаками, промышленными образцами или авторскими правами. Для защиты этой конфиденциальной информации предприятия используют коммерческую тайну.

Важно не путать интеллектуальную собственность и коммерческую тайну. Интеллектуальная собственность также может являться составной частью коммерческой тайной, однако правовой режим охраны и использования результатов интеллектуальной деятельности имеет иной порядок.

Право интеллектуальной собственности является подотраслью гражданского права и регулирует общественные отношения, связанные с охраной и использованием результатов интеллектуальной деятельности человека.

Интеллектуальная собственность (далее - ИС) – результаты человеческой деятельности, не имеющие материального выражения. Интеллектуальная собственность в ряде правовых систем, также именуется результатами интеллектуальной деятельности, а сама такая деятельность подвержена национальной и международной защите.

Интеллектуальная собственность является право-экономической категорией и юридическим термином.

Существует много видов интеллектуальной собственности, в зависимости от конкретного государства, их объем различен.

Наиболее известными типами являются авторские права, патенты, торговые марки и ноу-хау.

Основная цель права интеллектуальной собственности заключается в поощрении создания широкого спектра интеллектуальных товаров. Для достижения этой цели закон предоставляет гражданам и частным лицам права собственности на информацию и результаты интеллектуальной деятельности, которые они создают, как правило, на ограниченный период времени. Это дает экономический стимул для их создания, поскольку позволяет людям получать прибыль от информации и результатов интеллектуальной деятельности, которые они создают .

Эти экономические стимулы могут стимулировать инновации и способствовать техническому прогрессу стран, поэтому правовое регулирование охраны и использования результатов интеллектуальной деятельности имеет многоаспектный характер.

Правовая природа интеллектуальной собственности имеет некоторые отличия от традиционных видов собственности.

Так, в отличие от традиционной собственности, интеллектуальная собственность является «неделимой», поскольку неограниченное количество людей может «потреблять» интеллектуальный товар без его истощения.

Кроме того, инвестиции в интеллектуальные товары страдают от проблем присвоения: землевладелец может окружить свою землю крепким

забором и нанять вооруженных охранников, чтобы защитить ее, но производитель информации или литературы обычно может очень мало сделать, чтобы не дать своему первому покупателю реализовать его произведение и продавать его по более низкой цене.

Соответственно требуется сбалансирование прав ИС таким образом, чтобы они были достаточно эффективными для того, чтобы стимулировать создание интеллектуальных товаров, но не настолько существенными, чтобы они препятствовали широкому использованию товаров [56].

Для коммерческой тайны нет процесса регистрации или оценки. Поскольку отсутствует надзорный орган, владелец коммерческой тайны должен будет доказать действительность своей коммерческой тайны только в том случае, если он будет вынужден подать иск о незаконном присвоении коммерческой тайны. Суд проанализирует коммерческую тайну и определит, удовлетворяет ли она требованиям юрисдикции в отношении защиты коммерческой тайны в соответствии с действующим федеральным законом.

Информация о результатах интеллектуальной деятельности, в большей степени является открытой информацией, нежели коммерческая тайна.

Информация должна соответствовать трем основным требованиям. Во-первых, коммерческая тайна должна извлекать из своей секретности экономическую ценность – являться основным, либо одним из основных средством получения прибыли. Во-вторых, информация не должна быть легко известна или выяснена. В-третьих, владелец коммерческой тайны должен прилагать разумные усилия для сохранения секретности информации.

Коммерческая тайна должна иметь экономическую ценность из-за того, что она не является общеизвестной в отрасли. Чтобы определить, имеет ли такая информация экономическую ценность в результате секретности, могут быть рассмотрены такие факторы, как ценность информации для держателя коммерческой тайны, ценность для конкурентов, а также количество усилий или денег, затраченных на разработку информации. Если информация

представляет собой ценность для бизнеса, потому что она не попадает в руки конкурентов ,она может быть защищена как коммерческая тайна.

Например, если у производителя бумаги была машина, метод или процесс, который мог бы перерабатывать использованную бумагу в новую бумагу быстрее, эффективнее и с меньшими затратами, чем у его конкурентов, он мог бы продавать свои постпотребительские бумажные изделия по более низкой цене, в то время как все еще сохраняя прибыль. Такая информация будет очень востребована конкурентами и является уникальной ценностью для производителя бумаги, позволяя ему преодолевать конкуренцию и доминировать на рынке. Сохраняя информацию в качестве коммерческой тайны, производитель бумаги может извлечь выгоду из своего изобретения. Если бы производитель бумаги решил запатентовать изобретение, ему пришлось бы раскрыть информацию и утратить возможность монополизировать ее после истечения срока действия патента.

В целях сохранения действительной коммерческой тайны ,информация не может быть широко известной или легко обнаруживаемой другим лицом с использованием надлежащих средств. Информация должна быть не только секретной, она также должна оставаться секретной.

Например, если процесс, использованный для производства продукта, можно обнаружить, просто взглянув на продукт, этот процесс не будет подпадать под защиту коммерческой тайны, поскольку его легко установить. В этом случае изобретателю будет рекомендовано обратиться за патентной защитой

Чтобы определить, является ли информация известной или доступной для обнаружения ,учитываются определенные факторы, включая легкость получения информации, дублирование ,или обратное проектирование, степень, в которой информация известна за пределами бизнеса ,и степень, в которой информация известна в рамках бизнеса . Если информация широко известна или может быть легко обнаружена или скопирована, она не

подлежит защите коммерческой тайны. Вдобавок ,если какой-либо метод, процесс ,или техника можно легко реконструировать, они могут не соответствовать требованиям для действительной коммерческой тайны.

Наконец, и, возможно, самое главное, владелец коммерческой тайны должен всегда прилагать разумные усилия для сохранения секретности своей коммерческой тайны.

Для обеспечения разумных усилий компания должна принять ряд защитных мер, включая, помимо прочего, ограничение доступа к коммерческой тайне только важнейшими личными, маркировку документов как конфиденциальные, маркировку чувствительных областей как запрещенных, размещение физических барьеров, таких как стены, запертые двери ,и охранники вокруг чувствительных зон, ограничение доступа к компьютеру с помощью паролей и других мер ,и требование соглашений о конфиденциальности для всех сотрудников, которые могут столкнуться с коммерческой тайной на работе. Буквальный замок и ключ - лучшая политика в отношении коммерческой тайны [32].

Таким образом, основная информация, которая может быть ограничена в рамках коммерческой деятельности, самими субъектами такой деятельности может быть отнесена ими к коммерческой тайне, правовой режим которой охраняется в соответствии с действующим законодательством.

Коммерческие секреты, если они могут быть сохранены, имеют неопределенный срок действия и, следовательно, большую потенциальную ценность, чем результаты интеллектуальной деятельности.

Коммерческая тайна может представлять собой любую формулу, образец, устройство, процесс или компиляцию информации, которая будет использоваться в бизнесе в качестве основного или вспомогательного фактора генерации прибыли.

К коммерческой тайне может быть отнесена: информация о клиентах, данные о ценах, маркетинговые методы, источники поставок и технические

ноу-хау могут быть коммерческой тайной. Закон «О коммерческой тайне» определяет правовой режим такого вида информации. Ответственность за разглашение коммерческой информации предусмотрена различными нормативными правовыми актами. В соответствии со статей 14 ФЗ «О коммерческой тайне» за разглашение коммерческой тайне предусмотрена гражданско-правовая, административная, уголовная и дисциплинарная ответственность.

2.2 Понятие и значение банковской, налоговой тайны

Банковская, налоговая и корпоративная тайна являются также информацией, которая может быть ограничена в процессе осуществления предпринимательской деятельности.

Рассмотрим каждую из представленных видов информации с позиции её участия в рамках осуществления предпринимательской деятельности.

Общественные отношения, это определенный порядок взаимодействия людей друг с другом в конкретной ситуации. Когда ситуация приобретает важный общественный характер, конкретизация таких отношений закрепляется в законе, возникают соответствующие правоотношения.

С появлением государства, начинает функционировать финансовая и банковская системы. В зависимости от конкретного государства, такое функционирование может осуществлять как при активном, там и пассивном участии государства.

Любое современное государство, заинтересовано в том, чтобы банковская система функционировала достаточно эффективно, с позиции экономических механизмов. Для того чтобы это все реализовать, требуется достаточно разветвленная система источников банковского права.

Финансово-кредитная деятельность – это деятельность финансово-кредитных организаций в Российской Федерации.

Деятельность финансово-кредитных организаций, регулируется Федеральным законом «О банках и банковской деятельности» [17].

Финансово-кредитная организация (далее – ФКО) – это юридическое лицо, цель деятельности которого состоит в извлечении прибыли от посреднических операций на финансовом рынке. Такая организация действует на основании лицензии Центрального банка России, и может иметь любую форму собственности.

Финансово-кредитные организации, делятся на:

- кредитные организации,
- банк,
- банк с универсальной лицензией,
- банк с базовой лицензией,
- небанковская кредитная организация (кредитные организации, способные осуществлять исключительно определенные в рамках конкретного нормативно-правового акта, и им же установленные операции);
- иностранные банки.

Для того, чтобы наиболее конкретно определить значение и сущность финансово-кредитной деятельности, необходимо рассмотреть наиболее распространенную финансово-кредитную организацию – банк.

Банк, в качестве кредитной организации, может осуществлять следующие операции:

- привлекать во вклады денежные средства физических и юридических лиц;
- размещать средства от своего имени и за свой счет на условиях возвратности, платности, срочности;
- открывать и вести банковские счета физических и юридических лиц.

Небанковские кредитные организации, в отличие от банков, не могут осуществлять привлечение денежных средств и их размещение от своего имени и за свой счет.

Законодательством Российской Федерации, установлен запрет на осуществление кредитными организациями производственной, страховой и торговой деятельности.

Финансово-кредитная деятельность, активно влияет на работу денежного и фондового рынка любого государства, а также является объектом усиленного контроля и надзора на всех уровнях исполнительной и законодательной власти.

Банковская деятельность имеет решающее значение в рамках любого типа экономики. Наиболее ценная роль банковских операций проявляется в рыночной экономике, где финансово-экономическая система представляет собой единый взаимосвязанный механизм взаимодействия всех её элементов.

Субъекты предпринимательской деятельности являются активными участниками финансово-экономической системы, которые обеспечивают наполнение денежных потоков в рамках такой системы. При осуществлении коммерческой деятельности банки играют колоссальную роль в осуществлении большинства бизнес процессов.

Банки являются хранителями средств обмена людей и организаций. В настоящее время практически невозможно осуществлять финансовые операции без посредничества банков. Использование банков - необходимость. Таким образом, банки являются хранилищами огромной информации о своих клиентах.

Что касается отдельных лиц, часто существует общее желание сохранить конфиденциальность своих собственных экономических операций. Более состоятельные люди могут не желать раскрывать богатство детям, супругам, семье или наследникам и не желают привлекать внимание воров и мошенников.

Компании могут захотеть защитить себя от конкурентов и будут стремиться хранить конфиденциальную информацию о ценах, планах и стратегиях на будущее, изобретениях (до тех пор, пока они не защищены патентами) и своем финансовом состоянии.

Некоторая часть «беглого капитала» - это деньги, переводимые за границу для защиты от политических и экономических потрясений, например экспроприации, чрезмерно строгого валютного контроля, чрезмерного налогообложения, дискриминационных сборов и безудержной инфляции.

Банковская тайна может быть использована коррумпированными лицами, стремящимися скрыть доходы от своих правонарушений.

В соответствии со статьей 26 ФЗ «О банках и банковской деятельности», банковскую тайну можно определить в качестве сведений об операциях, о счетах и вкладах своих клиентов и корреспондентов.

Корпорации и индивидуальные предприниматели в процессе своей деятельности являются активными пользователями банковских услуг, что соответственно способствует тому, чтобы получаемая банками информация содержалась в конфиденциальных условиях.

Помимо соблюдения закона, законодательные органы стремятся сбалансировать несколько интересов в своей банковской политике. Во-первых, некоторые хотят поощрять сбережения в банках, национальных или зарубежных, и поэтому считают, что необходимо гарантировать секретность.

Страны, которые национализировали банки, могут особо подчеркнуть обязанность сохранения секретности, чтобы противостоять опасениям утечки информации в страну как собственник. Во-вторых, некоторые государственные органы хотят уберечь банковскую систему, основанную на доверии и репутации, от скверны и запаха неподобающего поведения.

Банковская система может оказаться под угрозой, если общественность потеряет доверие к ее целостности. По этой причине, среди прочего, системы лицензирования банков обычно требуют высоких стандартов честного управления и соблюдения закона.

Статья 26 ФЗ «О банках и банковских деятельности» определяет перечень сведений, которые не могут подпадать под режим банковской тайны. Эти сведения, в большей степени, связаны с деятельностью

должностных лиц органов власти, которые также являются участниками банковских отношений.

Налоговая тайна также является одним из видов информации ограниченного доступа.

Большинство субъектов предпринимательской деятельности являются налогоплательщиками. Обязанность платить налоги закреплена в рамках конституционных положений.

Организации в зависимости от вида деятельности и от налогового режима платят различные виды налогов.

Понятие налоговой тайны закреплено в статье 102 НК РФ. Под налоговой тайной следует понимать сведения, «полученные налоговым органом, органами внутренних дел, следственными органами, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, плательщике страховых взносов, за исключением сведений» [59]:

- общедоступная информация, в том числе та информация, которая стала таковой с ведома налогоплательщика (плательщика взносов);

- информация об идентификационном номере налогоплательщика;

- информация о нарушении налогового законодательства участниками налоговых правоотношений;

- информация о налогах и сборах предоставленная иностранными государствами;

- информация о налогах и сборах, предоставляемая в рамках избирательного процесса;

- информация, предоставляемая на информационные государственные и муниципальные ресурсы;

- сведения о специальных налоговых режимах;

- информация о налогах и сборах, полученная в рамках муниципального финансового контроля;

- информация о налогах и сборах за определенный календарный год, размещенная в открытых источниках;

- информация о постановки налогоплательщика на учет в юрисдикции иностранного государства;

- информация о налоговом учете физических лиц;

- информация об обеспечительных мерах, применяемая в целях налогового администрирования.

Закон определяет, что налоговая информация, которая распространена самим налогоплательщиком, либо с его согласия не относится к налоговой тайне.

В соответствии с частью 1 статьи 102 НК РФ, разглашением налоговой тайны будет являться использование или передача должностным лицом налогового органа другому лицу производственной или коммерческой тайны налогоплательщика.

Отсюда следует то что, охрана налоговой тайны осуществляется аналогично режиму охраны установленной для производственной, коммерческой или служебной тайны. По сравнению с государственной тайной, налоговая тайна охраняется на менее серьезном уровне. Вопросами охраны и защиты государственной тайны занимаются специализированные органы в сфере защиты информации и государственной безопасности .

Основной проблемой использования налоговой тайны, является то, что в процессе реализации гражданских правоотношений, контрагенты не могут получить достаточного количества сведений составляющих налоговую тайну из открытых источников. Сведения, составляющие налоговую тайну могли бы повлиять на вступление в правоотношения с конкретным юридическим лицом, индивидуальным предпринимателем.

Фактически, налоговая открытость (отсутствие скрытых сведений) позволяет осуществлять более честную деятельность, которая влияет на результата взаимодействия. Так, если бы дольщики строительных компаний могли бы получить данные о строительных компаниях (бухгалтерскую

отчетность, которая является налоговой тайны), то они могли бы избежать токсичных правоотношений еще на этапе подготовки к их вступлению.

В соответствии с пунктом 13 части 1 статьи 21 НК РФ, налогоплательщики имеют право на охрану и соблюдение налоговой тайны, что соответственно закрепляет обязанность налоговых и иных органов государственной власти (обладающих налоговой информации) соблюдать режим налоговой тайны.

За несоблюдение установленных прав и обязанностей участниками правоотношений, закон предусматривает юридическую ответственность [60].

Передача информации, содержащей налоговую тайну, предусмотрена только в случаях, когда это прямо вытекает из закона, либо международного договора. Так, не будет являться разглашением налоговой тайны налоговой информации, которая была получена правоохранительным органом от налогового органа в рамках расследования налогового преступления.

При разглашении сведений составляющих налоговую тайну, закон предусматривает административную и уголовную ответственность. Также, учитывая нормы процессуального законодательства, следует сказать о том, что за нарушение налоговой тайны также предусмотрена гражданско-правовая ответственность, которая может быть реализована либо непосредственно через право на иск в рамках судебной защиты, либо через гражданский иск в рамках уголовного или административного процесса [61].

В КОАП РФ [10] в статье 13.14 предусмотрена административная ответственность за разглашение налоговой тайны. Так, разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей. Совершение данного правонарушения наказывается вынесением штрафа на физических лиц в размере от пятисот до одной

тысячи рублей и на должностных лиц - от четырех тысяч до пяти тысяч рублей [61].

Уголовная ответственность за разглашение налоговой тайны предусмотрена частью 2 статьи 183 УК РФ. Уголовная ответственность, будучи разновидностью юридической ответственности, вытекает из несоблюдения лицом, правонарушителем, интересов государства, общества и личности, которые являются общественно охраняемыми и имеют более высокую ценность по отношению к другим общественным отношениям [20].

Совершение общественно опасного деяния, которое запрещено законом, под угрозой наказания, всегда подразумевает привлечения лица к уголовной ответственности. Совершение преступления, всегда ведет к тому, чтобы лицо его совершившее было подвергнуто уголовному наказанию.

В соответствии с частью 2 статьи 183 УК РФ [11], в качестве преступления следует квалифицировать незаконное разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе.

Применение ответственности за разглашение налоговой тайны должно быть более определенным и использоваться только в целях повышения качестве правоотношений. Закон должен определять существенные сведения, которые составляют налоговую тайну и те сведения, которые следует сделать общедоступными.

2.3 Предоставление доступа к сведениям, составляющим, банковскую, налоговую и коммерческую тайны

Следует отметить, что банковской тайной обладают кредитные организации. Данные организации обязаны хранить известные им сведения, составляющие банковскую тайну. Однако ряд федеральных законов дает прямое указание на распространение такой информации определенному

кругу субъектов. Так статья 86 НК РФ указывает случаи, в которых кредитные организации обязаны предоставить рассматриваемые нами сведения налоговым органам. Например, банк обязан сообщить в налоговый орган информацию об открытии или о закрытии счета, вклада организации, индивидуального предпринимателя, физического лица, не являющегося индивидуальным предпринимателем.

«В других случаях, для предоставления налоговому органу такой информации, требуется его официальный запрос. В данной ситуации, предоставление такой информации будет являться законным только в целях проверки клиента как налогоплательщика» [28]. Предоставление банковской тайны правоохранительным органам так же носит свою специфику и раскрывается в отдельных нормативно правовых актах. В качестве примера можно привести процедуру получения этих сведений следователями МВД. Указанные лица могут получить сведения, составляющие банковскую тайну только по решению суда.

«В настоящий момент, Курганской областной Думой, выдвинуто предложение о внесении изменений в статью 26 ФЗ «О банках и банковской деятельности». Изменения направлены на расширение полномочий Росреестра, а именно, на возможность получения его должностными лицами доступа к банковской тайне. Данное предложение обусловлено необходимостью своевременного удовлетворения требования кредиторов по делам о банкротстве, а именно - работников, которым не выплачена заработная плата» [57].

Прежде чем перейти к рассмотрению способов предоставления информации, составляющей коммерческую тайну, отметим санкции, которые принимаются вследствие ее разглашения или недобросовестного получения.

«За разглашение коммерческой тайны предусмотрены различные виды санкций - от дисциплинарного взыскания до уголовного наказания. Самое легкое наказание за разглашение сведений составляющих коммерческую тайну - замечание или выговор. Затем следует материальная, гражданско-

правовая, и административная ответственность. Наконец самый жесткий вид наказания - уголовная ответственность, которая предусматривает реальное лишение свободы» [57].

Самый широкая категория лиц, которым предоставляется доступ к коммерческой тайне, являются сотрудники предприятий.

«Как отмечает Минбалеев А. В. Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями» [57].

«В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работник обязан:

- выполнять установленный работодателем режим коммерческой тайны;

- не разглашать эту информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;

- возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей;

- передать работодателю при прекращении или расторжении трудового договора материальные носители информации, имеющиеся в пользовании работника и содержащие информацию, составляющую коммерческую тайну» [46].

«Одной из особенностей предоставления рассматриваемого нами типа тайны является закрепление таких сведений в договорах по оказанию аудиторских услуг. Сохранение коммерческой тайны является обязанностью аудитора, и разглашать такую тайну он вправе только с письменного согласия лица, в отношении которого проводится аудит» [58]. «Некоторые авторы считают, что при предоставлении сведений составляющих

коммерческую тайну целесообразно определить их ценность. Так, например Яковлева И.А. полагает, что определение ценности сведении составляющих коммерческую тайну является обязательным условием для установления режима коммерческой тайны» [58].

Законодатель определяет круг субъектов, которым обладатель сведений составляющих коммерческую тайну обязан их предоставить. В соответствии со ст. 6 ФЗ «О коммерческой тайне», по мотивированному запросу от государственного органа, органа МСУ, лицо, обладающее коммерческой тайной, предоставляет им необходимые сведения. В случае отказа со стороны лица обладающего информацией предоставить ее, указанные органы могут истребовать ее через суд. Помимо государственных органов и ОМСУ, данный тип информации могут запрашивать суды, органы предварительного следствия и дознания, по делам, которые находятся у них в производстве. При этом на сведения, содержащие коммерческую тайну и переданные вышеуказанным органам, должен быть наложен гриф «коммерческая тайна».

«В современных условиях модернизации организационных и административных процессов, должно происходить обновление принципов ведения предпринимательской деятельности» [39].

«В частности, в настоящее время, бумажные носители информации отходят на второй план. Все больше предприятий отдают предпочтение электронному документообороту. Это один из примеров роста роли инновационных методов и средств регулирования экономического оборота в целом, которые, в свою очередь, требуют особого контроля» [60] .

В связи с этим возникает потребность охраны и предоставления доступа к информации содержащей коммерческую тайну. В данном случае охрана и предоставление информации возможно только с помощью специальных технических средств и программ. В качестве примера можно привести пример мнение Мавринской Т.В. [45], она считает, что с помощью БЬР-систем, возможно осуществить защиту конфиденциальной информации должным образом, выявить недобросовестных сотрудников, отследить пути

утечки конфиденциальной информации - в том числе данных содержащих коммерческую тайну.

По моему мнению, действующие нормативные правовые акты не в полной мере раскрывают способы предоставления информации содержащей коммерческую тайну, и соответственно оставляют пробел для недобросовестных участников гражданских правоотношений. Паршуков М.И. [53] замечает, что если мы обратимся к сути проблемы, то сможем выявить конфликт интересов между участниками обществ и коммерческими организациями в области информационного обмена. По его мнению, современное законодательство не решает данных проблем, и требуется совместная работа предпринимателей, юристов, ученых, представителей законодательной власти для определения четкой границы между сохранением коммерческой тайны и ее предоставлением в случаях прямо прописанных в нормативных правовых актах.

«НК РФ четко определен круг лиц, которые имеют доступ к информации, содержащей налоговую тайну. К ним относятся должностные лица налоговых органов, органов внутренних дел, таможенных органов, органов следствия и государственного внебюджетного фонда. Общий порядок доступа к информации, содержащей налоговую тайну определяется, Налоговым кодексом РФ и Приказом МНС РФ от 03.03.2003 № БГ-3-28/96 «Об утверждении Порядка доступа к конфиденциальной информации налоговых органов»» [26]. Из этого общего порядка есть исключения. При осуществлении предпринимательской деятельности, предприниматели заинтересованы в надежности и честности своего контрагента. Для того чтобы избежать рисков связанных с недобросовестностью будущего партнера по бизнесу, и вследствие долгих и сложных судебных тяжб, предпринимателю следует проявить должную осмотрительность. В данном случае предприниматели могут обратиться к сайту ФНС, а именно к разделам «Прозрачный бизнес» или проверить своих контрагентов с помощью иных сервисов.

Следующая особенность предоставления доступа к налоговой тайне является признание таких сведений общедоступными. В данном случае сам предприниматель принимает решение о признании сведений о нем, которые содержат налоговую тайну - общедоступными. Это делается для возможности участия предпринимателя в тендере, либо данную информацию запрашивает крупный бизнес партнер. Процедура выглядит следующим образом: налогоплательщик, который планирует сделать налоговые сведения о себе общедоступными должен заполнить согласие соответствующей формы и направления его в ФНС. В данном случае необходимо правильно определить специальный код. В противном случае налоговые службы раскроют информацию, которую налогоплательщик раскрывать не хотел. Так же необходимо отметить, что отзыв такого согласия невозможен.

«На основании выше изложенного можно отметить следующее. Помимо общего порядка предоставления доступа к информации, содержащей банковскую, налоговую или коммерческую тайны, который предусмотрен действующими законами и иными НПА, существует ряд особенностей. Эти особенности необходимо учитывать при попытке получить доступ к данным видом информации. Так же, по нашему мнению, необходимо совершенствовать законодательство в данной сфере. Дать более четкие и конкретные определения налоговой и банковской тайны. Усовершенствовать порядок и способы охраны данных видов информации, в том числе от недобросовестных должностных лиц» [29].

Таким образом, следует констатировать, что на сегодняшний день основной проблемой правового регулирования предоставления информации ограниченного доступа в сфере предпринимательской деятельности является недостаточность существующих положений законодательства в этой сфере.

Учитывая общую проблематику российской правовой системы, российского общества и государства, получение информации ограниченного доступа и последующая её защита, вызывают ряд вопросов практического характера. Несмотря на недостаточность существующих положений,

практика защиты информации ограниченных правовых режимов, в рамках существующей национальной правовой реальности вызывает осложнения. Полагаю, что для нормально развития рыночной экономики, данные пробелы в сфере правового регулирования следует устранять.

Глава 3. Проблемы правового регулирования доступа к ограниченной информации в предпринимательской деятельности

3.1 Практические вопросы реализации защиты информации в сфере предпринимательской деятельности

Основные проблема защиты информации в предпринимательской сфере связаны с государственной политикой Российской Федерации в отношении Интернета и информации находящейся в открытом доступе.

На сегодняшний день, предпринимательское сообщество не обладает средствами и методами, которые могли бы способствовать защите их интересам, в рамках общей системы угроз вмешательства государства в частные интересы корпораций и индивидуальных предпринимателей.

С каждым годом, все больше и больше количества различных данных, в том числе коммерческой и конфиденциальной информации скапливается именно в Интернете. Существующие формы и способы защиты такой информации являются неэффективными для бизнеса.

Новые правила в отношении Интернета в России, большинство из которых вступили в силу 1 ноября 2019 г., а другие должны следовать в январе 2021 г., привлекли международное внимание и были публично названы российским «суверенным законом об Интернете». На самом деле такого нового закона не было, а скорее была серия поправок к существующим федеральным законам «О связи» и «Об информации, информационных технологиях и защите информации» [57].

Официально поправки направлены на защиту Интернета в России от внешних угроз. Фактически, они обеспечивают важнейшую правовую основу для создания централизованной системы управления Интернетом со стороны государственной власти, что теоретически позволяет изолировать российскую сеть от глобального Интернета.

Эти три поправки имеют особенно далеко идущие последствия:

- обязательная установка технических средств противодействия потенциальным угрозам;

- централизованное управление телекоммуникационными сетями в случае угрозы;

- механизм контроля линий связи, пересекающих границу России.

С помощью этих трех ключевых поправок Россия пытается достичь как минимум трех разных целей. Во-первых, он нацелен на создание механизма эффективного наблюдения за Интернетом в пределах его границ. С этой целью поправка, касающаяся установки «технических средств противодействия угрозам», позволяет усилить государственный контроль над информацией и предотвратить ее распространение в случае необходимости. Следовательно, реализация нового законодательства может дать российскому правительству возможность ограничить активность оппозиции в социальных сетях, помогая ему предотвращать протесты, подобные протестам 2011–2013 годов в преддверии выборов в российский парламент, Государственную Думу, запланированных на 2021 год.

Во-вторых, государство стремится стать ключевым регулятором Интернета в России. Недавняя поправка, позволяющая государству создавать централизованный контроль над интернет-инфраструктурой путем введения трансграничного контроля линий подключения и перенаправления трафика, является попыткой обеспечить изоляцию национальной сети от глобального Интернета, для чего государство может открывать и закрывать «цифровые границы» и определять поток информации внутри них по своему усмотрению. Хотя тотальный государственный контроль над Интернетом в России останется невозможным до тех пор, пока страна подключена к миру через существующую инфраструктуру глобального Интернета, принятие этой поправки режимом Путина было попыткой представить свой контроль над телекоммуникационными линиями, сетями и т. Д. и трафик как свершившийся факт [15].

В-третьих, Россия намерена расширить государственно-ориентированную модель Интернета на международный уровень. Поправка, направленная на создание инфраструктуры для национальной системы доменных имен (DNS), может, если она будет достигнута в соответствии с планом в январе 2021 года, создаст российский сегмент Интернета - параллельный и, вероятно, несовместимый с существующим. Этим шагом Россия не стремится изолировать себя от остального мира, а скорее создает прецедент, которому могут последовать другие государства, стремящиеся к суверенитету над своими сегментами Интернета. Предположительно, России потребуется еще более тесное сотрудничество с Китаем, чем она уже есть, для разработки технологий для достижения своих целей и координации своей интернет-политики на международном уровне. В долгосрочной перспективе,

Хотя некоторые последствия трех поправок все еще неясны, а некоторые нормативные акты и требования еще не приняты, новое законодательство уже несет в себе конкретные риски, которые касаются не только самой России, но и Германии и других европейских стран, которые сотрудничают с Россией и собственными компаниями. действующий внутри него [52].

Теперь обязательное «техническое оборудование для противодействия угрозам», например, также сможет определять приоритеты трафика. Он может задерживать поток одних типов сетевых пакетов, отдавая приоритет другим, повышая их производительность. На практике пользователи определенных веб-сайтов и сервисов могут испытывать медленный доступ или недоступность. Такая расстановка приоритетов может поставить под угрозу сетевой нейтралитет и привести к дискриминации компаний, не защищенных российским государством.

Тот факт, что для этого нового оборудования не существует ни технических требований, ни сертификации, также означает, что сбои в сети более вероятны. Компании, работающие в России, в свою очередь, могут

понести сопутствующий ущерб, вызванный новым оборудованием, с ограниченными возможностями возмещения убытков.

Кроме того, более вероятная перспектива так называемого «splinternet», когда сегменты Интернета контролируются и регулируются различными государствами и участниками, может привести к несовместимости технических, нормативных и операционных стандартов, что затрудняет трансграничное сотрудничество и совместимость глобального Интернета [8].

У России есть давняя политика в области информации и Интернета, с помощью которой она уже пыталась контролировать Интернет в предыдущие годы, как было также описано в недавнем документе DGAP Андрея Солдатова. Но в текущей практике государственные органы применяют уже существующие в России ограничительные законы об Интернете выборочно по двум причинам. Во-первых, из-за отсутствия технических возможностей некоторые законы не могут быть реализованы. Во-вторых, некоторые интернет-сервисы и приложения настолько популярны, что государство не блокирует их, чтобы избежать общественного недовольства [9].

Вообще говоря, чтобы получить большее влияние во внутреннем Интернете, государственные органы могут внедрять централизованные и децентрализованные механизмы контроля. Какой из них выбрать, в основном определяется сетевой инфраструктурой и объемом контроля стран над своими сетями. Китай, например, выбирает централизованное управление; страна поставила под свое иго провайдеров интернет-услуг (ISP) на раннем этапе, и трафик направляется через «узкие точки», сетевые узлы, через которые проходят данные при входе или выходе из внутренней сети страны. Такие страны, как Великобритания, Индия и Россия, в настоящее время имеют гораздо меньший контроль над своими сетями и внутренними интернет-провайдерами. В их случае предпочтителен децентрализованный подход. Власти вводят новые законы и политические меры и обязывают интернет-провайдеров соблюдать их. До этого момента, Россия была «самой большой и самой агрессивной» страной, осуществлявшей

децентрализованный контроль, о чем свидетельствуют законы, принятые с 2012 года, регулирующие Интернет. Новые поправки, внесенные в 2019 году, призваны предоставить российским властям более централизованные полномочия. Роскомнадзор - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций - и центральный пункт контроля над сетями и объектами связи, а также персональными данными в России, хочет отслеживать трафик в его источнике, не имея между собой интернет-провайдера. или интернет-сервисы, не соответствующие новым правилам [33].

Очевидно, Россия сейчас пытается догнать то, что Китай быстро реализовал в первые дни Интернета: централизованные и эффективные механизмы контроля в основе сети.

В 2016 году вступил в силу Закон Яровой (назван в честь Ирины Яровой, члена партии «Единая Россия» в Госдуме и соавтора закона). С тех пор телекоммуникационные компании были обязаны хранить содержание текстовых сообщений, телефонных разговоров, изображений и видео в течение шести месяцев, а также их метаданные в течение трех лет на территории России. Они должны предоставить эту информацию службам безопасности по запросу.

Для российских властей адрес посылки может быть достаточным индикатором, чтобы блокировать запросы с нежелательных веб-сайтов. Одним из возможных решений было бы для пользователя скрыть адрес пакета, который он или она хочет отправить, перенаправив его через виртуальную частную сеть (VPN). В этом случае пользователь общается не напрямую с интернет-провайдером, а через одну или несколько организаций между ними. Это делает пункт назначения запроса видимым только для поставщика услуг VPN, но не для интернет-провайдера. Но, поскольку российские власти также пытаются использовать системы DPI или аналогичные технологии для отключения VPN-сервисов, этот обходной путь может рано или поздно перестать быть жизнеспособным вариантом.

Другой обходной путь, который используется в настоящее время, - это метод, называемый «входом в домен», с помощью которого запрос перенаправляется на тот же сервер после того, как установлено HTTPS-соединение. Этот метод, среди прочего, использовался Telegram для обхода IP-запретов Роскомнадзора. Однако и этот обходной путь становится все труднее реализовать, поскольку такие компании, как Amazon или Google, которые используют серверы, также используемые для доступа к доменам, стремятся положить конец этой практике.

Вышеупомянутые положения дают государственным органам возможность создать «аварийный выключатель», относительно простой в использовании механизм, который можно использовать для отключения большей части российского Интернета. В случае такого отключения даже системы обхода DPI, VPN или другие неопознанные соединения не будут работать - связь становится физически невозможной.

Глобальный Интернет силен и избыточен, потому что его трафик обрабатывается сетью компьютеров и серверов; поэтому данные могут проходить по разным путям, чтобы достичь места назначения. Объем централизованного обмена трафиком и узких мест сильно влияет на способность правительства цензурировать и подавлять потоки данных. Чем меньше количество узких мест, тем легче ими управлять [30].

С введением этой новой поправки российские власти ослабят устойчивую структуру российского Интернета, направляя трафик через централизованные, контролируемые государством точки подключения, которые могут быть отключены в случае «угрозы». Российские власти могут вскоре отключить основные части сети и, таким образом, предотвратить проникновение или распространение информации, критичной по отношению к правительству, внутри страны.

В прошлом в разных странах происходило несколько преднамеренных отключений Интернета в разных масштабах. Умышленное отключение на месте теоретически возможно в любой стране со слабой правовой системой -

потому что его можно протолкнуть с небольшим юридическим сопротивлением. Например, одно такое отключение произошло в августе 2019 года во время митингов в центре Москвы; BBC утверждает, что его запросили правоохранительные органы. В ноябре 2019 года Иран на несколько дней отключил большую часть своего интернета. Однако это общенациональное отключение стало возможным только потому, что страна полагается на передачи данных через узкие точки и имеет очень ограниченное количество интернет-провайдеров, которые все контролируются государством. В отличие от Ирана, у России более 40 провайдеров на своих границах, много интернет-провайдеров и - на данный момент - нет крупных узких мест. Эти параметры затрудняли выполнение любого крупного отключения Интернета в России. Новые поправки, однако, создают новую правовую основу именно для такого сценария, тем самым повышая вероятность остановки [43].

Опасения бизнеса быть отключенными от Интернета, выраженные в пояснительной записке, не совсем правдоподобны. Прежде всего, поскольку ICNN является независимой организацией, вмешательство со стороны правительства США с юридической точки зрения почти исключено. Более того, правительство США, скорее всего, технически не способно закрыть домены, связанные с российскими веб-сайтами. Всемирной DNS управляет IANA (Управление по присвоению номеров в Интернете), подразделение ICANN, расположенное в Калифорнии. Домены верхнего уровня (TLD), такие как .ru или .de, хранятся в так называемых файлах корневой зоны. Эти файлы, которые управляются ICANN и могут считаться основой Интернета, в основном хранятся на 13 серверах корневой зоны по всему миру, десять из которых расположены в США, а по одному - в Нидерландах, Швеции и Японии. Но файлы TLD также хранятся на многих других серверах имен. Если, например, 10 корневых серверов на территории США будут изменены таким образом, что домены российских веб-сайтов будут перенаправлены, останутся еще три других корневых сервера и все серверы имен. Как только

обнаруживается манипуляция с файлами корневой зоны, поставщики D№S могут остановить процесс зеркалирования с корневых серверов США. Следовательно, на всех остальных DNS-серверах по-прежнему будут файлы, предоставляющие доступ к российским доменным именам. Следовательно, даже если почти все корневые серверы расположены в США, отключение правительством США ДВУ, связанных с российскими веб-сайтами, нереалистично. Как только обнаруживается манипуляция с файлами корневой зоны, поставщики D№S могут остановить процесс зеркалирования с корневых серверов США. Следовательно, на всех остальных DNS-серверах по-прежнему будут файлы, предоставляющие доступ к российским доменным именам. Следовательно, даже если почти все корневые серверы расположены в США, отключение правительством США ДВУ, связанных с российскими веб-сайтами, нереалистично. Как только обнаруживается манипуляция с файлами корневой зоны, поставщики DNS могут остановить процесс зеркалирования с корневых серверов США. Следовательно, на всех остальных DNS-серверах по-прежнему будут файлы, предоставляющие доступ к российским доменным именам. Следовательно, даже если почти все корневые серверы расположены в США, отключение правительством США ДВУ, связанных с российскими веб-сайтами, нереалистично [37].

На этом фоне кажется, что целью этой новой поправки является не защита Интернета в России от внешних атак, а, скорее, упреждающий шаг к отделению своего национального сегмента от инфраструктуры глобального Интернета, чтобы получить статус государства.

Прежде всего, проприетарный DNS сделает Россию независимой от ICANN, в которой, по мнению Кремля, доминируют США. И хотя техническая реализация кажется непростой, национальная DNS является ключевой частью, которая позволит государству отключить внутренний Интернет на длительный срок. Тогда России не придется справляться с международным трафиком и, следовательно, с нежелательной информацией, исходящей или поступающей из страны.

Помимо общей политики российской власти в сфере информации и Интернета, самая большая проблема - это не штрафы или другие нормативные последствия, как некоторые могут подумать. Взаимодействие с российским органом по защите данных в случае инцидента, связанного с безопасностью данных, может быть обременительным и привести к штрафам (которые довольно небольшие - примерно до 1000 долларов США), но не более того. Очевидно, самая большая угроза - это потенциальный ущерб репутации.

В мае атака WannaCry заразила тысячи компьютеров по всему миру, и некоторые юридические фирмы начали делиться своим опытом в области соблюдения требований кибербезопасности, предлагая решения для пострадавших компаний. После упомянутой атаки Пети на крупную юридическую фирму США вполне может оказаться, что клиенты в будущем дважды подумают, прежде чем обращаться к ней за советом по кибербезопасности. Ущерб репутации фирмы, очевидно, значительный, и все же его можно оценить количественно. С другой стороны, Очевидно, что в современном мире практически невозможно оставаться на 100% защищенным от любых угроз кибербезопасности. Даже компании, для которых кибербезопасность имеет первостепенное значение, по-прежнему уязвимы для атак кибербезопасности просто потому, что они используют информационные технологии в своей повседневной деятельности.

Как правило, российским компаниям необходимо обеспечить соответствие своих систем в России техническим требованиям Федеральной службы безопасности (ФСБ) и Федеральной службы по техническому и экспортному контролю России (ФСТЭК). Как правило, целесообразно, чтобы формирование российской ИТ-среды и связанных с ней процедур соответствия ИТ проводилось при содействии российской компании, специализирующейся на ИТ-безопасности, и имеющей лицензию ФСТЭК на выполнение работ, связанных с безопасностью данных (защита конфиденциальной информации). Компания, занимающаяся ИТ-

безопасностью, также может помочь с подготовкой набора внутренней документации: внутренних документов по техническим вопросам защиты персональных данных, описания инфраструктуры ИТ-безопасности и мер, которые компания должна предпринять для предотвращения утечки данных (например, модели угроз, технические задания). Они также могут посоветовать, какое оборудование и программное обеспечение необходимо установить для обеспечения безопасности данных. Очевидно, что на данном этапе развития ИТ-технологий настоятельно рекомендуется не полагаться на собственные ИТ-ресурсы, а вызвать стороннего поставщика услуг ИТ-безопасности и позволить профессионалам построить «стены» безопасности данных компании.

Основное беспокойство вызывает пресловутая локализация данных. Из-за недавнего закона о локализации данных сбор личных данных от россиян и дальнейшее прямое хранение в облаке, расположенном за границей, больше не разрешены.

Закон ввел новую процедуру, ограничивающую доступ к веб-сайтам, нарушающим российское законодательство о персональных данных, и ввел требование хранить персональные данные граждан России на серверах, расположенных в России (это, очевидно, дает огромный толчок к развитию индустрии центров обработки данных в России).

Персональные данные граждан России должны храниться и обрабатываться с использованием баз данных, находящихся в России. Требование можно выполнить, разместив базу данных сайта с личными данными россиян в дата-центре или сервере в России. Эта российская база данных должна быть первичной, а внешнее облако должно быть «вторичной» базой данных (т. Е. Только частичной или полной (зеркальной) копией первичной российской базы данных). По сути, это означает, что первоначальный хостинг должен находиться в России. Некоторое время требования к локализации данных практически не соблюдались. Однако в 2016 году большое внимание общественности привлекло крупное дело,

связанное с LinkedIn. Окружной суд России удовлетворил иск российского органа по защите данных (Роскомнадзор) об ограничении доступа к LinkedIn на территории России. Суд установил, что LinkedIn хранит и обрабатывает личные данные граждан России на серверах, расположенных за пределами России. На этом основании суд признал LinkedIn нарушающим закон о персональных данных и обязал Роскомнадзор принять меры по ограничению доступа к Li№kedIn. В настоящее время LinkedIn остается заблокированным в России [47].

Еще одна проблема, вызывающая озабоченность, - это поправки к российскому закону об информации, которые, наконец, вступили в силу 1 июля 2018 года. Поправки напрямую затрагивают телекоммуникационную и интернет-отрасли России.

В частности, операторам мобильной связи необходимо хранить записи всех телефонных звонков и содержание всех текстовых сообщений в течение шести месяцев, что влечет за собой огромные расходы, в то время как интернет-компании (например, мессенджеры) должны хранить записи всех телефонных звонков и содержание всех текстовых сообщений за шесть месяцев и соответствующие метаданные за один год. Кроме того, поправки требуют предоставления любых таких сообщений российской полиции и разведке по их запросу и установки специальных систем, используемых для целей расследования или «согласования использования программного и аппаратного обеспечения с властями».

Поправки уже привели к случайным блокировкам (например, BlackBerry Messenger); однако из-за ограниченной популярности таких мессенджеров дела о принудительном исполнении не привлекали особого внимания. Затем все изменилось с делом об одном из самых популярных в России мессенджеров - Telegram.

Telegram часто комментировал в прессе, что не может предоставить ключи дешифрования из-за природы технологии сквозного шифрования, в то время как ФСБ полагала, что это технически возможно. Telegram отказался

предоставить ФСБ какие-либо ключи дешифрования, поэтому 13 апреля 2018 года Таганский районный суд Москвы удовлетворил ходатайство Роскомнадзора о блокировании доступа к Telegram. 16 апреля 2018 года Роскомнадзор обратился к операторам связи с просьбой начать блокировку мессенджера. Все российские операторы связи обязаны заблокировать доступ к соответствующим ресурсам [36].

Юристы Telegram безуспешно обжаловали это решение. По состоянию на апрель 2018 года Роскомнадзор пытался заблокировать Telegram, используя его IP-адрес, что кажется неэффективной стратегией. Telegram решил не подчиняться решению суда и бросить вызов Роскомнадзору (к счастью, он фактически не присутствует в России) и начал перескакивать с одного IP-адреса на другой. В свое время Роскомнадзор блокировал миллионы IP-адресов, что вызывало перебои в работе многих интернет-сервисов (в том числе в сетях Amazon и Google) и вызывало негативную критику Роскомнадзора со стороны других органов власти, интернет-омбудсмена и бизнеса. Дело продолжается, и Telegram все еще доступен, несмотря на действия Роскомнадзора.

Помимо стандартных мер предосторожности в отношении конфиденциальности, таких как зашифрованные комнаты данных и соглашения о неразглашении, компании, заключающие сделки M&A в России, должны рассмотреть вопросы передачи персональных данных до начала процесса комплексной проверки. Как уже упоминалось, в связи с недавним законом о локализации данных сбор личных данных граждан России и дальнейшее прямое хранение в облаке, расположенном за границей, больше не разрешены.

Следовательно, потенциальный иностранный покупатель должен дважды проверить, хранятся ли личные данные (например, сотрудников целевой компании) в российской первичной базе данных и позволяет ли соответствующее согласие, данное такими сотрудниками продавцу, передавать их данные покупателю.

Таким образом, несмотря на относительно устойчивые подходы в рамках правового регулирования защиты информации использующейся в предпринимательской деятельности, существующие проблемы в защите информации ограниченного доступа имеют комплексный характер, в основном связанные с усилением государственного контроля в информационном секторе. Причем подобная практика осуществляется с динамической прогрессией, что заставляет некоторых представителей бизнеса (которые могут себе это позволить) перемещаться в другие страны и оттуда вести свой бизнес на территории России.

Административный контроль, который в большей степени не является оправданным, также не способствует развитию информационного обеспечения компаний, что также заставляет владельцев и управляющий корпораций принимать меры по защите информации, вне существующих правовых концепций.

3.2 Неправомерное использование информации ограниченного доступа в предпринимательской деятельности

Правительство России очень заинтересовано в борьбе с киберпреступностью и даже вводит в законы различные правила, направленные на повышение кибербезопасности бизнеса. Например, все компании, работающие с персональными данными, должны применять определенные технические и организационные меры, направленные на защиту данных, а также использовать программное обеспечение, сертифицированное российскими властями.

Любое компьютерное мошенничество, несанкционированный доступ к данным или создание вредоносного программного обеспечения могут повлечь за собой уголовную ответственность. Однако количество реальных случаев осуждения хакеров довольно невелико. Причина этого неясна и, безусловно, вызывает предположения.

Россия отказалась ратифицировать Конвенцию Совета Европы о киберпреступности, и, судя по обсуждениям в российском правительстве, Россия не ратифицирует эту конвенцию. Официальные лица российского правительства заявили, что они не согласны с положениями конвенции, предусматривающими санкционированный доступ одного государства-члена к компьютерным данным, хранящимся на территории другого государства-члена, без предварительного согласия последнего. Чиновники оправдывают это соображениями национальной безопасности [38].

Представители государства заявили, что подход России к борьбе с киберпреступностью заключается в «оперативном и адекватном сотрудничестве правоохранительных органов разных стран, а также недопущении проведения расследований на иностранной территории без уведомления правоохранительных органов. заинтересованное государство ». Более того, власти считают, что Россия рассматривает возможность продвижения подхода, предусматривающего разработку глобальной конвенции о борьбе с преступлениями в информационной сфере вместо Будапештской конвенции, которая применяется только на региональном уровне и не будет полностью эффективной.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

- соблюдение конфиденциальности информации ограниченного доступа;

- реализацию права на доступ к информации.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства

Российской Федерации об информации, информационных технологиях и о защите информации.

Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

- своевременное обнаружение фактов несанкционированного доступа к информации;

- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

- постоянный контроль за обеспечением уровня защищенности информации;

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям [54].

Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации;

Нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

Нарушение требований в сфере защиты информации ограниченного доступа влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Лица, виновные в нарушении обработки, включая сбор и хранение, биометрических персональных данных, несут административную, гражданскую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

- либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

- либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

Провайдер хостинга, оператор связи и владелец сайта в сети «Интернет» не несут ответственность перед правообладателем и перед пользователем за ограничение доступа к информации и (или) ограничение ее распространения в соответствии с требованиями настоящего Федерального закона.

Глава 28 Уголовного кодекса Российской Федерации (далее - УК РФ) включает нормы, предусматривающие ответственность за преступления в сфере компьютерной информации.

Неправомерным считается доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты.

Что касается общественно опасных последствий, то под уничтожением информации необходимо понимать приведение ее или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Не будет считаться уничтожением информации простое переименование файла, а также автоматическая замена старой версии файлов новой. Перенос информации на другой носитель не является в контексте уголовного закона уничтожением компьютерной информации лишь в том случае, если в результате этих действий доступ правомерных пользователей к информации не оказался существенно затруднен либо исключен.

Неправомерный доступ к информации ограниченного доступа, в случае наличия признаков состава преступления, может быть квалифицироваться в рамках статьи 272 УК РФ.

Традиционно признак «с использованием служебного положения» вменяется, если лицо, совершившее преступление, являлось должностным лицом, лицом, выполняющим управленческие функции, в коммерческих или иных организациях или государственным либо муниципальным служащим, не отвечающим признакам должностного лица. Однако историческое толкование нормы приводит к выводу, что использующими служебное положение применительно к ст. 272 УК РФ должны признаваться те, кто имел возможность доступа к компьютерной информации в силу выполняемой работы (по трудовому, гражданско-правовому договору). Следовательно, субъектами квалифицированного состава могут стать программисты, системные администраторы, операторы и т. п.

Так, приговором Центрального районного суда г. Твери А. была признана виновной в совершении неправомерного доступа к охраняемой законом компьютерной информации, повлекшей модификацию компьютерной информации, осуществленного лицом с использованием своего служебного положения. Согласно материалам дела, А. состояла на должности старшего оператора ЭВиВМ группы операционного обслуживания абонентов Территориального участка г. Тверь ООО «Г.» и в рамках своих должностных обязанностей осуществляла изменение параметров и перерасчеты в лицевых счетах клиентов ООО «Г.» согласно представленным документам, а также осуществляла проверку подлинности и соответствие представленных документов необходимым критериям. По просьбе своего знакомого А. внесла в карточку лицевого счета абонента Д. искаженные данные о замене приборов учета газа, тем самым осуществила модификацию компьютерной информации [41].

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

В Перечень информации конфиденциального характера, утвержденный Указом Президента Российской Федерации от 06.03.1997 № 188, включены

сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные). В частности, к персональным данным относятся фамилия, имя, отчество, пол, возраст, образование, место жительства физического лица.

Гражданин вправе обратиться к прокурору с заявлением о возбуждении дела об административном правонарушении в связи с разглашением информации с ограниченным доступом (ст. 13.14, ч. 1 ст. 28.4 КоАП РФ).

Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами. Информация, содержащаяся в государственных информационных системах, является официальной. Государственные органы, определенные в соответствии с нормативным правовым актом, регламентирующим функционирование государственной информационной системы, обязаны обеспечить достоверность и актуальность информации, содержащейся в данной информационной системе, доступ к указанной информации в случаях и в порядке, предусмотренных законодательством, а также защиту указанной информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

За разглашение служебной информации ограниченного распространения, а также нарушение порядка обращения с документами, содержащими такую информацию, государственный служащий (работник организации) может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

С учетом конкретных обстоятельств за разглашение служебной тайны может наступать уголовная ответственность, как правило, в тех условиях, когда информация одновременно относится к двум и более видам тайн (ст. ст. 138, 285, 310, 311, 320 УК РФ).

Заключение

Понятие «информации» является всеобъемлющим и в зависимости от конкретной ситуации и интерпретации может иметь разное значение. В аспекте правового регулирования, отношений содержащих информационные аспекты, следует прибегать к нормативному толкованию данного термина, так как в национальной правовой системе понятие «информации» имеет правовое закрепление.

Основное значение информации заключается в передачи между субъектами информационного взаимодействия различных сведений, которые могут быть абсолютно любыми. Право на получение информации, обязанности по предоставлению той или иной информации, ограничения оборота какой-либо информации являются определенной формой отношений с конкретными видами информации и в зависимости от требований закона подлежат определенной правовой форме регулирования.

Право на информацию – это сформулированное в национальных и международных правовых актах право человека на свободный поиск, получение, передачу, производство и распространение информации любым законным способом.

Право на доступ к информации – это право человека на получение публичной и частной информации публичного характера, в рамках требований закона государства.

Информация ограниченного доступа в первую очередь закрепляется в различных нормативных правовых актов. Условия ограничения доступа к таким сведениям определяется в зависимости от конкретного вида правоотношений. Следует отметить, что в различных правоотношениях могут встречаться смешенные виды тайн, которые могут находиться на стыке различных нормативных актов. В предпринимательской деятельности, ограничение информации осуществляется в целях сохранения определенных позиций на рынке для недопущения потери конкурентного преимущества,

что способствует развитию и процветанию субъектов предпринимательской деятельности.

Несмотря на относительно устойчивые подходы в рамках правового регулирования защиты информации, использующейся в предпринимательской деятельности, существующие проблемы в защите информации ограниченного доступа имеют комплексный характер, в основном связанные с усилением государственного контроля в информационном секторе. Причем подобная практика осуществляется с динамической прогрессией, что заставляет некоторых представителей бизнеса (которые могут себе это позволить) перемещаться в другие страны и оттуда вести свой бизнес на территории России.

Административный контроль, который в большей степени не является оправданным, также не способствует развитию информационного обеспечения компаний, что также заставляет владельцев и управляющий корпораций принимать меры по защите информации, вне существующих правовых концепций.

Предусмотренный подход законодателя в Гражданском кодексе РФ, по вопросу того, что информация с ограниченным доступом, составляющая коммерческую тайну, выступает объектом единого исключительного права, считаем, является неверным. Поскольку происходит необоснованное смешение исключительного права и права, гарантирующего обладателю такой информацией, защиту от третьих лиц (право на конфиденциальность информации), которое необходимо рассматривать в качестве самостоятельного интеллектуального права.

«Деловая конфиденциальная информация» в отличие от «секрета производства» не должна признаваться объектом исключительных прав. За обладателем такой информации должно закрепляться только право на конфиденциальность информации.

Обладателями информации с ограниченным доступом, составляющей коммерческую тайну, являются граждане-предприниматели и юридические

лица в связи с осуществлением ими предпринимательской деятельности, однако пользователями такой информации могут выступать и физические лица (не являющиеся индивидуальными предпринимателями).

Предлагается законодательное закрепление применения гражданско-правовой ответственности к нарушителю права на коммерческую тайну путем возложения на нарушителя — обязанности по выплате денежной компенсации обладателю информации, составляющей коммерческую тайну. Кроме того, законодательно внести пределы такой денежной компенсации для определения судом размера выплаты в случае невозможности точной оценки объема причиненных обладателю такой информации убытков. Вышеуказанные теоретические выводы и практические предложения основываются на проведенном сравнительно-правовом анализе отечественного законодательства, правоприменительной практики, а также опыта зарубежного стран и международно-правового регулирования отношений в сфере защиты информации с ограниченным доступом в предпринимательской деятельности.

Список используемой литературы и используемых источников

1. Амелин, Р. В. Информационное право в схемах. Учебное пособие / Р.В. Амелин, С.А. Куликова, С.Е. Чаннов. - М.: Проспект, 2016. – С. 93.
2. Атаян Г. Ю., Амвросова О. Н. Банковская тайна / Атаян Г. Ю., Амвросова О. Н. // Государственная служба и кадры. 2018
3. Антоновский М.В., Горбешко В.В. Особенности предоставления доступа к сведениям, составляющим банковскую, налоговую и коммерческую тайну // Скиф. 2019. №12-2 (40).
4. Бордак И.В., Росенко А.П. Разработка метода количественной оценки и прогнозирования безопасности информации ограниченного доступа на основе Марковских случайных процессов // Доклады ТУСУР. 2017. №4.
5. Всеобщая декларация прав человека: Декларация Генеральной Ассамблеей ООН от 10.12.1948// Российская газета. 10.12.1998
6. Галиев Р.С., Васильков К.А. Проблемы реализации государственными служащими конституционного права на свободную передачу и распространение информации в контексте практики Европейского суда по правам человека // Вестник экономической безопасности. 2017. №3.
7. Гогина Е.А., Смоленская О.А. Организация работы с документами, содержащими грифы ограничения доступа // Символ науки. 2017. №3.
8. Гражданский кодекс Российской Федерации (часть вторая): Федеральный закон от 26.01.1996 № 14-ФЗ (ред. от 27.12.2019, с изм. от 28.04.2020) // Собрание законодательства РФ. 29.01.1996. № 5, ст. 410.
9. Гражданский кодекс Российской Федерации (часть третья): Федеральный закон от 26.11.2001 № 146-ФЗ (ред. от 18.03.2019) // Российская газета. № 233, 28.11.2001.
10. Ельчанинова Н.Б. Проблемы совершенствования законодательства в сфере ограничения доступа к противоправной

информации в сети Интернет // Общество: политика, экономика, право. 2017. №12.

11. Закирова А.Р., Мухаметзянова А.М. Анализ дебиторской задолженности как инструмент повышения эффективности деятельности сельскохозяйственного предприятия / Закирова А.Р., Мухаметзянова А.М. // Профессия бухгалтера - важнейший инструмент эффективного управления сельскохозяйственным производством: Сборник научных трудов по материалам III Международной научно-практической конференции, посвященной памяти профессора В.П. Петрова 2014 г.

12. Иванова А.П. Организация систем защиты информации с ограниченным доступом // Вестник науки и образования. 2018. №14-1 (50).

13. Каминский А.М., Камалова Г.Г. Конфиденциальность в частной детективной деятельности: правовые и тактические вопросы обеспечения информационной безопасности частного сыска // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2018. №4 (44).

14. Камалова Г.Г. Пределы и ограничения в информационном праве России // Национальная безопасность / nota bene. 2020. №2.

15. Камалова Г.Г. Сравнительный Информационно-правовой анализ российского и зарубежного законодательства о коммерческой тайне // Финансовое право и управление. 2017. №1.

16. Конкина А.В., Страбыкина Ю.С., Татаринова Е.П. Эволюция научных представлений о правовом статусе директора юридического лица / Конкина А.В., Страбыкина Ю.С., Татаринова Е.П. // Вестник Волжского университета им. В.Н. Татищева. 2018. Т. 1. № 2. С. 109-116.

17. Конституция Российской Федерации: Принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 [Электронный ресурс] // Официальный текст Конституции РФ с внесенными поправками от 14.03.2020 опубликован на Официальном интернет-портале правовой информации http://www.pravo.gov.ru, 04.07.2020.

18. Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 30.12.2001 № 195-ФЗ (ред. от 11.06.2021) // Парламентская газета. № 2-5, 05.01.2002.

19. Клементьева В.С. Право на информацию как основа реализации системы основных прав и свобод человека и гражданина в киберпространстве // Вестник экономической безопасности. 2016. №2.

20. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А. В. Бриллианто-ва. - Москва: Проспект, 2017. - Т. 2. - С. 643.

21. Кириленко В.П., Алексеев Г.В. Противодействие идеологии современного терроризма // Управленческое консультирование. 2018. №5 (113).

22. Лузан С.Н. О вопросе цензуры в России - одного из видов ограничения права на информацию // Вопросы науки и образования. 2017. №9 (10).

23. Ловцов Д.А., Федичев А.В. Архитектура национального классификатора правовых режимов информации ограниченного доступа // Правовая информатика. 2017. №2.

24. Мавринская Т. В., Лошкарёв А. В., Чуракова Е. Н. DLP-системы и тайна личных переписок / Мавринская Т. В., Лошкарёв А. В., Чуракова Е. Н. // Интерактивная наука. 2017. №14.

25. Минбалеев А. В. Правовая охрана коммерческой тайны: очередная реформа законодательства / Минбалеев А. В. // Вестник УрФО. безопасность в информационной сфере № 2(16). 2015

26. Нардина О.В. Ограничение конституционного права на доступ к получению и распространению информации в сети "интернет" в связи с противодействием экстремизму и терроризму // Наука. Общество. Государство. 2017. №4 (20).

27. Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая

ответственность за правонарушения. Учебное пособие / В.К. Новиков. - М.: Горячая линия - Телеком, 2015. – С. 69.

28. О защите прав человека и основных свобод. Конвенция Заключена в г. Риме 04.11.1950 (с изм. от 13.05.2004) (вместе с "Протоколом [№ 1]" (Подписан в г. Париже 20.03.1952), "Протоколом № 4 об обеспечении некоторых прав и свобод помимо тех, которые уже включены в Конвенцию и первый Протокол к ней" (Подписан в г. Страсбурге 16.09.1963), "Протоколом № 7" (Подписан в г. Страсбурге 22.11.1984)) // Собрание законодательства РФ. 08.01.2001. № 2, ст. 163.

29. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 18.03.2019) // Российская газета. № 165, 29.07.2006.

30. О безопасности: Федеральный закон от 28.12.2010 № 390-ФЗ (ред. от 05.10.2015) // Российская газета. № 295, 29.12.2010.

31. Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 06.07.2016) // Российская газета. № 160, 18.08.1995.

32. О коммерческой тайне: Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 18.04.2018) // Российская газета. № 166, 05.08.2004.

33. Об акционерных обществах: Федеральный закон от 26.12.1995 № 208-ФЗ (ред. от 31.07.2020, с изм. от 24.02.2021) (с изм. и доп., вступ. в силу с 01.01.2021) // Российская газета. № 248, 29.12.1995.

34. О банках и банковской деятельности: Федеральный закон от 02.12.1990 № 395-1 (ред. от 30.12.2020) // Российская газета. № 27, 10.02.1996.

35. Основы законодательства Российской Федерации о нотариате: Федеральный закон (утв. ВС РФ 11.02.1993 № 4462-1) (ред. от 30.12.2020) // Российская газета. № 49, 13.03.1993.

36. О свободе совести и о религиозных объединениях: Федеральный закон от 26.09.1997 № 125-ФЗ (ред. от 02.12.2019) // Российская газета. № 190, 01.10.1997.

37. О кредитных историях: Федеральный закон от 30.12.2004 № 218-ФЗ (ред. от 31.07.2020) // Российская газета. № 2, 13.01.2005.

38. О государственной гражданской службе Российской Федерации: Федеральный закон от 27.07.2004 № 79-ФЗ (ред. от 08.12.2020) (с изм. и доп., вступ. в силу с 01.01.2021) // Российская газета. № 162, 31.07.2004.

39. Об адвокатской деятельности и адвокатуре в Российской Федерации: Федеральный закон от 31.05.2002 № 63-ФЗ (ред. от 31.07.2020) // Российская газета. № 100, 05.06.2002.

40. О средствах массовой информации: Закон РФ от 27.12.1991 № 2124-1 (ред. от 30.12.2020) (с изм. и доп., вступ. в силу с 01.01.2021) // Российская газета. № 32, 08.02.1992.

41. Об утверждении Перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) // Российская газета от 14.3.1997 г.

42. Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности: Постановление Правительства РФ от 03.11.1994 № 1233 (ред. от 06.08.2020) [Электронный ресурс] // СПС Консультант Плюс http://www.co№sulta№t.ru/docume№t/co№s_doc_LAW_54870

43. Об утверждении Порядка доступа к конфиденциальной информации налоговых органов: Приказ МНС РФ от 03.03.2003 № БГ-3-28/96 (Зарегистрировано в Минюсте РФ 26.03.2003 № 4335) [Электронный ресурс] // СПС Консультант Плюс: http://www.co№sulta№t.ru/docume№t/co№s_doc_LAW_41541

44. Пашнина Т.В. Дискуссионные аспекты определения термина «Право на информацию» // Вестник ЮУрГУ. Серия: Право. 2017. №2.

45. Паршуков М. И. Проблемы предоставления сведений, составляющих коммерческую тайну, участникам хозяйственных обществ // Мониторинг правоприменения. 2014. №2

46. Петрова Е.А. Ограничения свободы доступа детей к информации как пример законодательных ограничений (с позиции юридической техники) // Юридическая техника. 2018. №12.

47. Слесарев Ю.В., Лосяков А.В. Проблемы защиты конфиденциальной информации в сети интернет: правовой аспект // БГЖ. 2018. №1 (22).

48. Семейный кодекс Российской Федерации: Федеральный закон от 29.12.1995 № 223-ФЗ (ред. от 04.02.2021) // Российская газета. № 17, 27.01.1996.

49. Татаринова Е.П. Роль использования инновационных технологий в договорах купли-продажи / Татаринова Е.П. // Вопросы российского и международного права. 2018. Т. 8. № 10А. С. 47 -55.

50. Таможенный кодекс Евразийского экономического союза: Международный договор (приложение № 1 к Договору о Таможенном кодексе Евразийского экономического союза) // Официальный сайт Евразийского экономического союза http://www.eaeunion.org/, 12.04.2017

51. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 11.06.2021) // Собрание законодательства РФ. 17.06.1996, № 25, ст. 2954.

52. Феоктистов Д.Е. Вопросы обеспечения конфиденциальности в деятельности омбудсменов // Наука. Общество. Государство. 2020. №3 (31).

53. Щепотьев А.В. Влияние кредитной истории на стоимость действующего бизнеса // Имущественные отношения в РФ. 2019. №5 (212).

54. Червяковский А.В. Риски, возникающие вследствие ограничения права на доступ к информации // Юридическая техника. 2019. №13.

55. Червяковский А.В. Проблемы ограничения прав граждан на доступ к информации в сети "Интернет" // Юридическая техника. 2018. №12.

56. Яковлева И. А. Новый взгляд на предоставление доступа к конфиденциальной информации в предпринимательской деятельности: тенденции, принципы, требования к запросам, пути преодоления законодательных пробелов // Проблемы экономики и юридической практики. 2013. №5.

57. Ellsberg, Daniel (30 May 2014). "Daniel Ellsberg: Snowden would not get a fair trial – and Kerry is wrong". The Guardian. Retrieved 2014-09-26.

58. Goldsmith, Jack (29 September 2010). "Classified Information in Woodward's 'Obama's Wars'". Lawfare. Retrieved 5 September 2015.

59. Lerner, Brenda Wilmoth, & K. Lee Lerner, eds. Terrorism: Essential primary sources. Thomson Gale, 2006.

60. Myers, Steven Lee; Mazzetti, Mark (February 5, 2016). "Agencies Battle Over What Is 'Top Secret' in Hillary Cli№ton's Emails" – via NYTimes.com.

61. Priest, Dana; Arkin, William (19 July 2010). "A hidden world, growing beyond control". The Washington Post. Archived from the original on 20 July 2010. Retrieved 5 September 2015.