

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
**Федеральное государственное бюджетное образовательное учреждение
высшего образования**
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Юридический институт	Кафедра <u>«Частное и публичное право»</u>
Направление подготовки	<u>40.04.01 «Юриспруденция»</u>
Магистерская программа	<u>Гражданское право; предпринимательское право</u>

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему «Информация как объект гражданско-правового регулирования и
способы ее защиты в современных условиях»

Студент <u>23зююгм1</u>	_____	<u>Кипурова Ангелина Романовна</u>
	(подпись, дата)	(фио полностью)

Научный руководитель: к.ю.н., доцент ФГБОУ ВО _____ Казакова Е.Б.
(подпись, дата)

Консультанты:

по _____	_____	_____
(наименование раздела, звание, должность)	(подпись, дата)	(фамилия, инициалы)

по _____	_____	_____
(наименование раздела, звание, должность)	(подпись, дата)	(фамилия, инициалы)

Нормоконтролер: <u>к.ю.н., доцент</u>	_____	<u>Портнова Е. В.</u>
	(подпись, дата)	(фамилия, инициалы)

Рецензент <u>Индивидуальный предприниматель</u>	_____	<u>Ошкина О. А.</u>
(должность, место работы)	(подпись, дата)	(фамилия, инициалы)

Работа допущена к защите (протокол заседания кафедры от _____ № __)

Заведующий кафедрой <u>ЧиПП</u>	_____	<u>Казакова Е.Б.</u>
	(подпись)	(фамилия, инициалы)

Работа защищена с оценкой _____ (протокол заседания ГЭК от _____ № __)

Секретарь ГЭК	_____	<u>Вдовина Т. Е.</u>
	(подпись)	(фамилия, инициалы)

Пенза 2025 г.

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Юридический институт
Направление подготовки 40.04.01 «Юриспруденция»

УТВЕРЖДАЮ
Зав. кафедрой ЧиПП
_____/Казакова Е. Б./
01.12.2023 г.

ЗАДАНИЕ

на выпускную квалификационную работу студентки гр.№23зююгм1

Кипуровой Ангелины Романовны

1. **Тема работы:** Информация как объект гражданско-правового регулирования и способы ее защиты в современных условиях
2. **Научный руководитель:** к. ю. н., доцент Е.Б. Казакова
3. **Дата выдачи задания:** 01.12.2023
4. **Срок сдачи студентом законченной работы:** 22.12.2025
5. **Перечень подлежащих разработке вопросов:**
 - 5.1. Информация как объект гражданских прав: понятие и признаки.
 - 5.2. Классификация и правовые режимы информации.
 - 5.3 Договорные механизмы регулирования и защиты информации.
 - 5.4. Внедоговорные способы защиты информации в гражданском праве.
 - 5.5. Анализ судебной практики по защите информации в гражданских правоотношениях.
 - 5.6. Направления совершенствования гражданско-правового регулирования информации.

6. Консультанты по работе, с указанием относящихся к ним разделов работы

Раздел	Консультант	Подпись, дата	
		Задание выдал	Выполненное задание принял
Введение		01.12.2023 Казакова Е. Б	04.05.2024 Казакова Е. Б
Теоретико-правовые основы информации как объекта гражданско-правового регулирования		05.04.2024 Казакова Е. Б	09.09.2024 Казакова Е. Б
Гражданско-правовое регулирование оборота и защиты информации		09.09.2024 Казакова Е. Б	07.12.2024 Казакова Е. Б
Современные вызовы и перспективы развития правового регулирования информации		07.12.2024 Казакова Е. Б	15.09.2025 Казакова Е. Б
Заключение		15.09.2025 Казакова Е. Б	22.12.2025 Казакова Е. Б

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	5
1 ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИИ КАК ОБЪЕКТА ГРАЖДАНСКО ПРАВОВОГО РЕГУЛИРОВАНИЯ.....	8
1.1 Информация как объект гражданских прав: понятие и признаки.....	8
1.2 Классификация и правовые режимы информации.....	14
2 ГРАЖДАНСКО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБОРОТА И ЗАЩИТЫ ИНФОРМАЦИИ.....	27
2.1 Договорные механизмы регулирования и защиты информации.....	27
2.2 Внедоговорные способы защиты информации в гражданском праве.....	39
3 СОВРЕМЕННЫЕ ВЫЗОВЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИИ.....	50
3.1 Анализ судебной практики по защите информации в гражданских правоотношениях.....	50
3.2 Направления совершенствования гражданско-правового регулирования информации.....	57
ЗАКЛЮЧЕНИЕ.....	64
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	67

ВВЕДЕНИЕ

Актуальность темы исследования обусловлена возрастающим значением информации как самостоятельной нематериальной ценности, имеющей высокую экономическую и юридическую значимость в условиях цифровизации и стремительного развития информационных технологий.

В условиях цифровой экономики и активного развития технологий информация становится одним из ключевых ресурсов в гражданском обороте. Она используется как в предпринимательской деятельности, так и в повседневных правовых отношениях между гражданами и организациями. При этом правовая природа информации остаётся сложной и до конца не определённой.

Информация обладает особыми свойствами: она нематериальна, может существовать в неограниченном числе копий, передаваться мгновенно и независимо от территории. Эти особенности делают её регулирование с позиции традиционного гражданского права весьма затруднительным. Кроме того, информация может одновременно выступать как объект интеллектуальной собственности, коммерческой тайны, персональных данных, служебной или иной охраняемой законом тайны. Всё это требует комплексного подхода к определению её статуса и разработке эффективных правовых механизмов защиты.

Особую значимость приобретают вопросы защиты информации, в том числе в рамках договорных обязательств. В практике встречаются многочисленные случаи нарушения соглашений о конфиденциальности, незаконного распространения данных, а так же утечки сведений, составляющих коммерческую тайну.

В настоящий момент отношения, связанные с регулированием информации в гражданском обороте в Российской Федерации (далее - РФ) регламентируются в соответствии с:

- Гражданским кодексом РФ;

- Гражданским процессуальным кодексом РФ;
- Кодексом РФ об административных правонарушениях;
- Уголовным кодексом РФ.

Имеющаяся законодательная база в данной сфере не всегда позволяет обеспечить эффективные меры по борьбе с разнообразными формами нарушений в указанной области.

Объектом исследования являются общественные отношения, возникающие в процессе создания, оборота, защиты и использования информации в рамках гражданских правоотношений.

Предмет исследования составляют правовые нормы, регулирующие оборот и защиту информации в РФ.

Цель работы - комплексное гражданско-правовое исследование информации как объекта правового регулирования и правовых механизмов её защиты в современных условиях цифровой трансформации.

Цель работы определила постановку следующих исследовательских задач:

- проанализировать правовую природу информации как объекта гражданских прав;
- определить особенности договорного и внедоговорного видов защиты информации;
- рассмотреть классификацию и правовые режимы информации в гражданском праве;
- исследовать судебную практику по спорам, связанным с защитой информации;
- предложить направления по совершенствованию гражданско-правового регулирования информации и средств её защиты.

Общие теоретические вопросы гражданского права, а также вопросы правовой природы информации, условий её гражданско-правового оборота и защиты рассматривали в своих трудах: Е.В. Богданов, И.Л. Бачило, Н.В. Багрова, Б.М. Гонгало, С.П. Гришаев, В.А. Дозорцев, И.А. Зенин, М.Н.

Кузнецов, Д.С. Лебедева, С.Я. Малышев, А.П. Полянский, Е.А. Суханов, С.И. Сулова, С.К. Резников, В.А. Рясенцев, В.П. Шатров, Г.Ф. Шершеневич, А.Б. Черных, А.К. Юрченко, В.Ф. Яковлев А.О. Яценко, и другие.

Методологическую основу исследования составили такие общие методы научного познания, как: диалектический, метод анализа и синтеза, системный, так и частно-научные: сравнительно-правовой, формально-логический и др.

Апробация результатов исследования осуществлялась путем публикации научных статей:

1. Кипурова А.Р. Общие положения и правовое регулирование информации в гражданском праве // Актуальные проблемы гражданского права: сб. ст. по материалам регион. научно-практ. конф. Пенза : Изд-во ПГУ, 2024.

2. Кипурова А.Р. Электронные сделки и смарт-контракты в системе гражданского права // Актуальные проблемы гражданского права: сб. ст. по материалам регион. научно-практ. конф. Пенза : Изд-во ПГУ, 2025.

Структура работы обусловлена целями и задачами исследования. Магистерская диссертация состоит из введения, трех глав, объединяющих шесть параграфов, заключения и списка использованных источников.

1 ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИИ КАК ОБЪЕКТА ГРАЖДАНСКО ПРАВОВОГО РЕГУЛИРОВАНИЯ

1.1 Информация как объект гражданских прав: понятие и признаки

В вопросе того является ли информация объектом гражданских правоотношений, следует отметить, что рассматривая историю внесения изменений в ст. 128 ГК РФ, информация была объектом гражданских прав в первоначальной редакции ГК РФ 1994 года. Однако, в результате введения в действие ч. IV ГК РФ с 1 января 2008 года, информация была исключена из объектов гражданского права.¹

Граница между информацией и результатами интеллектуальной деятельности стерлась, что, собственно, и стало причиной исключения информации из перечня объектов гражданских прав.²

Признание информации в качестве самостоятельного объекта гражданского права продолжает оставаться предметом научной дискуссии. На сегодняшний день в юридическом сообществе отсутствует единая точка зрения относительно правовой природы информации, а также её возможного статуса в системе объектов гражданских прав. Учитывая огромную роль информации в современных общественных и экономических отношениях, а также стремительное развитие цифровых технологий, необходимость детального теоретического и нормативного осмысления данного феномена приобретает особую актуальность.

Ученый-правовед Е.А. Суханов определяет информацию в качестве самостоятельного объекта гражданских прав, отмечая при этом, что объектом гражданских прав будет являться далеко не любая информация.³

¹ Колохина В. М. Информация как объект гражданских прав // Международный журнал гуманитарных и естественных наук. – 2023. – № 6-1. - (81). – С. 74.

² Тухватулина А. Г. Информация как объект гражданских прав // Вестник молодых ученых и специалистов Самарского университета. – 2020. – № 2. - (17). – С. 246.

³ Афанасьева А. А. Информация как объект гражданского права // Вопросы российской юстиции. – 2020. – № 9. – С. 1156.

Некоторые ученые и юристы, такие как Черных А.Б., Малышев С.Я., в своих исследованиях отмечают, что правовая связь информации и её носителя имеет практическое значение в случае, когда важен сам носитель, а не только содержание. Примером могут быть данные, зафиксированные на бумажном или электронном носителе, которые обладают материальной формой, требующие защиты от несанкционированного доступа.

Закрепление сведений на материальном носителе не преобразовывает информацию в материальный объект, она по-прежнему остаётся неосязаемым благом.¹

В теории права объектом правовых отношений считаются те вещи, на которые направлены субъективные права и обязанности участников отношений, либо то, что является основанием для их возникновения.

Согласно ч. 1 ст. 5 Федерального закона «Об информации, информационных технологиях и о защите информации», информация может быть объектом различных типов правовых отношений, например - публичных или гражданских. Это означает, что информация может быть включена в любые правовые отношения. В данном контексте выделены публичные и гражданские правоотношения, что соответствует традиционному делению всех правоотношений на частные, где государство не является стороной или присутствует только в роли владельца имущественных интересов без властного воздействия, и публичные, в которых одним из участников является государство, действующее через свои органы и основанное на властных полномочиях.

Действующее законодательство закрепляет принцип свободного использования и передачи информации между лицами, за исключением случаев, когда иное предусмотрено федеральными законами. В частности, доступ к информации или порядок её распространения могут быть ограничены специальными нормативными актами. Данная правовая конструкция

¹ Тухватулина А.Г. Информация как объект гражданских прав // Вестник молодых учёных и специалистов Самарского университета. - 2020. - №2. - (17). - С. 248.

соотносится с положениями пункта 1 и 2 ст. 129 Гражданского кодекса Российской Федерации (в редакции Федерального закона "О внесении изменений в подраздел 3 раздела 1 части первой Гражданского кодекса Российской Федерации" от 02.07.2013 № 142-ФЗ), где устанавливается, что объекты гражданских прав могут свободно переходить от одного субъекта к другому посредством универсального правопреемства (например, в результате наследования или реорганизации юридического лица), так и иными способами, при условии отсутствия ограничений их оборотоспособности. Более того, указанные нормы допускают возможность установления законом особых ограничений в отношении определённых объектов, включая случаи, когда владение ими допускается лишь определённым субъектам или осуществление сделок на основании специального разрешения. Таким образом, правовой режим информации в аспекте её передачи и использования тесно связан с общими принципами оборотоспособности объектов гражданского права.

Действительно, информация является неотъемлемым элементом современных общественных отношений. С развитием технологий и глобализацией значение информации стремительно возрастает, и она становится объектом правового регулирования, в том числе в рамках гражданского права.

На сегодняшний день, Гражданский кодекс РФ не содержит положений, которые прямо регулировали бы передачу или обмен информацией как самостоятельным объектом гражданских прав. Это создает вакуум в правовом поле и приводит к ситуации, когда информация регулируется в рамках иных правовых категорий, таких как результаты интеллектуальной деятельности и нематериальные блага.

Более того, положения статьи 5 Федерального закона «О коммерческой тайне» позволяют увидеть, что информация, не подлежащая защите в качестве коммерческой тайны (например, данные о нарушении законодательства или о задолженностях по выплатам заработной платы и социальных пособий),

зачастую не поддается документированию или иному материальному выражению.¹

Соотношение информации с нематериальными благами представляет собой весьма сложный вопрос. Согласно статье 150 ГК РФ, к нематериальным благам относятся такие ценности, как жизнь и здоровье, достоинство личности, личная неприкосновенность, честь и доброе имя, деловая репутация, неприкосновенность частной жизни и жилища, личная и семейная тайна, свобода передвижения и выбора места пребывания и жительства, имя гражданина, авторство и иные нематериальные блага, которые принадлежат гражданину с момента рождения или в силу закона, не подлежат отчуждению и не могут быть переданы другим лицам иным способом.²

Среди нематериальных благ особое значение имеет личная и семейная тайна, поскольку они тесно связаны с информацией, что подчёркивается рядом статей Гражданского кодекса Российской Федерации и сопутствующими правовыми актами. Личная и семейная тайна как нематериальные блага имеют информационную природу и заключаются в сведениях, которые их носитель стремится сохранить конфиденциальными. Личная тайна охватывает сведения о частной жизни, которые человек не желает разглашать: это может быть информация о личных переживаниях, состоянии здоровья, религиозных убеждениях, политических взглядах и т. д. Семейная тайна включает в себя данные о взаимоотношениях внутри семьи, финансовом состоянии её членов, их привычках и личной жизни в семейном кругу.

Личная и семейная тайна, являясь объектом гражданских прав, содержит внутри себя другой объект - информацию о частной жизни и семейных отношениях.

В свою очередь, такие нематериальные блага, как доброе имя, честь, достоинство и деловая репутация, также тесно связаны с определёнными

¹ Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (ред. от 08.08.2024) // Собрание законодательства РФ. - 09.08.2004. - № 32. - Ст. 3283.

² Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 №51-ФЗ (ред. от 01.08.2025) // Собрание законодательства РФ. - 05.12.1994. - № 32. - Ст. 3301.

сведениями о личности. Эти блага формируются на основе информации о человеке.

На сегодняшний день информация пересекается с правовым регулированием интеллектуальной собственности и нематериальных благ, что приводит к необходимости чёткого разделения этих понятий. Без ясных критериев такого разделения возникает риск неопределённости и сложности в защите прав на информацию в рамках гражданского оборота.

Информация обладает дополнительным характером, то есть она может выступать частью или средством выражения этих объектов. Например, информация, связанная с результатами интеллектуальной деятельности, нередко является их неотъемлемым компонентом, так как создание нематериальных благ или интеллектуальных продуктов сопряжено с мыслительной деятельностью и обменом сведениями.

Некоторые авторы также отмечают, что информация может входить в состав других объектов гражданских прав, а именно: нематериальных благ и результатов интеллектуальной деятельности.¹

Информация и результаты интеллектуальной деятельности представляют собой два вида нематериальных объектов, тесно связанных с человеческой мыслительной деятельностью. Оба объекта возникают в процессе интеллектуального труда и часто реализуются через материальные носители. Эта схожесть приводит к ряду проблем правового разграничения между ними, что является важным аспектом регулирования в рамках гражданского права. Особую значимость эта проблема приобрела в период становления понятия "информация" как объекта гражданских прав в российском законодательстве (1995–2008 гг.), когда было важно определить границы между информацией и результатами интеллектуальной деятельности.

Информация и результаты интеллектуальной деятельности действительно имеют много общего, поскольку их происхождение связано с

¹ Болтанова Е. С., Имекова М. П. Генетическая информация в системе объектов гражданских прав // Lex Russica. - 2019. - № 6. - С. 114.

мыслительной деятельностью человека. Оба объекта нематериальны, тесно связаны с личностью автора и реализуются через определённые носители, например, документы, чертежи, литературные произведения, патенты и т.д.

Однако ключевое различие между ними заключается в характере правового регулирования. Результаты интеллектуальной деятельности регулируются через специальные нормы авторского, патентного и смежного законодательства. Информация же долгое время рассматривалась более обобщённо и в отечественном праве впервые вопрос о её включении в число объектов гражданских прав был поставлен в 1995 году. Тогда под информацией понимались данные, не подпадающие под специальные режимы охраны, например, служебная или коммерческая тайна, а также иная информация, не подпадающая под другие правовые категории.

Информация обладает уникальными характеристиками, выделяющими её среди других объектов гражданских прав:

Во-первых, она нематериальна, то есть не имеет собственной физической формы и существует лишь в виде знаний, фактов или данных. Для её фиксации используются материальные носители, но сами сведения не идентичны носителю. Уничтожение бумаги или электронного файла не ведёт к исчезновению самой информации.

Во-вторых, информация в отличие от вещей не «изнашивается» при использовании. Один и тот же объем данных может применяться многократно, сохраняя свое количество и содержание. При этом ценность сведений зависит от их актуальности, со временем они могут устаревать или, наоборот, приобретать особую значимость.

В-третьих, информация имеет различную ценность в зависимости от сферы применения. В одних случаях она обладает коммерческой ценностью для компании (например, технологии, финансовые отчёты), а в других - социальной (сведения о политических процессах, социальных изменениях).

И наконец, информация легко воспроизводится и передаётся, что одновременно является её преимуществом и слабым местом. С одной стороны,

она доступна широкому кругу лиц, но с другой стороны возникает риск неконтролируемого копирования и распространения, особенно в цифровой среде. Именно это обстоятельство объясняет актуальность разработки специальных правовых механизмов её защиты.

Подводя итог, можно отметить, что в современном праве информация постепенно укрепляет своё значение как объект гражданских прав. Её нематериальный характер, а так же способность многократно использоваться обществом требуют дальнейшего нормативного уточнения и развития правовых подходов, что подтверждается анализом законодательства и судебной практики.

1.2 Правовые режимы и классификация информации

Классификация информации в гражданском праве играет значительную роль, так как именно от её вида зависят способы защиты и ответственность при нарушении соответствующих норм. В основе регулирования лежат как общие положения Гражданского кодекса РФ, так и ряд специальных законов. Так, например, Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» закрепляет базовые принципы обращения с информацией, Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» регулирует порядок обработки и защиты персональных данных, а так же Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», он определяет режим охраны сведений, имеющих действительную или потенциальную коммерческую ценность. В совокупности эти и другие акты формируют правовую основу, позволяющую разграничивать различные виды информации и устанавливать для них специальные режимы защиты.

Одним из ключевых подходов к классификации является разделение информации на общедоступную (открытую) и информацию, доступ к которой

ограничен федеральными законами.¹ Исходя из вышесказанного, различают общий и специальный правовые режимы информации.

Под правовым режимом информации обычно понимают установленный законом порядок её обращения. Речь идёт о нормах, которые регулируют владение и использование сведений, их передачу другим лицам, а также условия ограничения доступа к информации. Правовой режим позволяет определить место информации среди объектов гражданских прав и очертить допустимые пределы её оборота. Кроме того, он определяет меры ответственности за нарушения, связанные с неправомерным использованием или разглашением информации.

Общий правовой режим информации применяется к сведениям, которые не подлежат специальным ограничениям, и доступ к ним свободен. Общие принципы этого режима установлены в части 4 статьи 29 Конституции РФ и позволяют любому лицу свободно искать, получать, передавать, производить и распространять информацию любым законным способом.²

В своей работе Рожкова М.А. подчеркивает: «Иными словами, п. 2 ст. 7 Закона об информации для всех видов общедоступной информации – закон не предусматривает изъятий – установлен общий правовой режим: в отношении такой информации разрешен любой способ использования, ограничивается только ее распространение – оно должно осуществляться в соответствии с требованиями соответствующего федерального законодательства.»³

Что касается специального правового режима, он применяется к сведениям, требующих защиты из-за конфиденциальности или потенциальной угрозы для общества. Например, это государственная тайна, персональные

¹ Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 01.09.2025) "Об информации, информационных технологиях и о защите информации // Собрание законодательства РФ. - 31.07.2006. - № 31. - (1 ч.). - Ст. 3448.

² Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Собрание законодательства Российской Федерации. - 2009. - № 4. - Ст. 445.

³ Рожкова М. А. «Общедоступная информация», «открытые данные» и «персональные данные, разрешенные субъектом для распространения» – что это такое и как они между собой связаны? [Электронный ресурс] // URL: https://zakon.ru/blog/2021/1/13/obschedostupnaya_informaciya_otkrytye_dannye_i_personalnye_dannye_razreshennye_subektom_dlya_raspros (дата обращения: 11.07.2025).

данные, коммерческая тайна, а также информация в сфере интеллектуальной собственности, каждая из которых регулируется отдельными законами и требует соблюдения строгих ограничений и разрешений для доступа к ним.

Далее рассмотрим более подробно следующую классификацию информации.

Информация в зависимости от порядка ее предоставления или распространения подразделяется:

1) Информация, свободно распространяемая.

Этот вид информации может быть получен, использован и распространен любыми лицами без ограничений, если иное не предусмотрено федеральными законами. К данной категории относятся нормативно-правовые акты, официальные государственные данные, информация о деятельности государственных органов, а также иные сведения, доступ к которым не ограничен;

2) Информация, предоставляемая по соглашению лиц, участвующих в соответствующих отношениях.

Данный вид информации становится доступным только при наличии соглашения между сторонами, например, в рамках договора. Это может быть информация, относящаяся к коммерческой тайне, служебные сведения, данные, передаваемые в ходе делового сотрудничества. В соответствии с Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне», такие сведения защищены, а доступ к ним возможен только на основании соглашения сторон.

3) Информация, которая в соответствии с федеральными законами подлежит предоставлению или распространению.

Законодательство предусматривает перечень сведений, обязательных к раскрытию. Например, в соответствии с Федеральным законом от 08.08.2001 № 129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей», сведения из Единого государственного реестра юридических лиц (ЕГРЮЛ) являются общедоступными. Аналогично,

налоговая отчетность, экологическая информация, результаты государственных закупок и др., подлежат обязательному раскрытию в силу закона.

4) Информация, распространение которой в Российской Федерации ограничивается или запрещается.

К данной категории относятся сведения, распространение которых ограничено в целях защиты конституционного строя, прав и свобод граждан, обеспечения безопасности государства. В частности, Федеральный закон от 21.07.1993 № 5485-1 «О государственной тайне» регулирует доступ к сведениям, отнесенным к государственной тайне, а Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» устанавливает ограничения на обработку и распространение персональных данных граждан.

В настоящее время в судах различных инстанций периодически рассматриваются уголовные дела, связанные с опубликованием в открытой печати и других, в том числе электронных, средствах массовой информации сведений, составляющих государственную тайну.¹

Перейдем к следующей классификации, которая более конкретно раскрывает каждый вид информации, это классификация – по субъектам владения. Основой любого информационного взаимодействия является информационная деятельность его участников.²

В гражданском праве информация может принадлежать различным субъектам, от чего зависит объем их прав на использование, распоряжение и защиту информации. В зависимости от принадлежности информация может классифицироваться на:

- Информация, принадлежащую государству.

Государство является владельцем значительного объема информации, которая может иметь как открытый, так и ограниченный доступ. Такая

¹ Гулак М. Л. О некоторых аспектах распространения и защиты информации // Моя профессиональная карьера. – 2020. – Т. 2. - № 9. – С. 135.

² Дженакова Е.В. О классификации субъектов правоотношения по распространению информации // Российское право: образование, практика, наука. – 2021. – № 3. – С. 53.

информация играет ключевую роль в обеспечении функционирования государственных институтов, регулировании общественных отношений и обеспечении национальной безопасности.

Законодательство Российской Федерации предусматривает, что определенная информация, находящаяся в распоряжении государственных органов, должна быть общедоступной. Например, нормативно-правовые акты, статистические данные, сведения о деятельности органов власти и иные сведения, которые не относятся к категории ограниченного доступа.

Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации" регулирует порядок предоставления такой информации. Кроме того, Конституция РФ в статье 29 гарантирует право каждого гражданина на доступ к информации о деятельности государственных органов.

Часть информации, находящейся в распоряжении государства, имеет закрытый характер и охраняется в силу ее стратегической значимости. Федеральный закон от 21 июля 1993 года № 5485-1 "О государственной тайне" определяет перечень сведений, которые могут быть отнесены к государственной тайне, включая данные в сфере обороны, внешней политики, разведки и контрразведки, а также экономической и научно-технической деятельности. Несанкционированное распространение такой информации влечет за собой ответственность, в том числе и уголовную.

Помимо государственной тайны, существует информация, которая не является секретной, но имеет ограниченный доступ в силу служебной необходимости. Это касается внутренней документации органов власти, а также баз данных. Доступ к такой информации регулируется внутренними регламентами и нормативными актами государственных органов.

В настоящее время данные правоотношения регулируются Положением о порядке обращения со служебной информацией ограниченного распространения, а также актами федеральных органов исполнительной власти (муниципальных органов), принятыми в развитие данного Положения.

Указанные акты не используют термин "служебная тайна", а оперируют понятием "служебная информация ограниченного распространения".¹

- Информация, принадлежащая юридическим лицам (коммерческая тайна);

Юридические лица, включая коммерческие и некоммерческие организации, также обладают значительным объемом информации, которая может представлять коммерческую ценность, быть объектом интеллектуальной собственности или относиться к внутренним корпоративным сведениям.

Одной из ключевых категорий информации, принадлежащей юридическим лицам, является коммерческая тайна. Федеральный закон от 29 июля 2004 года № 98-ФЗ "О коммерческой тайне" регулирует установление режима конфиденциальности информации в организациях. Под коммерческой тайной понимаются сведения, имеющие коммерческую ценность и не являющиеся общедоступными, например, производственные технологии, маркетинговые стратегии, финансовые отчеты.

Для защиты коммерческой тайны предприятие должно официально установить соответствующий режим, включающий ограниченный доступ к информации, использование соглашений о неразглашении (NDA) и технические меры защиты.

Информация может быть объектом исключительных прав, если она относится к интеллектуальной собственности. Согласно части четвертой Гражданского кодекса РФ (ГК РФ), к объектам интеллектуальных прав относятся произведения науки, литературы и искусства, программное обеспечение, базы данных, изобретения, промышленные образцы и товарные знаки, секреты производства (ноу-хау) и тд.

Защита интеллектуальной собственности осуществляется через регистрацию прав, заключение лицензионных договоров и судебную защиту в

¹ Борисов М.А. Проблемы правового регулирования информации в современных условиях // Конституционное и муниципальное право. - 2023. - № 6. - С. 41.

случае незаконного использования. Незаконное использование интеллектуальной собственности влечет гражданско-правовую, административную и уголовную ответственность.

- Информация, принадлежащая физическим лицам;

Физические лица обладают правами на личную, персональную и иную информацию, защищаемую гражданским законодательством. Важно отметить, что в условиях цифровизации вопросы защиты личных данных и информации о частной жизни приобретают особую актуальность.

Федеральный закон от 27 июля 2006 года № 152-ФЗ "О персональных данных" регулирует обработку и защиту персональных данных граждан. Персональные данные включают любую информацию, относящуюся к определенному физическому лицу: фамилию, имя, отчество, дату рождения, адрес, паспортные данные, номер телефона и тд.

Действующее законодательство устанавливает важное правило, согласно которому персональные данные имеют особый правовой режим, и запрещает свободный оборот такого рода сведений, кроме случаев выраженного согласия субъекта персональных данных, а также других случаев, прямо установленных в законе. Все это позволяет сделать вывод о том, что персональные данные находятся под юридической защитой и в кибернетическом пространстве.¹

Сбор, обработка и хранение персональных данных допускаются только при наличии согласия субъекта данных, за исключением случаев, предусмотренных законом. Например, обработка данных без согласия возможна в рамках исполнения договора, соблюдения законодательства или защиты жизненно важных интересов гражданина.

Информация о частной жизни гражданина охраняется статьей 152.2 ГК РФ и включает сведения о семейных отношениях, состоянии здоровья, личной переписке и иных аспектах жизни, не подлежащих публичному раскрытию без согласия субъекта.

¹ Рассолов И. М. Право и Интернет. Теория кибернетического права: монография / 3-е изд., доп.- Москва: Норма: ИНФРА-М. - 2022. - С. 304.

Нарушение права на неприкосновенность частной жизни может повлечь за собой гражданско-правовую ответственность, включая возмещение морального вреда. Кроме того, Конституция РФ (ст. 23 и ст. 24) гарантирует защиту частной жизни и персональных данных граждан.

Следующая классификации информации- по форме существования.

Информация как объект гражданско-правового регулирования может существовать в различных формах, каждая из которых определяет способы ее фиксации, хранения, распространения и защиты. В российском законодательстве не закреплена единая классификация информации по форме существования, однако на основе анализа нормативных актов и научных исследований можно выделить четыре основные категории: документированная, не документированная, цифровая и биометрическая информация. Каждая из этих форм обладает особыми правовыми характеристиками, влияющими на ее гражданско-правовую защиту.

1. Документированная информация – это информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать. Она играет ключевую роль в гражданском обороте, поскольку может служить доказательством в суде, подтверждать наличие прав и обязанностей, а также быть объектом различных правовых сделок.

Процесс занесения информации на материальный носитель проходит в соответствии с установленным специальными ответственными за это госорганами порядком. Данная процедура осуществляется сразу с несколькими важными задачами, такими, как: установление владельца информации, обеспечение условий защиты информации в процессе ее обработки, будущего хранения и возможной передачи.¹

Например, документированная информация может быть представлена в различных формах: письменные документы (договоры, официальные акты, личная переписка, бухгалтерская отчетность); графические и изобразительные

¹ Фастович Г. Г. К вопросу о формировании правовых режимов информации в Российской Федерации // Аграрное и земельное право. – 2021. – № 10. - (202). – С.8.

материалы (чертежи, схемы, карты, фотографии); аудио- и видеозаписи (протоколы заседаний, свидетельские показания, зафиксированные в аудиоформате).

Документированная информация может иметь юридическую силу, если она соответствует требованиям законодательства.

Документированная информация охраняется нормами гражданского законодательства, а также специализированными законами. Например, персональные данные в документированной форме подлежат защите по Федеральному закону № 152-ФЗ "О персональных данных", а коммерческая тайна – по Федеральному закону № 98-ФЗ "О коммерческой тайне".

2. Недокументированная информация – это информация, которая не включена в перечень основных документов и не имеет классификационного кода, подготовленная в произвольной форме.¹ Она существует в устной форме, в виде знаний, навыков, опыта, а также интуитивных представлений.

К недокументированной информации относятся:

- Устные переговоры и договоренности, не закреплённые в письменной форме;
- Идеи и замыслы, не выраженные в объективной форме;
- Навыки и компетенции специалистов, не зафиксированные в документах.

Недокументированная информация может приобретать юридическое значение при наличии доказательств ее существования. Например, свидетельские показания могут подтвердить факт устной договоренности.

Недокументированная информация в большинстве случаев не подлежит прямой правовой защите, так как отсутствуют материальные доказательства ее существования. Однако при определенных условиях она может защищаться через институт интеллектуальной собственности. Например, если идея

¹ Нуриддинов Д. Р. Структура и содержание информационного обеспечения кадастра недвижимости // Основные принципы развития землеустройства и кадастров: материалы XVIII Всероссийской научно-практической конференции, Новочеркасск, 27–29 апреля 2021 года. Том Выпуск 18. – Новочеркасск: Новочеркасский инженерно-мелиоративный институт имени А.К. Кортунова ФГБОУ ВПО «Донской государственный аграрный университет». - 2021. – С. 182.

получает материальное выражение (фиксируется в патенте, статье, чертеже), то она приобретает правовую охрану.

3. Цифровая информация.

С развитием информационных технологий выделилась отдельная категория – цифровая информация. Она представлена в виде электронных данных, существующих на цифровых носителях и передаваемых через сети связи.

Цифровая информация обычно включает в себя:

- Электронные документы (например, договоры, юридически значимые переписки, цифровые копии бумажных документов);
- Программы для ЭВМ и базы данных, защищенные нормами авторского права;
- Цифровой контент такой как изображения, видеоматериалы, тексты, аудиофайлы).

Защита цифровой информации обеспечивается различными законодательными актами. Основные из них: Федеральный закон от 27 июля 2006 г., № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 №230-ФЗ.

Цифровая информация, будучи относительно новым явлением, получает все большее признание в праве и требует особых средств защиты в условиях цифровизации общества.

Применительно к гражданскому обороту информация может быть предметом обязательств, объектом защиты гражданских прав, а также составлять существенные условия договоров (например, лицензионных соглашений, договоров о неразглашении и т. д.). В связи с этим необходимо четкое понимание правового режима информации, включая ее классификацию, способы регулирования и механизмы защиты.

Стоит отметить что, в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ "Об электронной подписи", документ, подписанный электронной подписью, обладает юридической силой, аналогичной бумажному носителю.

4. Биометрическая информация.

Данный вид информации представляет собой данные, которые фиксируют уникальные физиологические или поведенческие характеристики человека, позволяющие его идентифицировать. В условиях технологического прогресса и повсеместного распространения информационных технологий биометрическая информация играет важную роль в системах безопасности, доступе к различным сервисам и идентификации пользователей. Однако её использование также связано с определёнными правовыми рисками, что требует специфического правового регулирования.

Каждый из видов физиологических или поведенческих характеристик является уникальным для каждого человека и может использоваться для его идентификации или аутентификации в различных системах, таких как системы контроля доступа, мобильные приложения, онлайн-сервисы и т.д.

В России принят ряд нормативно-правовых документов, содержание которых регулирует использование биометрических данных, в которых определены важнейшие положения о персональных данных с выделением биометрических данных.¹

В соответствии с ч 1. ст. 11 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", обработка биометрических персональных данных допускается только при наличии письменного согласия субъекта персональных данных. Это положение подчеркивает, что биометрическая информация рассматривается как категория персональных данных,

¹ Панова С. М. Биометрия: содержание биометрии и ее применение в России // Экономика и инновации: Сборник статей участников межвузовской научно-практической конференции. В 3-х томах, Москва, 21–23 ноября 2023 года. – Москва: Российский экономический университет им. Г.В. Плеханова. - 2024. – С. 176.

требующая особой защиты, аналогично персональным данным специальной категории.

Закон также обязывает оператора персональных данных обеспечивать защиту биометрических данных от неправомерного или случайного доступа, уничтожения, изменения, блокировки, копирования и распространения. Кроме того, в случае нарушения этих требований возможна административная или уголовная ответственность.

Следует отметить, что вопросы использования биометрических персональных данных получили подробное регулирование в Федеральном законе от 29 декабря 2022 г. № 572-ФЗ "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации.

Данный федеральный закон регулирует порядок функционирования Единой биометрической системы (ЕБС) и определяет, каким образом осуществляется идентификация и аутентификация граждан с использованием биометрических данных. В законе подробно описаны этапы этой процедуры, а также распределены полномочия между государственными органами, контролирующими сферу защиты информации. В частности, значительная роль отведена Федеральной службе безопасности, Федеральной службе по техническому и экспортному контролю и Роскомнадзору, которые отвечают за надзор и соблюдение установленных требований.

Таким образом, разграничение видов информации позволяет более ясно представить, какие правовые инструменты применяются для её свободного оборота и какие механизмы предусмотрены для защиты сведений, требующих особого режима. Наибольшее значение имеют нормы, регулирующие доступ к сведениям, которые составляют коммерческую или государственную тайну, а также к персональным и биометрическим данным, поскольку именно в этих

сферах наиболее остро проявляется необходимость баланса между интересами субъектов гражданских отношений и публичными интересами.

Классификация информации по субъектам владения показывает, что её правовой режим напрямую зависит от того, кому она принадлежит. Так, государственная информация регулируется в особом порядке, здесь необходимо учитывать одновременно требования прозрачности и задачи государственной безопасности. Если речь идёт о юридических лицах, то основной акцент делается на охране экономических интересов. Для этого используются такие правовые механизмы, как режим коммерческой тайны и институт интеллектуальной собственности. В отношении физических лиц главным объектом регулирования выступают персональные данные и сведения о частной жизни, что предопределяет необходимость специальных правил их обработки, хранения и защиты.

Отдельного внимания заслуживает классификация информации по форме её существования. Современные процессы цифровизации, внедрение биометрических технологий и переход на электронный документооборот ставят новые задачи перед гражданским правом. Они требуют не только уточнения правового статуса информации в новых формах, но и разработки практических инструментов её защиты в условиях стремительно развивающейся цифровой среды.

2 ГРАЖДАНСКО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБОРОТА И ЗАЩИТЫ ИНФОРМАЦИИ

2.1 Договорные механизмы регулирования и защиты информации

Заклучение договоров выступает одним из основных способов правовой защиты информации. Именно через них стороны могут определить, кто и на каких условиях имеет право пользоваться сведениями, передавать их или ограничивать доступ. Кроме того, договор позволяет заранее закрепить ответственность за нарушение установленных правил, что особенно важно в условиях активного оборота данных.

В договорных отношениях можно выделить несколько направлений, которые чаще всего используются для защиты информации.

1. Конфиденциальность информации.

На практике одним из первых условий становится обязательство сторон сохранять в тайне полученные сведения. Чаще всего это выражается в соглашении о неразглашении (NDA), где указываются границы использования данных, запрет на их передачу третьим лицам, а также последствия нарушения этих правил. Такие положения важны не только для коммерческой тайны, но и для любых данных, утечка которых может нанести ущерб.

2. Защита интеллектуальной собственности.

Договор может включать и положения о защите объектов интеллектуальной собственности: авторских прав, патентов, товарных знаков и других объектов интеллектуальной собственности. В практике такие условия имеют принципиальное значение, так как нарушение исключительных прав часто влечёт серьёзные убытки. Поэтому стороны обычно заранее оговаривают порядок использования результатов интеллектуальной деятельности и меры ответственности - от штрафов и компенсаций до расторжения договора.

3. Защита персональных данных.

В условиях цифровизации особое внимание уделяется защите персональных данных. Заключение договора с обязательствами по соблюдению законодательства в области защиты персональных данных становится неотъемлемой частью правовых отношений. В тексте договора стороны могут установить как организационные, так и технические меры защиты, а также закрепить санкции за нарушения, связанные с утечкой или ненадлежащей обработкой данных.

Таким образом, договор выступает не просто формальной процедурой, а действенным механизмом регулирования отношений в сфере защиты информации. Его содержание напрямую зависит от характера обмениваемых сведений и интересов сторон, что позволяет выстраивать гибкую и в то же время юридически надёжную систему гарантий.

Договоры, направленные на защиту информации, могут заключаться с различными участниками правоотношений - от сотрудников и партнёров до клиентов и поставщиков. В этих договорах обычно фиксируются не только обязанности сторон по сохранению конфиденциальности, но и порядок обращения с данными, например, правила обмена, доступ к информации, условия её хранения или последующего уничтожения. Важным элементом таких соглашений является определение ответственности за возможные утечки информации. Нарушение условий о неразглашении может повлечь не только имущественные потери, но и серьёзные правовые последствия для сторон.

В рамках гражданского законодательства Российской Федерации договоры, регулирующие защиту информации, играют ключевую роль в обеспечении безопасности данных, их конфиденциальности и предотвращении несанкционированного использования. Эти механизмы защиты являются важной составляющей правового поля, направленного на регулирование использования и оборота информации, что особенно актуально в условиях стремительного развития технологий и глобализации информационных процессов.

Перейдем к подробному рассмотрению договорных механизмов.

Соглашение о неразглашении информации (NDA). Основной целью подписания NDA является предупреждение утечки конфиденциальной информации, используемой в деловых отношениях при передаче информации, а также создание правовых оснований для возможности компенсации убытков в случае нарушения соглашения одной из сторон.¹

Термин NDA (от англ. Non-Disclosure Agreement) обозначает соглашение о неразглашении информации. Такие соглашения могут оформляться либо в виде самостоятельного договора, либо как отдельный раздел в рамках основного договора между сторонами. В тексте NDA, как правило, подробно фиксируется перечень информации, подлежащей защите, обязательства участников соглашения по соблюдению режима конфиденциальности, а также санкции за нарушение условий сохранения тайны.

NDA оформляется на основе норм гражданского права - как самостоятельный договор или как приложение к трудовому договору с работником, регулируя, в частности, вопросы защиты служебной, коммерческой или иной охраняемой информации.

Эффективность NDA в значительной степени зависит от того, насколько оно встроено в общую систему управления информационной безопасностью, действующую в организации. То есть, для надлежащего функционирования соглашение должно быть частью комплексной стратегии защиты информации, охватывающей не только юридические, но и технические аспекты обеспечения безопасности.

Организационно-правовая система предполагает наличие внутренних регламентов, должностных инструкций и иных документов, регулирующих порядок обращения с конфиденциальными сведениями. При этом положения

¹ Русецкая И. А. NDA как инструмент обеспечения конфиденциальности информации// Информационная безопасность: вчера, сегодня, завтра: Сборник статей по материалам III Международной научно-практической конференции. – Москва: Российский государственный гуманитарный университет. - 2020. – С. 41.

NDA могут распространяться и на технические меры защиты. Например, устанавливать запреты или ограничения на использование облачных сервисов, видеонаблюдения, а также требования по шифрованию данных.

Соглашения о неразглашении информации (NDA) в научной литературе классифицируются на две основные категории.

Первая категория представляет собой одностороннее соглашение, при котором одна сторона передает другой стороне определённые сведения с условием их сохранения в тайне от третьих лиц. Такой формат соглашений преимущественно используется в сфере трудовых правоотношений, когда работник получает доступ к перечню конфиденциальных данных и несет ответственность за их несанкционированное разглашение в соответствии с условиями заключенного договора.

Второй тип NDA представляет собой взаимное соглашение о неразглашении, заключающееся в том, что каждая из сторон передаёт другой стороне информацию, требующую защиты от раскрытия третьим лицам. На практике такие соглашения находят широкое применение в процессе создания совместных предприятий, слияния компаний или ведения стратегического партнёрства, где обе стороны обмениваются ценными данными и взаимно обязываются обеспечивать их конфиденциальность.

На сегодняшний день соглашения о неразглашении активно используются в области информационных технологий. NDA распространяются, в частности, на обязательства о сохранении в тайне исходного кода программного обеспечения, персональных данных пользователей, технической документации и других результатов интеллектуальной деятельности. Согласно условиям таких соглашений, раскрытие данных, независимо от формы их выражения — устной или письменной, строго запрещено.

NDA оформляется в виде гражданско-правового договора между физическими или юридическими лицами и может быть составлено в свободной форме.

В большинстве NDA между коммерческими компаниями указывается обязанность о возврате или уничтожении любой конфиденциальной информации по первому требованию передающей стороны или в случае расторжения NDA.¹

В российском праве на данный момент отсутствует установленный максимальный срок действия NDA. Это позволяет сторонам самостоятельно определить срок его действия: он может быть ограничен конкретной датой, либо установлен на определённый период времени. В практике делового оборота стандартной является фиксация срока действия NDA в пределах десяти лет.

Дополнительно некоторые соглашения предусматривают право правообладателя информации на односторонний отказ от условий NDA. Причем обязанность сохранять конфиденциальность может сохраняться даже после расторжения основного трудового договора между сторонами.

С точки зрения российского законодательства, для эффективной защиты информации в рамках NDA необходимо соблюдение ряда обязательных условий: четкое определение периода действия обязательств о неразглашении, подробная регламентация прав и обязанностей сторон по поддержанию режима конфиденциальности, а также ясное и недвусмысленное определение перечня информации, подлежащей охране.

Таким образом, соглашения о неразглашении остаются одним из наиболее действенных инструментов правового регулирования защиты информации, особенно в сферах, где конфиденциальность данных имеет важное значение для сохранения конкурентных преимуществ.

Лицензионные соглашения. В современных условиях цифровой экономики правовая охрана компьютерных программ приобретает особую значимость, особенно в случаях, когда разработанное программное

¹ Девярых Н. П. Защита конфиденциальной информации путем подписания соглашения о неразглашении // Эволюция российского права: Материалы XIX Международной научной конференции молодых ученых и студентов, Екатеринбург, 29–30 апреля 2021 года / Уральский государственный юридический университет. – Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования "Уральский государственный юридический университет". - 2021. – С. 615.

обеспечение предназначено для использования широким кругом пользователей. Одним из наиболее распространённых и эффективных юридических инструментов, применяемых для защиты прав на исходный код программы, является лицензионный договор. Этот механизм получил широкое признание как в правовой практике Российской Федерации, так и в международной деловой среде.

Согласно статье 1235 Гражданского кодекса Российской Федерации, лицензионным договором признаётся соглашение, в соответствии с которым одна сторона — лицензиар, обладающий исключительными правами на результат интеллектуальной деятельности или средство индивидуализации, — предоставляет или обязуется предоставить другой стороне, то есть лицензиату, право использования соответствующего объекта в пределах, оговорённых договором.¹ Такое соглашение позволяет устанавливать рамки использования интеллектуального продукта, не отчуждая при этом исключительных прав, что делает данный тип договора принципиально отличным от договора об отчуждении исключительного права, где такие права полностью переходят к другой стороне.

Лицензионный договор обладает рядом характерных юридических признаков: он является двусторонним, консенсуальным и возмездным. Это означает, что договор считается заключённым с момента достижения соглашения по его существенным условиям, а также предполагает встречные обязательства сторон и получение вознаграждения за предоставление прав на использование интеллектуальной собственности.

Право использования того или иного объекта интеллектуальной собственности, согласно условиям, указанным в договоре, составляет предмет лицензионного договора.²

¹ Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 27.07.2025) // Собрание законодательства РФ. - 25.12.2006. - № 52. - (1 ч.). - Ст. 5496.

² Стеблина Е.К., Попов В.В. Юридические особенности исключительной лицензии. Защита прав сторон такого лицензионного договора // Вестник науки №6. - (75). - том 1. - 2024. - С. 722.

Особую актуальность лицензионные договоры приобретают в контексте регулирования прав на программное обеспечение. Они позволяют автору или правообладателю чётко определить условия, при которых допускается использование продукта, включая ограничения на его воспроизведение, распространение, модификацию, а также на доступ к исходному коду. Кроме того, такие договоры нередко содержат положения о соблюдении режима конфиденциальности, что обеспечивает дополнительную защиту правомочий владельца программы.

Среди разновидностей лицензионных соглашений особое место занимает так называемая ординарная (простая) лицензия, при которой лицензиар предоставляет лицензиату право использовать объект интеллектуальной собственности, но при этом сохраняет за собой право предоставлять аналогичные лицензии третьим лицам.

Во-вторых, (с некоторой долей условности) сублицензионный договор, согласно которому лицензиат с согласия лицензиара предоставляет третьему лицу (сублицензиату) право использования результата интеллектуальной деятельности или средства индивидуализации в пределах тех прав и тех способов использования, которые предусмотрены лицензионным договором для лицензиата (п. 1, 2 ст. 1238 ГК РФ);¹

Рассмотрим следующий вид – это открытая лицензия. Прежде всего, под открытой лицензией понимается договор, заключаемый по правилам договора присоединения, в рамках которого автор либо иной правообладатель (лицензиар) предоставляет всем заинтересованным лицам — лицензиатам — право на использование произведения науки, литературы или искусства на условиях простой (неисключительной) лицензии. Данная форма лицензии регламентируется п.1 ст.1286.1 ГК РФ.

Следующей разновидностью, имеющей более ограниченное и строго регламентированное применение, выступает принудительная лицензия.

¹ Рожкова М.А. О различиях между лицензионным договором и пользовательским соглашением // Журнал Суда по интеллектуальным правам. - 2024. - Декабрь. - № 4. - (46). - С. 122.

Данный механизм не является распространённым и применяется исключительно при наличии совокупности юридических обстоятельств, которые образуют соответствующий правовой состав. Особенности регулирования принудительной лицензии закреплены в статье 1362 Гражданского кодекса Российской Федерации.

Ключевым основанием для предоставления такой лицензии является факт длительного неиспользования патентообладателем принадлежащего ему объекта патентных прав, что влечёт за собой создание дефицита на рынке соответствующих товаров, работ или услуг. Такая ситуация оценивается как препятствующая нормальному обороту технологий и не отвечающая интересам общества, а также экономики в целом.

В случае возникновения подобного положения заинтересованное в использовании объекта лицо должно обратиться к правообладателю с предложением заключить лицензионный договор на разумных и добросовестных условиях. Это предложение должно сопровождаться доказательствами того, что лицо обладает технической и организационной возможностью эффективно использовать объект патентного права.

Если правообладатель отказывается от заключения договора либо игнорирует обращение, заинтересованное лицо получает право на обращение в суд с требованием о предоставлении ему неисключительной лицензии. Рассмотрев доводы сторон и установив наличие всех необходимых условий, суд может вынести решение, обязывающее правообладателя заключить лицензионный договор. При этом суд самостоятельно определяет условия предоставления лицензии, руководствуясь принципами разумности, соразмерности и баланса интересов сторон.

В соответствии с положениями статьи 1236 Гражданского кодекса Российской Федерации, лицензионные соглашения могут различаться по объему передаваемых прав, что позволяет выделить два основных типа лицензий: простую (неисключительную) и исключительную.

Простая (или неисключительная) лицензия предполагает предоставление лицензиату права на использование результата интеллектуальной деятельности или средства индивидуализации без ограничения для лицензиара использовать объект самостоятельно либо предоставлять аналогичные лицензии другим лицам. При этом по умолчанию, если иное не указано в договоре, лицензия считается неисключительной. Ограничения, устанавливаемые в рамках такой лицензии, могут соответствовать тем, что применяются и к исключительной форме лицензирования.

Неисключительная лицензия крайне удобна в случаях массового распространения продукта интеллектуальной деятельности, когда у конечных потребителей не возникает необходимость ограничения права лицензиара на выдачу лицензий другим лицензиатам.¹

Далее рассмотрим особенности исключительной лицензии.

Исключительная лицензия (пп. 2 п. 1 ст. 1236 ГК РФ) предоставляет лицензиату определенный объем прав: лицензиар обязуется не заключать аналогичных соглашений с третьими лицами. Однако российское законодательство не требует, чтобы лицензиар полностью отказывался от самостоятельного использования объекта лицензирования. Часть четвертая ГК РФ ограничивается лишь обязанностью не предоставлять лицензии иным лицам, что, по сути, не препятствует самому лицензиару осуществлять использование объекта в тех же пределах, что и лицензиат, при условии, что иное не предусмотрено соглашением. Таким образом, правообладатель сохраняет за собой исключительное право на объект и может самостоятельно реализовывать его в гражданском обороте, а также защищать свои интересы, не нарушая условий заключённого лицензионного договора.

¹ Горбунова М. В. Особенности лицензионного договора в сфере авторского и смежных прав. Открытая лицензия // Вызовы современности и стратегии развития общества в условиях новой реальности: Сборник материалов XVIII Международной научно-практической конференции, Москва, 30 июня 2023 года. – Москва. - 2023. – С. 88.

В российской практике допускается значительная договорная свобода в установлении параметров использования лицензии. В договоре стороны вправе определить географические границы действия лицензии, способы использования объекта, срок её действия, запрет на предоставление сублицензий, а также иные условия, ограничивающие права лицензиата в соответствии с принципом диспозитивности гражданского права.

Отдельного внимания заслуживает вопрос правового восприятия лицензионных соглашений в сфере программного обеспечения среди конечных пользователей. В постсоветский период, особенно в начале 2000-х годов, когда стали массово распространяться программные продукты на физических носителях (CD, DVD), многие разработчики внедрили практику обязательного подтверждения согласия с лицензионным соглашением в электронном формате. Перед началом установки программного обеспечения пользователю предлагалось ознакомиться с текстом лицензионного договора, содержащимся во всплывающем окне, и выразить своё согласие, отметив соответствующую графу. Тем не менее, несмотря на формальное выражение согласия, большинство пользователей соглашение не читали, воспринимая его как техническое препятствие к установке, а не как юридически значимый документ.

В настоящее время технология распространения программ претерпела изменения: цифровые продукты всё чаще приобретаются и скачиваются через интернет-платформы и магазины приложений. Однако общий уровень правовой культуры в вопросе ознакомления с лицензионными условиями остаётся низким. Пользователи по-прежнему склонны игнорировать содержание лицензионных соглашений, не осознавая их правовую значимость, в том числе возможные ограничения, касающиеся передачи, модификации или коммерческого использования программного продукта.

Подобное отношение пользователей к лицензионному договору может привести к закономерным последствиям. Так, обратимся к одному из наиболее распространенных видов нарушений исключительного права —

«софтлифтинг».¹ Под данным термином понимается установка одной и той же копии легально приобретённой программы на несколько устройств, вопреки положениям лицензионного соглашения, регулирующего порядок использования данного программного продукта.

Характерным примером софтлифтинга может служить ситуация, при которой один пользователь приобретает лицензионную копию программного обеспечения, а затем осуществляет её установку не только на собственное устройство, но также передаёт её другому лицу, например, знакомому или коллеге. В рассматриваемом случае программное обеспечение фактически используется двумя пользователями, несмотря на то, что производителем была предоставлена лицензия только на одного конечного пользователя.

Такое поведение нарушает положения договора-оферты, заключаемого при приобретении или установке программного продукта, и прямо противоречит условиям, определяющим количество допустимых установок, а также запрет на распространение программного обеспечения третьим лицам без соответствующего разрешения правообладателя.

Договоры с положениями о коммерческой тайне. Информация, составляющая коммерческую тайну, - это сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.²

¹ Боднарук Ю.М. Способы нарушения исключительного права правообладателя на программу для ЭВМ через призму понятия «Пиратства» // Вестник ВУиТ. - 2021. - №2. - (98). – С. 185.

² Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (ред. от 08.08.2024) // Собрание законодательства РФ. - 09.08.2004. - № 32. - Ст. 3283.

Сведения могут быть признаны коммерческой тайной только при выполнении ряда условий:

Во-первых, информация должна обладать реальной или потенциальной экономической ценностью для её обладателя. Такая ценность проявляется в том, что использование сведений даёт организации конкурентные преимущества, то есть, позволяет повысить эффективность деятельности, снизить затраты или разработать более выгодные способы работы. В качестве примеров можно привести уникальные производственные технологии, разработанные внутри компании методики переговоров или оригинальные схемы организации бизнеса.

Во-вторых, рассматриваемая информация не должна находиться в свободном доступе либо быть общеизвестной. При этом сам факт потенциальной возможности получения аналогичных сведений иными лицами не исключает их охраны. Важнее, чтобы обладатель действительно предпринимал меры для сохранения конфиденциальности.

В-третьих, необходимо официальное введение режима коммерческой тайны. Для этого на практике используются самые разные приёмы: специальные пометки на документах, утверждённые правила внутреннего документооборота, ограничение круга работников, имеющих доступ к секретным данным, назначение ответственных лиц и т.п. Без этих действий даже ценная и закрытая информация не будет отнесена к режиму коммерческой тайны.

Кроме того, договорные механизмы играют важную роль в защите конфиденциальных сведений. Через трудовые, подрядные и иные гражданско-правовые соглашения стороны могут заранее определить, какие именно сведения относятся к конфиденциальным, как они должны использоваться и какие последствия наступят в случае их разглашения. Такой подход позволяет урегулировать возможные споры ещё до их возникновения и тем самым повысить уровень защищённости данных в деловой практике.

Особого внимания заслуживают договоры, содержащие положения о коммерческой тайне. Они не только фиксируют обязанности сторон по сохранению секретности, но и напрямую влияют на конкурентоспособность компании, так как препятствуют незаконному использованию деловых и технологических разработок.

Договорные механизмы, как и любой другой правовой институт, требуют тщательного подхода и учета специфики каждой конкретной сделки. Только при правильном оформлении, с учётом действующего законодательства, такие соглашения действительно обеспечивают надёжную правовую защиту.

В целом, договорные способы защиты информации представляют собой важный элемент правового регулирования в условиях цифровизации и глобализации. Они помогают не только обеспечить безопасность сведений, но и поддерживать баланс интересов участников гражданских отношений.

2.2 Внедоговорные механизмы регулирования и защиты информации

Внедоговорные механизмы - это правовые способы защиты информации, которые не основаны на договоре между сторонами, а вытекают из закона, правовых норм или публичного интереса. Сейчас эта сфера активно развивается в условиях цифровизации, увеличения информационных рисков и киберугроз.

Наиболее распространённые виды внедоговорных механизмов в российской правовой системе включают:

1. Конституционные и публично-правовые механизмы;

Конституция Российской Федерации закрепляет основополагающие права личности, среди которых особое место занимает право на защиту частной жизни. В соответствии со ст. 23 и ст. 24 Конституции РФ, каждому человеку гарантируется неприкосновенность частной жизни, охрана личной и

семейной тайны, а также защита тайны переписки, телефонных переговоров и иных видов коммуникаций, включая электронные сообщения.

Особенностью данных гарантий является их безусловный характер: они предоставляются каждому гражданину и не требуют заключения специальных соглашений или договоров между субъектами. Это означает, что защита прав в данной сфере осуществляется не через частно-правовые механизмы, а посредством публично-правовых институтов, уполномоченных государством обеспечивать соблюдение конституционных положений.

Механизмы реализации этих прав включают в себя, прежде всего, обращение в судебные органы - как способ восстановления нарушенных прав и получения компенсации за вред, причинённый их нарушением. Кроме того, значимую роль играют органы прокуратуры, осуществляющие надзор за соблюдением законности, в том числе в сфере охраны частной жизни. Наряду с ними действует и институт Уполномоченного по правам человека в Российской Федерации, к которому граждане могут обратиться в случае нарушения их личных прав и свобод, включая право на защиту частной жизни.

С развитием информационных технологий появились и новые способы передачи сообщений между людьми в самых разных формах – текстовых сообщений в социальных сетях и «мессенджерах», текстовых сообщений, а также файлов, отправленных посредством электронной почты и облачных хранилищ, видеозвонков и др.¹ Однако именно расширение каналов коммуникации породило новые юридические вызовы, связанные с обеспечением конфиденциальности, контролем за обработкой персональных данных, а также защитой от несанкционированного доступа и утечки информации.

Верховный Суд Российской Федерации признаёт подлежащей защите любую коммуникацию, содержащую сведения, полученные с нарушением закона, независимо от её содержания и формы. В частности, в пункте 6

¹ Бажанов Е. С. Защита права тайны на переписку и обмена информацией в период цифровизации общества// Безопасность. Управление. Искусственный интеллект. – 2024. – Т. 4. - № 4. - (4). – С. 2.

Постановления Пленума Верховного Суда РФ от 25 декабря 2018 г. № 46 прямо указано, что наличие в объекте посягательства сведений, составляющих личную или семейную тайну, не влияет на наступление ответственности. Уголовное преследование возможно за само нарушение тайны коммуникации. Это свидетельствует о том, что правовая охрана распространяется не только на традиционные формы переписки (почтовые, телефонные), но и на новые цифровые каналы обмена информацией - мессенджеры, электронную почту, облачные сервисы и иные средства коммуникации, активно используемые в условиях цифровизации.

2. Гражданско-правовые механизмы;

Согласно ст. 1064 ГК РФ, вред, причиненный личности или имуществу гражданина, а также вред, причиненный имуществу юридического лица, подлежит возмещению в полном объеме лицом, причинившим вред.¹ Это положение охватывает и случаи несанкционированного распространения конфиденциальной информации, нарушения права на неприкосновенность частной жизни, разглашения персональных данных или коммерческой тайны без договора.

В случае вторжения в частную жизнь, распространения персональных данных или иных форм неправомерного вмешательства, гражданин может потребовать взыскания компенсации морального вреда (ст. 151 ГК РФ). Такая компенсация направлена не на восстановление утраченного имущества, а на возмещение страданий, вызванных нарушением личных прав.

Ярким примером может служить ситуация, когда публикуются фотографии частного характера в СМИ или социальных сетях, это может служить основанием для иска о компенсации морального вреда за вторжение в частную жизнь.

Согласно ст. 150 и ст. 152 Гражданского кодекса РФ, каждому гражданину обеспечивается охрана таких нематериальных благ, как честь,

¹ Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. - 29.01.1996. - № 5. - Ст. 410.

достоинство и деловая репутация. Эти ценности подлежат судебной защите в случае распространения о гражданине ложных или порочащих честь и достоинство сведений. Особенно актуальным этот механизм стал в условиях развития цифровой среды и социальных сетей, где информация распространяется мгновенно и часто без возможности предварительного контроля.

Итак, если лицо понесло фактические убытки в результате незаконного распространения информации, оно вправе требовать компенсацию на основании статьи 15 Гражданского кодекса РФ. При этом необходимо доказать факт нарушения, причинно-следственную связь и размер убытков.

Например, сотрудник покидает компанию и передаёт конфиденциальную маркетинговую стратегию конкурирующей организации, которая начинает использовать её в своих интересах. Владелец информации может взыскать убытки, возникшие из-за потери конкурентных преимуществ.

Так же, стоит отметить, что Гражданский кодекс допускает применение мер самозащиты, в том числе в информационных отношениях (ст. 14 ГК РФ). Это может выражаться в блокировке доступа к цифровым платформам, самостоятельном изъятии информации из общего доступа, уведомлении провайдеров об удалении нарушающего материала и т.п.

К внедоговорным механизмам также относятся законодательные нормы, устанавливающие автоматическую охрану определённых категорий информации. Например, генетические данные гражданина защищаются без необходимости заключения специального соглашения между пациентом и медицинским учреждением. Это вытекает из требований закона и возлагает ответственность на организацию независимо от соглашения сторон.

Судебной практике, к сожалению, известны случаи грубых нарушений принципа конфиденциальности: несанкционированное раскрытие медицинских сведений работодателям, кредиторам, страховщикам, несогласованное с пациентом сообщение их его родственникам и иным лицам. Вопросы соблюдения врачебной тайны неоднократно были предметом

рассмотрения Конституционным Судом РФ в аспектах правомерности обработки персональных данных, допустимости получения таких сведений работодателями, отказа от предоставления документации пациенту о его психическом здоровье, возможности получения информации представителем и др. Статистические данные также подтверждают многочисленные прецеденты пренебрежения режимом врачебной тайны, причем самыми разнообразными способами, включая размещение информации в сети Интернет.¹

4. Уголовно-правовые меры;

Современное информационное общество характеризуется широким распространением и доступностью сведений, значительная часть которых имеет открытый характер и предназначена для неограниченного круга пользователей. Однако наряду с публичной информацией в правовом пространстве существует категория сведений, к которым установлен режим ограниченного доступа. Такие сведения получили в законодательстве и правоприменительной практике наименование - информация ограниченного распространения. К ней относятся:

1. Конфиденциальная информация. Так, согласно статье 2 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», под конфиденциальностью информации понимается обязательство лица, получившего доступ к определённым сведениям, не раскрывать их третьим лицам без согласия их владельца.²

Ст. 272 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации, которая также может быть конфиденциальной.³

¹ Крюкова Е.С. Врачебная тайна в аспекте охраны генетической информации // Правовое государство: теория и практика. - 2021. - №2. - (64). – С. 13.

² Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 01.09.2025) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. - 31.07.2006. - № 31. - (1 ч.). - Ст. 3448.

³ Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 17.11.2025) // Собрание законодательства РФ. - 17.06.1996. - № 25. - Ст. 2954.

В соответствии с пунктом 4 статьи 5 Федерального закона от 20 апреля 1995 года № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов», к числу охраняемых сведений относятся данные о лицах, находящихся под государственной защитой, а также информация об их имуществе и мерах, направленных на обеспечение их безопасности.¹

Нарушение режима конфиденциальности в указанных случаях влечёт за собой уголовную ответственность, что подчеркивает высокий уровень охраны данной информации. Так, статья 311 Уголовного кодекса Российской Федерации устанавливает ответственность за разглашение сведений о мерах безопасности, применяемых в отношении защищаемых лиц, а статья 320 УК РФ - за разглашение сведений о лицах, подлежащих защите, и их служебной деятельности. Эти положения направлены на обеспечение личной безопасности сотрудников правоохранительных и контрольных органов, а также лиц, находящихся под особой охраной государства.

2. Служебная информация ограниченного распространения. Нормативное регулирование порядка работы с такой информацией осуществляется, прежде всего, на основании Положения о порядке обращения со служебной информацией ограниченного распространения. К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами.² Данный акт распространяется на федеральные органы исполнительной власти, а также на

¹ Федеральный закон от 20.04.1995 № 45-ФЗ (ред. от 28.02.2025) "О государственной защите судей, должностных лиц правоохранительных и контролирующих органов" // Собрание законодательства РФ. - 24.04.1995. - № 17. - Ст. 1455.

² Постановление Правительства РФ от 3 ноября 1994 г. № 1233 (ред. от 08.10.2024) "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" // Собрание законодательства РФ. - 25.07.2005. - № 30. - (ч. II). - Ст. 3165.

специальные уполномоченные органы, осуществляющие управление в ключевых отраслях - в частности, в сфере использования атомной энергии и космической деятельности.

Особое внимание уделяется юридическим последствиям нарушения режима обращения с данной категорией информации. В случаях, когда такие нарушения совершаются по вине должностного лица и приводят к значимым негативным последствиям, законодательство предусматривает уголовную ответственность за халатность. (ст. 293 УК РФ).

3. Информация, имеющая гриф «особой важности», «совершенно секретно» и «секретно». Степени секретности сведений и грифы секретности носителей этих сведений, порядок засекречивания сведений и их носителей регламентируются Законом Российской Федерации «О государственной тайне». Уголовная ответственность наступает за передачу, собирание, похищение или хранение в целях передачи документов, содержащих государственную тайну (ст. 275, 276 УК РФ), ее разглашение (ст. 283 УК РФ), за незаконное получение сведений, составляющих государственную тайну (ст. 283.1 УК РФ), нарушение требований по защите государственной тайны (ст. 283.2 УК РФ), утрату документов, содержащих государственную тайну (ст. 284 УК РФ).¹

4. Информация, запрещенная к распространению. Так, согласно пунктам 6 и 7 статьи 10 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», под запрет подпадает информация, содержащая признаки пропаганды войны, возбуждения расовой, национальной, религиозной ненависти или вражды.

Российское законодательство последовательно ограничивает оборот информации, способной дестабилизировать общественные отношения, угрожать межнациональному миру или создавать условия для экстремистской деятельности. Эти меры реализуются через систему уголовно-правовых

¹ Мартыненко Н. Э. Уголовно-правовые средства охраны информации и противодействия информационным угрозам // Труды Академии управления МВД России. - 2022. - № 4. - (64). – С. 71.

санкций, направленных на защиту основ конституционного строя, прав и свобод граждан.

5. Административно-правовые меры;

Правовые основания для привлечения к административной ответственности в сфере информационного права закреплены в главе 13 Кодекса Российской Федерации об административных правонарушениях (далее - КоАП РФ), включающей более сорока составов административных правонарушений, прямо или косвенно затрагивающих информационные отношения.

В последние годы прослеживается устойчивая тенденция к усложнению форм и способов совершения административных правонарушений, что обусловлено активным использованием цифровых платформ, социальных сетей, мессенджеров и иных онлайн-средств коммуникации. На этом фоне особое значение приобретают нормы, направленные на противодействие правонарушениям, совершаемым с применением Интернета. К таким правонарушениям, в частности, относятся: правонарушения в области связи и информации (гл. 13 КоАП РФ); связанные с распространением сведений, порочащих честь и достоинство граждан; связанные с нарушением прав и свобод отдельных категорий граждан.

Данная правоприменительная практика предопределила необходимость дополнения Особенной части КоАП РФ новыми составами административных правонарушений, напрямую связанными с регулированием отношений, возникающих в цифровой среде. Эти изменения носят охранительный характер и направлены на формирование правовой среды, способной эффективно защищать общественные интересы от современных информационных угроз.

Важным административным инструментом контроля в данной сфере является деятельность Роскомнадзора - уполномоченного государственного органа, осуществляющего надзор за соблюдением законодательства о персональных данных и защите информации. На основании действующих

нормативно-правовых актов Роскомнадзор наделён правом принимать меры по ограничению доступа к информационным ресурсам, нарушающим установленный порядок обработки персональных данных.

Основными отличительными признаками административного информационного правонарушения являются: то, что объектом посягательства является порядок государственного управления в информационной сфере, связанный с обеспечением прав и свобод человека и гражданина; противоправность как признак, подчеркивающий направленность деяния на нарушение установленных нормами административного наказания правил поведения.¹

6. Защита интеллектуальной собственности.

Интеллектуальная собственность в Российской Федерации представляет собой совокупность исключительных прав, принадлежащих физическим или юридическим лицам на результаты интеллектуальной деятельности, а также средства индивидуализации товаров, работ, услуг и предприятий. Согласно статье 1225 Гражданского кодекса Российской Федерации, к объектам интеллектуальной собственности относятся произведения науки, литературы и искусства, изобретения, полезные модели, промышленные образцы, товарные знаки, программы для ЭВМ, базы данных, селекционные достижения, топологии интегральных микросхем, а также секреты производства (ноу-хау).²

Интеллектуальные права, будучи личными нематериальными и имущественными, подлежат особой охране со стороны государства, поскольку их нарушение зачастую наносит значительный экономический, репутационный или моральный ущерб правообладателям. В условиях цифровой экономики эффективная система защиты интеллектуальных прав

¹ Светова Е. К. Тенденции развития института административной ответственности за правонарушения в информационной сфере // Юридическая ответственность за правонарушения в информационной сфере: вопросы теории и практики: Сборник материалов Международной научно-практической конференции, Санкт-Петербург, 21 октября 2021 года. – Санкт-Петербург: Центр научно-информационных технологий "Астерион". - 2022. – С. 25.

² Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 23.07.2025) // Собрание законодательства РФ. - 25.12.2006. - № 52. - (1 ч.). - Ст. 5496.

приобретает стратегическое значение, будучи одним из факторов обеспечения национальной конкурентоспособности и инновационного развития.

Гражданский кодекс Российской Федерации в ст. 1252 предусматривает следующие способы защиты:

- признание права;
- пресечение действий, нарушающих право или создающих угрозу его нарушения;
- возмещение убытков или выплата компенсации;
- изъятие и уничтожение контрафактной продукции;
- публикация судебного акта о допущенном нарушении;

С 2013 года в России функционирует специализированный Суд по интеллектуальным правам, который рассматривает споры в кассационном порядке, а также по первой инстанции по искам, связанным с признанием недействительными актов Роспатента и аннулированием регистрации прав на объекты ИС.

Наличие специализированного судебного органа позволило сформировать единую и стабильную судебную практику, в том числе по делам о патентных спорах, недобросовестной конкуренции в сфере ИС и обороте контрафактной продукции.

В дополнение к гражданско-правовым способам действуют административные и уголовные меры, закреплённые в КоАП РФ и УК РФ. Так, статья 7.12 КоАП РФ предусматривает административную ответственность за незаконное использование объектов авторского права и смежных прав, нарушение прав на изобретения и промышленные образцы. В случае причинения значительного ущерба нарушитель может быть привлечён к уголовной ответственности по статьям 146 и 147 УК РФ, предусматривающим лишение свободы и штрафы.

Также активно используется механизм защиты авторских прав в интернете. При обнаружении нарушений правообладатель вправе обратиться в Роскомнадзор с заявлением о блокировке ресурса, распространяющего

контрафакт. Внесение сайта в реестр нарушителей может происходить в досудебном порядке при повторных нарушениях.

На данный момент в российском обществе происходит трансформация сферы интеллектуальной собственности, т.е. радикальное изменение формы, вида или направления движения права, приводящее к перестройке значительной части существующего правопорядка. Она будет включать в себя преобразование системы права (в т. ч. системы законодательства), а также последующее преобразование правовой культуры и правоприменения. Новые особенности мультимедийных продуктов подтолкнули к изменениям подходов регулирования. Это вызвало необходимость в адаптации частично устаревших гражданско-правовых норм под вновь созданные объекты творчества.¹

¹ Хмелевская А. С. Защита интеллектуальной собственности в условиях цифровой трансформации экономики// Экономика и управление инновациями. – 2024. – № 1. - (28). – С. 28.

3 СОВРЕМЕННЫЕ ВЫЗОВЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИИ

3.1 Анализ судебной практики по защите информации в гражданских правоотношениях

Самый ценный ресурс в наше время - это информация. Информация является стратегическим ресурсом в современном мире. Как говорил Найтан Майер Ротшильд, «кто владеет информацией, тот владеет миром». Обеспечение информационной безопасности имеет исключительную актуальность, что обусловлено значением информации, технологий, процессов информатизации в современном обществе.¹

Сегодня юридический фундамент информационного общества представлен множеством нормативно-правовых актов. При этом под информационной безопасностью понимается прежде всего сохранение оптимального баланса между доступностью данных, их целостностью и конфиденциальностью.

На практике дела данной категории оказываются весьма непростыми. При их рассмотрении суды сталкиваются с необходимостью назначения специальных экспертиз, анализа значительных объёмов доказательств и применения сложных технических знаний. Итоговый анализ судебных решений показывает отсутствие единого подхода, что во многом связано со спецификой каждого конкретного спора.

Защита способов передачи информации является необходимым условием и гарантией защиты информации и обеспечения безопасности коммуникации.²

¹ Старкова А. Г. Проблемы защиты информации правовыми средствами // Актуальные проблемы современной юридической науки и практики: Сборник трудов, посвященный 90-летию основания Астраханского государственного университета и 25-летию организации и деятельности юридического факультета Астраханского государственного университета, Астрахань. - 2022. - С. 139.

² Мещерякова М.А. Конституционное право на тайну коммуникации: понятие и содержание // Юридическая наука и правоохранительная практика. - 2020. - № 3. - (53). - С. 131.

Конституция Российской Федерации в ст. 23 к коммуникации относит переписку, телефонные переговоры, почтовые, телеграфные и иные сообщения. Более подробно эта гарантия раскрывается в специальных законах. В частности, Закон «О почтовой связи» в ст. 15 прямо указывает, что под охраной находятся не только сообщения, но и сопутствующие сведения - адреса пользователей, информация о почтовых отправлениях и денежных переводах и иные сообщения.¹ В свою очередь, Закон «О связи» в ст. 63 закрепляет, что защита распространяется на телефонные переговоры, почтовые отправления, телеграфные и иные сообщения, передаваемые по сетям электросвязи и сетям почтовой связи.²

Важно отметить, что правовая защита распространяется и на сам факт осуществления коммуникации. Ещё раньше юристы отмечали, что объектом охраны при тайне переписки является как текст писем, так и сам факт обмена ими. Сегодня это правило распространилось на новые средства связи и теперь под защитой находятся сведения о телефонных соединениях, а также информация, передаваемая через цифровые каналы. Такое расширение воспринимается как естественное продолжение права на тайну коммуникаций в условиях технологического прогресса.

При этом право на тайну коммуникации не действует в ситуациях, когда сами участники добровольно сделали переписку или переговоры публичными, например опубликовали их в открытых источниках. В таких ситуациях обязанность государства или операторов связи по обеспечению конфиденциальности не возникает, так как участники добровольно не пользуются правом на тайну коммуникации.

Рассмотрим дело, где суд рассматривал факт умышленного нарушения права гражданина на тайну переписки и иных сообщений, закреплённого в статье 23 Конституции РФ. Ибрагимов Т.А. при участии неустановленных

¹ Федеральный закон от 17.07.1999 № 176-ФЗ (ред. от 31.07.2025) "О почтовой связи" // Собрание законодательства РФ. - 19.07.1999. - № 29. - Ст. 3697.

² Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 31.07.2025) "О связи" // Собрание законодательства РФ. - 14.07.2003. - № 28. - Ст. 2895.

соучастников осуществил неправомерный перевыпуск SIM-карты, принадлежащей потерпевшему Комарицыну И.С., с использованием поддельного удостоверения личности. После активации SIM-карты он получил SMS-сообщения, содержащие коды доступа к мессенджерам WhatsApp и Telegram, и передал их соучастникам.

В результате указанных действий был осуществлён несанкционированный вход в личные аккаунты потерпевшего, что повлекло за собой как блокировку информации, так и нарушение тайны его личной переписки.

По итогам разбирательства Ибрагимов Т.А. был признан виновным в совершении преступлений, предусмотренных ч. 1 ст. 138 УК РФ (нарушение тайны переписки) и ч. 3 ст. 272 УК РФ (неправомерный доступ к компьютерной информации). Ему было назначено условное наказание в виде 2 лет 6 месяцев лишения свободы.¹

Таким образом, рассмотренное уголовное дело свидетельствует о наличии механизмов правовой защиты информации и конституционных прав граждан в Российской Федерации. Судебная практика подтверждает, что нарушение права на тайну переписки и сообщений квалифицируется как уголовно наказуемое деяние, а правоохранительные и судебные органы обладают средствами реагирования на подобные правонарушения в целях обеспечения информационной безопасности и защиты частной жизни.

Так же довольно значимой сферой правового регулирования выступает охрана авторских и смежных прав в Интернете, где нарушение прав обладателей интеллектуальной собственности приобрело массовый характер. Именно поэтому законодатель уделяет особое внимание выработке механизмов пресечения подобных нарушений.

¹ Решение Басманного районного суда № 01-0486/2023 от 12.07.2023 [Электронный ресурс] // URL: <https://www.mos-gorsud.ru/rs/basmannyj/services/cases/criminal/details/0539efc0-20b0-11ee-a079-c5d4cc8e4c60?docsDateFrom=13.07.2023&docsDateTo=13.07.2023&formType=fullForm> (дата обращения: 18.08.2025).

С принятием Федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» от 30.12.2020 № 530-ФЗ, защита авторских прав в Интернете стала гораздо эффективнее. Федеральный закон № 530-ФЗ расширил инструменты защиты правообладателей, дав им возможность оперативно реагировать на незаконное распространение контента. Прежде всего, был установлен внесудебный порядок защиты авторских прав в Интернете. Теперь владельцы интернет-ресурсов обязаны размещать на своих площадках данные о наименовании, адресе и контактной информации, куда могут поступать заявления о нарушении исключительных прав. Кроме того, им предоставлено право внедрять специальные электронные формы для подачи подобных обращений. Рассмотрение поступивших заявлений должно производиться в течение суток, и в случае подтверждения факта нарушения администрация сайта обязана удалить незаконно размещённый материал.

Помимо этого, расширена практика применения обеспечительных мер, если раньше ограничение доступа к ресурсу через суд применялось исключительно в отношении фильмов, то с мая 2015 года такая мера распространяется на все виды объектов авторских и смежных прав, за исключением фотографий. При повторяющихся нарушениях сайт может быть заблокирован окончательно, а исполнение таких решений возложено на Роскомнадзор совместно с операторами связи и хостинг-провайдерами.

Таким образом, защита авторских прав в Интернете осуществляется по двум каналам: внесудебному и судебному. Первый вариант является более быстрым и удобным для правообладателей, однако он не исключает возможности обращения в суд. Определённые сложности возникают в ситуации с ресурсами, созданными исключительно для незаконного распространения чужого контента. При этом крупные интернет-платформы, такие как социальные сети, уже выработали внутренние механизмы блокировки спорных материалов, что делает защиту прав более эффективной.

Стоит отметить, что в соответствии с положениями ст. 1270 ГК РФ, создатель произведения или его правообладатель обладает исключительным правом на использование результата творчества в любых формах и законных способах.

Однако на практике такие права нередко нарушаются, и наиболее распространённым способом их защиты выступает взыскание компенсации, включая компенсацию причинённого морального вреда.

Гражданин С. подал иск в суд к владельцу интернет-ресурса, заявив о нарушении его прав и требуя компенсации морального вреда. Основанием послужило то, что на сайте без его согласия и без указания авторства была размещена фотография, созданная им в период исполнения служебных обязанностей по трудовому договору с обществом – средством массовой информации. Исключительное право на данный снимок принадлежали работодателю.

Ранее арбитражным судом уже было принято решение в пользу работодателя, которому присуждена компенсация за незаконное использование указанной фотографии.

Суд первой инстанции отказал гражданину С. в удовлетворении требований, посчитав, что автор передал исключительное право на фотографию работодателю, и защита прав уже была обеспечена в рамках арбитражного процесса.

Апелляционная инстанция отменила это решение, обязав владельца сайта выплатить С. компенсацию морального вреда. При этом суд указал, что предметом иска С. являлась защита личного неимущественного права автора на имя, а не имущественных прав работодателя. Размещение фотографии без указания автора нарушило это право.

Суд кассационной инстанция поддержал выводы суда апелляционной инстанции, подчеркнув, что личное неимущественное право на имя (ст. 1228 ГК РФ) является неотчуждаемым и непередаваемым. Следовательно, даже в отношении служебных произведений автор сохраняет возможность защиты

своего права, в том числе путем взыскания компенсации морального вреда (ст. 1251 ГК РФ), независимо от того, что правообладатель уже защитил исключительное право в арбитражном суде (ст. 1301 ГК РФ).

Итак, подобные дела демонстрируют, что суды при разрешении споров учитывают специфику как исключительных прав, так и неотчуждаемых личных прав автора, формируя единообразие подходов в правоприменении.

Существенное место в судебной практике занимают споры, связанные с использованием и разглашением сведений, составляющих коммерческую тайну. Здесь также прослеживается необходимость поиска баланса между интересами работодателя, обеспечивающего сохранность конфиденциальных данных, и правами работников, имеющих доступ к такой информации.

Термин "разглашение информации" применительно к конфиденциальной ее разновидности может быть раскрыт через понятие "разглашение информации, составляющей коммерческую тайну", сформулированное в п. 9 ст. 3 Закона о коммерческой тайне. Согласно указанной норме разглашение информации, составляющей коммерческую тайну, представляет собой действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.¹

Важно понимать, что при рассмотрении случаев недобросовестной конкуренции правовое значение имеет прежде всего активное действие лица, допустившего разглашение охраняемой информации.

Следовательно, квалификация подобных ситуаций должна учитывать характер поведения работника, допустившего разглашение сведений, которые находятся под режимом коммерческой или иной тайны. Суды неоднократно отмечали, что увольнение в таких случаях является законным, если компания

¹ Городов О.А., Петров А.В., Шмигельская Н.А. Недобросовестная конкуренция: учебно-практическое пособие / под ред. О.А. Городова. М.: Юстицинформ. - 2020. - С. 324.

установила режим защиты информации, а сотрудник, нарушая его, направлял секретные данные на личную электронную почту.

Характерным примером нарушения режима охраны конфиденциальной информации является, когда руководитель одного из отделов, чьи должностные обязанности предполагали доступ к важной коммерческой информации, использовал эти сведения в нарушение установленного режима. Было установлено, что он систематически пересылал данные, относящиеся к коммерческой тайне, на электронные адреса третьих лиц, в том числе конкурентов компании. (Определение СК по гражданским делам Девятого кассационного суда общей юрисдикции от 25 апреля 2024 г. по делу № 8Г-2539/2024).¹

Судебная практика показывает, что даже «простая пересылка» документов может стоить человеку работы. Например, один из сотрудников отправил со служебной почты на личную Excel файл с клиентской базой, данные о сделках, а также персональные данные более трёхсот человек. (Определение СК по гражданским делам Шестого кассационного суда общей юрисдикции от 18 апреля 2024 г. по делу № 8Г-2305/2024[88-9086/2024]).²

Оба спора показали, что при надлежащем установлении режима коммерческой тайны суды склонны защищать интересы работодателя. Так, увольнение сотрудников, переславших на личные почтовые ящики информацию, содержащую конфиденциальные сведения, было признано правомерным, несмотря на их несогласие с подобной квалификацией своих действий.

Практика судов демонстрирует, что при надлежащем обеспечении работодателем режима коммерческой тайны любое нарушение его

¹ Определение Девятого кассационного суда общей юрисдикции по делу № 8Г-2539/2024 от 25 апреля 2024 г. [Электронный ресурс] // URL: https://9kas.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=12460863&case_uid=e74bbd91-7567-475c-aa24-b05bbadaa064&delo_id=2800001&new=2800001 (дата обращения: 27.08.2025).

² Определение Шестого кассационного суда общей юрисдикции по делу № 8Г-2305/2024[88-9086/2024] от 18 апреля 2024 г. [Электронный ресурс] // URL: https://6kas.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=6891335&case_uid=d3ec3736-5edc-4147-9acb-2c490644ec8f&delo_id=2800001&new=2800001 (дата обращения: 27.08.2025).

работниками, в том числе пересылка конфиденциальных данных на личные электронные адреса, квалифицируется как противоправное деяние. Подобные действия влекут применение дисциплинарных мер, включая увольнение. При этом в рамках законодательства, а именно Гражданского кодекса Российской Федерации и Федерального закона № 98-ФЗ «О коммерческой тайне», ключевое значение имеет как сам факт разглашения, так и подтверждение того, что работодатель предпринял все необходимые меры для охраны информации. Наличие внутренней документации и подписанных обязательств о неразглашении суды расценивают как существенные юридически значимые обстоятельства.

Таким образом, можно сказать, что информация сегодня, это не просто данные, а реальный ресурс, от которого зависит безопасность и развитие общества. Именно поэтому её охрана стала одной из ключевых задач права. Судебная практика подтверждает, что нарушения в сфере информационных отношений могут иметь самые разные формы - от неправомерного доступа к переписке до незаконного распространения контента или разглашения коммерческих секретов. Судебная практика демонстрирует готовность правоприменителей защищать как имущественные, так и личные неимущественные права, учитывая специфику каждого спора. В то же время остаются проблемные вопросы, связанные с защитой информации, но правовая система постепенно учится работать с вызовами информационного общества. Всё это указывает на необходимость дальнейшего совершенствования правовых механизмов защиты информации в условиях стремительного технологического развития.

3.2 Направления совершенствования гражданско-правового регулирования информации

Современные общественные отношения динамично развиваются под влиянием информационных технологий, именно поэтому вопрос о

закреплении в законе определения «информация» и включении ее в перечень объектов гражданских прав по-прежнему остаётся открытым и вызывает споры. Дело в том, что в российском праве пока что отсутствует единое, общепризнанное определение понятия информация. Учёные и практики предлагают разные подходы, в их позициях нередко прослеживаются существенные расхождения. В такой ситуации логичным представляется формирование перечня признаков информации, на основе которых можно было бы выработать более полное и согласованное определение.

Любопытно, что в последние годы термин «информация» всё чаще вытесняется словом «данные», которое многие специалисты считают более подходящим в условиях цифровизации. Данные рассматриваются с экономической точки зрения, что актуально не только для бизнеса, но и осуществления государственного управления.¹ При этом работа с ними практически всегда связана с использованием современных технологий, позволяющих обрабатывать большие объёмы сведений, которые человек самостоятельно обработать уже не способен.

В научной литературе подчёркивается, что дефиниция информации нуждается в уточнении. Исследователи предлагают рассматривать её не только в юридическом аспекте, но и через философские, социологические, политические и экономические категории. Такой междисциплинарный подход объясняется многогранностью самого явления: информация воспринимается по-разному в зависимости от отрасли права или сферы научных исследований.

Особое значение для регулирования в условиях цифровой среды приобретают свойства информации. Если ранее считалось, что она неразрывно связана с носителем, то сегодня под влиянием технологий эта зависимость меняется. Облачные сервисы и хранилища позволяют использовать информацию без привязки к конкретному физическому носителю. Зачастую источник её хранения даже невозможно определить, что наглядно

¹ Санникова Л.В., Харитонов Ю.С. Цифровые активы: правовой анализ: монография. М.: 4 Принт. - 2020. - С. 57.

демонстрирует отход от прежних представлений о фиксированности информации на носителе.

Впервые идея систематизировать нормы информационного законодательства в виде единого кодифицированного акта была озвучена ещё в 2014 году. Тогда Институт государства и права РАН предложил проект Информационного кодекса РФ, который вызвал интерес и получил позитивные отклики как в научной, так и в общественной среде. Однако политическая поддержка проекта оказалась недостаточной, что фактически остановило его дальнейшее продвижение.

Новый виток дискуссии развернулся в 2015–2017 годах, когда в публичном пространстве заговорили о Цифровом кодексе. Одним из первых сторонников был интернет-омбудсмен В.Н. Мавричев. В дальнейшем, в 2023 году, данную концепцию официально поддержало Министерство цифрового развития, связи и массовых коммуникаций РФ, заявив, что документ должен стать основой комплексного регулирования цифровых технологий и телекоммуникаций.

Цифровой кодекс должен объединить и систематизировать действующие нормы, касающиеся электронных сделок, облачных технологий, искусственного интеллекта, защиты персональных данных и иных сфер.

Проведённый анализ показывает, что регулирование информации в гражданском праве пока остаётся неполным и противоречивым. Исключение термина «информация» из перечня объектов гражданских прав в ст. 128 ГК РФ породило ситуацию, при которой нормы кодекса не согласуются с положениями Федерального закона «Об информации, информационных технологиях и о защите информации». В итоге в практике мы видим, что отдельные виды информации (например, персональные данные или сведения, относящиеся к коммерческой тайне) защищаются специальными законами, а другие фактически оказываются без должного правового режима.

Кроме того, современным законодательством не определены механизмы разрешения некоторых ситуаций, являющихся последствиями цифровизации.

Примером такой ситуации может служить восстановление доступа к украденному интернет-аккаунту. Единой нормативно определённой модели того, как действовать в такой ситуации, нет. Каждая интернет-платформа разрабатывает свои внутренние правила такого восстановления.¹

В научной литературе эта проблема неоднократно поднималась, и многие авторы подчёркивают необходимость закрепления универсального подхода к информации как к объекту гражданских прав. Одним из очевидных решений выглядит возвращение самого понятия «информация» в ст. 128 ГК РФ, что позволило бы устранить имеющиеся противоречия. Но этого недостаточно, важно также разграничить виды информации и определить их правовой режим, поскольку именно в классификации заключается смысл к дальнейшему развитию информационного законодательства.

Не стоит забывать и о более масштабной инициативе - это разработке Информационного кодекса Российской Федерации. Идея создания такого акта обсуждается уже давно и в перспективе могла бы объединить и систематизировать нормы, которые сегодня разбросаны по множеству законов. Кодекс дал бы единые определения и правила обращения информации, обеспечив тем самым большую определённость для всех участников информационных отношений.

Таким образом, можно выделить несколько приоритетных шагов: во-первых, вернуть «информацию» в перечень объектов гражданских прав; во-вторых, закрепить на законодательном уровне классификацию информации и разграничить правовые режимы её видов; в-третьих, либо принять отдельный Информационный кодекс, либо провести глубокую унификацию ГК РФ и специальных федеральных законов. Совокупность этих мер позволит устранить существующие пробелы, а также обеспечить надёжную основу для регулирования информационных отношений в условиях цифровой трансформации общества.

¹ Захаров А.Е. Феномен цифрового права. Возможен ли Цифровой кодекс? // Евразийская адвокатура. - 2025. - № 1. - (72). - С. 154.

Отдельного внимания заслуживает опыт Китайской Народной Республики, где в последние годы сформирована комплексная система нормативных актов, регулирующих сферу информации и данных.

Национальный информационный консультативный комитет КНР определяет информационную безопасность как ключевой компонент системы национальной безопасности, который необходим для обеспечения устойчивого, здорового применения информационных технологий, а также для социальной и культурной стабильности и идеологического развития.¹

Во-первых, важным шагом стало принятие Закона КНР о кибербезопасности от 7 ноября 2016 г., который закрепил основы регулирования в области информационной безопасности. В нём были установлены требования к локализации данных, правила передачи информации за пределы страны, а также меры по обеспечению защиты информации в деятельности сетевых операторов. В Китае действует требование обязательного указания подлинных сведений о пользователе при регистрации, а также установлена обязанность сохранять опубликованные материалы на территории страны не менее шести месяцев.

Во-вторых, в 2021 г. был принят Закон КНР о безопасности данных, который впервые на законодательном уровне классифицировал данные на несколько категорий («обычные», «важные» и «критически важные»). Для каждой категории определён особый правовой режим, включая меры по защите данных и порядок их трансграничной передачи. Данный закон направлен на обеспечение национальной безопасности и стабильности цифровой экономики.

В-третьих, в том же году вступил в силу Закон КНР о защите персональной информации (принят 20 августа 2021 г., вступил в силу 1 ноября 2021 г.). Его положения во многом сопоставимы с европейским Общим регламентом по защите данных (GDPR). Закон закрепил принципы обработки

¹ Ромашкина Н.А., Задремайлова В.Г. Эволюция политики КНР в области информационной безопасности // Пути к миру и безопасности. – 2020. - С. 122.

персональных данных, необходимость получения согласия субъекта, ограничения на сбор избыточной информации, а также строгий порядок трансграничной передачи персональных данных.

25 октября 2023 года в Китае было создано Национальное бюро данных (НБД), призванное координировать планирование и строительство цифрового Китая, цифровой экономики и цифрового общества на национальном уровне.¹

Особенностью китайского подхода является то, что регулирование информации рассматривается не только с позиции защиты прав личности, но и через призму государственной безопасности и суверенитета. В китайской правовой модели информация и данные трактуются как стратегический ресурс, требующий строгого контроля со стороны государства.

Подводя итог, можно сказать, что для России ключевой задачей является переход от разрозненных норм к целостной модели правового регулирования информации. Анализ научных источников и практики показывает, что попытки дать универсальное определение информации сталкиваются с её многогранностью: для юриста она значит одно, для экономиста другое, для философа третье. При этом само понятие «данные», активно вытесняющее традиционное «информация», подчёркивает сдвиг акцентов в сторону их экономического и технологического значения. Это ещё раз подтверждает необходимость системного подхода к выработке единой концепции, способной охватить все аспекты данного феномена.

Современные процессы цифровизации наглядно демонстрируют, что правовое регулирование информации пока не успевает за скоростью развития технологий. Несмотря на то, что институт информационных отношений давно стал частью гражданского оборота, их правовая основа в России остаётся фрагментарной и внутренне противоречивой. Отсутствие единого подхода к пониманию информации и её места в системе объектов гражданских прав

¹ Цзя. Шаосюе. Обзор законодательства и практики КНР в области развития современного цифрового права // RUDN Journal of Law. - 2024. - Т. 28. - № 3. - С. 533.

создаёт пробелы, которые особенно ощутимы в условиях трансформации экономики и усложнения социальных взаимодействий.

ЗАКЛЮЧЕНИЕ

Проведённое исследование позволило увидеть, что в современных условиях информация становится одним из ключевых ресурсов развития общества и экономики. Стремительное внедрение цифровых технологий, рост объёмов обработки данных, а также рост значимости информационных потоков в деловой, частной сферах обуславливают необходимость её признания самостоятельным объектом гражданских прав и определения правовых механизмов её защиты.

Действующее регулирование информации демонстрирует её двойственную природу, с одной стороны, она выступает как нематериальное благо, с другой как экономически значимый ресурс, включаемый в гражданский оборот. Такая двойственность создаёт определённые трудности в квалификации конкретных случаев. Охрана информации должна строиться с учётом баланса интересов всех участников правоотношений. Стоит отметить, что совершенствование правовых механизмов в данной сфере является важнейшей задачей для устойчивого развития гражданских правоотношений и цифровой экономики Российской Федерации.

Отдельного внимания заслуживает соотношение договорных и внедоговорных способов защиты. В первом случае речь идёт о предусмотренных соглашением сторон механизмах, например, включении специальных условий о конфиденциальности, использовании лицензионных договоров, соглашений о неразглашении (NDA) и иных инструментов, позволяющих заранее урегулировать возможные нарушения. Внедоговорные способы носят более широкий характер и включают в себя меры гражданско-правовой, административной и уголовной ответственности. Такая дифференциация оправдана тем, что в условиях цифровой экономики стороны далеко не всегда находятся в договорных отношениях, а угрозы информационной безопасности возникают и за пределами частноправовых связей.

Российское законодательство прямо ограничивает оборот информации, которая способна причинить вред обществу: пропаганда войны, разжигание ненависти, распространение экстремистских материалов. В реальности такие дела становятся всё более актуальными, особенно в условиях активного использования социальных сетей и мессенджеров. Здесь государство применяет административные меры, включая деятельность Роскомнадзора, который вправе блокировать ресурсы и ограничивать доступ к незаконным материалам.

Не менее важным направлением правового регулирования выступает охрана интеллектуальной собственности. Включение в перечень объектов гражданских прав результатов интеллектуальной деятельности и средств индивидуализации позволило выстроить целую систему защиты прав авторов и правообладателей. Суд по интеллектуальным правам, а также нормы КоАП РФ и УК РФ сыграли ключевую роль в формировании устойчивой судебной практики и обеспечении баланса интересов в этой сфере. Особенно значимыми стали механизмы защиты авторских прав в интернете, включая возможность блокировки сайтов, распространяющих нелегальный контент.

Вместе с тем, проведённый анализ выявил и ряд нерешённых проблем. Среди них - недостаточная адаптация действующих норм к стремительно меняющимся цифровым условиям, фрагментарность правоприменительной практики и необходимость дальнейшего уточнения понятийного аппарата информационного права. Всё это указывает на то, что защита информации остаётся динамично развивающейся сферой, требующей постоянного обновления правовых инструментов и выработки единых подходов в судебной практике.

В этой связи важным направлением развития представляется совершенствование законодательной базы. Перспективным направлением развития права по анализируемой теме может выступить создание кодифицированного акта в сфере информационного права - Информационного кодекса РФ, который объединил бы нормы о правовом режиме информации, о

коммерческой тайне, о защите персональных данных, а также специальные правила о цифровых правах. Такой подход позволил бы устранить имеющиеся противоречия и закрепить чёткие механизмы защиты информации. Кроме того, необходимо разработать новые способы охраны информации как объекта гражданских прав, учитывающие особенности её существования в цифровой форме.

Таким образом, проведённое исследование подтверждает, что информация прочно закрепились в системе объектов гражданского права и со временем занимает всё более важное место в гражданском обороте. Однако существующее правовое регулирование пока не в полной мере соответствует вызовам цифровой эпохи.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно-правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Собрание законодательства Российской Федерации. - 2009. - № 4. - Ст. 445.
2. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 №51-ФЗ (ред. от 01.08.2025) // Собрание законодательства РФ. - 05.12.1994. - № 32. - Ст. 3301.
3. Гражданский кодекс Российской Федерации (часть вторая)" от 26.01.1996 № 14-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. - 29.01.1996. - № 5. - Ст. 410.
4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 17.11.2025) // Собрание законодательства РФ. - 17.06.1996. - № 25. - Ст. 2954.
5. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 04.11.2025) // Собрание законодательства РФ. - 07.01.2002. - № 1 (ч. 1). - Ст. 1.
6. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (ред. от 31.07.2025) // Собрание законодательства РФ. - 18.11.2002. - № 46. - Ст. 4532.
7. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 27.07.2025) // Собрание законодательства РФ. - 25.12.2006. - № 52 (1 ч.). - Ст. 5496.
8. Федеральный закон от 20.04.1995 № 45-ФЗ (ред. от 28.02.2025) "О государственной защите судей, должностных лиц правоохранительных и контролирующих органов" // Собрание законодательства РФ. - 24.04.1995. - № 17. - Ст. 1455.
9. Федеральный закон от 17.07.1999 № 176-ФЗ (ред. от 31.07.2025)

«О почтовой связи» // Собрание законодательства РФ. - 19.07.1999. - № 29. - Ст. 3697.

10. Федеральный закон от 08.08.2001 № 129-ФЗ (в ред. от 28.12.2024) «О государственной регистрации юридических лиц и индивидуальных предпринимателей» // Собрание законодательства РФ. - 13.08.2001. - № 33 (часть I). - Ст. 3431.

11. Федеральный закон от 07.07.2003 № 126-ФЗ (в ред. от 31.07.2025) «О связи» // Собрание законодательства РФ. - 14.07.2003. - № 28. - Ст. 2895.

12. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (ред. от 08.08.2024) // Собрание законодательства РФ. - 09.08.2004. - № 32. - Ст. 3283.

13. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 01.09.2025) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. – 2006. – № 31. – Ст. 3448.

14. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) «О персональных данных» // Собрание законодательства РФ. - 31.07.2006. - №31 (1 ч.). - Ст. 3451.

15. Федеральный закон от 06.04.2011 № 63-ФЗ (в ред. от 01.09.2025) «Об электронной подписи» // Собрание законодательства Российской Федерации. – 2011. – № 15. – Ст. 2036.

16. Федеральный закон от 02.07.2013 № 187-ФЗ (ред. от 01.10.2014) «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях» // Собрание законодательства РФ. - 08.07.2013. - № 27. - Ст. 3479.

17. Федеральный закон от 30.12.2020 № 530-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. - 04.01.2021. - № 1 (часть I). - Ст. 69.

18. Закон Российской Федерации от 27.12.1991 № 2124-1 (ред. от

23.07.2025) «О средствах массовой информации» // Российская газета. - № 32.
- 08.02.1992.

19. Закон Российской Федерации от 21.07.1993 № 5485-1 (в ред. от 24.06.2023) «О государственной тайне» // Собрание законодательства РФ. - 1997. – № 41. – Ст. 8220-8235.

20. Постановление Правительства РФ от 3.11.1994 № 1233 (ред. от 09.10.2024) "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" // Собрание законодательства РФ. – 25. 07. 2005 № 30 Ст. 3165.

21. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // Собрание законодательства РФ. - 15.05.2017 № 20 Ст. 2901.

22. Решение Басманного районного суда № 01-0486/2023 от 12.07.2023 [Электронный ресурс] // URL: <https://www.mos-gorsud.ru/rs/basmannyj/service/s/cases/criminal/details/0539efc0-20b0-11ee-a079-c5d4cc8e4c60?docsDateFrom=13.07.2023&docsDateTo=13.07.2023&formType=fullForm> (дата обращения: 18.08.2025).

23. Определение Девятого кассационного суда общей юрисдикции от 25 апреля 2024 г. по делу № 8Г-2539/2024 [Электронный ресурс] // URL: https://9kas.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=12460863&case_uid=e74bbd91-7567-475c-aa24-b05bbadaa064&delo_id=2800001&new=2800001 (дата обращения: 27.08.2025).

24. Определение Шестого кассационного суда общей юрисдикции от 18 апреля 2024 г. по делу № 8Г-2305/2024[88-9086/2024] [Электронный ресурс] // URL: https://6kas.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=6891335&case_uid=d3ec3736-5edc-4147-9acb-2c490644ec8f&delo_id=2800001&new=2800001 (дата обращения: 27.08.2025).

Учебная и научная литература

25. Блажеев, В. В., Егорова, М. А. Цифровое право: учебник / под общ. ред. В.В. Блажеева, М. А. Егоровой. – М.: Проспект. - 2020. - 640 с.
26. Городов, О. А., Петров, А. В., Шмигельская, Н. А. Недобросовестная конкуренция: учебно-практическое пособие / под ред. О. А. Городова. – М.: Юстицинформ. - 2020. - 324 с.
27. Карпычева, М.В., Хужина, А. М. Гражданское право: учебник в 2 томах. Том 1 / под общ. ред. М.В. Карпычева, А. М. Хужина. — 2-е изд., перераб. и доп. — Москва: ИНФРА-М. - 2024. - 447 с.
28. Карпычева, М. В., Хужина, А. М. Гражданское право: учебник: в 2 томах. Том 2 / под общ. ред. М. В. Карпычева, А. М. Хужина. — 2-е изд., перераб. и доп. — Москва: ИНФРА-М. - 2023. - 602 с.
29. Пашенцев, Д. А., Малахов, В. П., Залоило, М. В. Субъект права. Стабильность и динамика правового статуса в условиях цифровизации. / Д. А. Пашенцев [и др.]. - М.: Инфотропик Медиа. - 2022. - 480 с.
30. Рассолов, И. М. Право и Интернет. Теория кибернетического права: монография / И. М. Рассолов // 3-е изд., доп. — Москва: Норма: ИНФРА-М. - 2022. - 304 с.
31. Чаннов, С. Е. Информационное право: учебник / под ред. С. Е. Чаннова. — Москва: Норма: ИНФРА-М. - 2024. - 448 с.

Публикации в научных журналах, сборниках и СМИ

32. Афанасьева, А. А. Информация как объект гражданского права / А. А. Афанасьева // Вопросы российской юстиции. – 2020. – № 9. – С. 1156-1163.
33. Аксенова, М. А. Концепция "электронного лица" в правовом пространстве / М.А. Аксенова // Юрист. - 2020. - № 7. - С. 18 - 24.
34. Болтанова, Е. С., Имекова, М. П. Генетическая информация в системе объектов гражданских прав / Е.С. Болтанова, М. П. Имекова // Lex Russica. - 2019. - №6. - С. 110–120.
35. Борисов, М. А. Проблемы правового регулирования информации в современных условиях / М. А. Борисов // Конституционное и муниципальное

право. - 2023. - № 6. - С. 39 - 41.

36. Балычев, А. П. Коммерческая тайна как вид конфиденциальной информации: правовое регулирование в Российской Федерации / А. П. Балычев // Вестник науки. – 2024. – Т. 2. - № 4. - (73). – С. 208-218.

37. Бажанов, Е. С. Защита права тайны на переписку и обмена информацией в период цифровизации общества / Е. С. Бажанов, Л. Д. Туршук // Безопасность. Управление. Искусственный интеллект. – 2024. – Т. 4. - № 4. - (4). – С. 2-7.

38. Бокова, А. О. К вопросу о гражданско-правовой защите коммерческой тайны / А. О. Бокова, А. Н. Мануковская, Н. С. Хохлов // Право и государство: теория и практика. – 2023. – № 12. - (228). – С. 316-320.

39. Боднарук, Ю.М. Способы нарушения исключительного права правообладателя на программу для ЭВМ через призму понятия «Пиратства» / Ю.М. Боднарук // Вестник ВУиТ. - 2021. - №2. - (98).

40. Волченко, А. В. Информация как объект корпоративных правоотношений / А. В. Волченко // Символ науки: международный научный журнал. – 2022. – № 4-1. – С. 68-70.

41. Горбунова, М. В. Особенности лицензионного договора в сфере авторского и смежных прав. Открытая лицензия / М. В Горбунова // Вызовы современности и стратегии развития общества в условиях новой реальности: сб. материалов XVIII Междунар. науч.-практ. конф., Москва, 30 июня 2023 года. – Москва. - 2023. – С. 87–91.

42. Девярых, Н. П. Защита конфиденциальной информации путем подписания соглашения о неразглашении / Н. П. Девярых // Эволюция российского права: материалы XIX Междунар. науч. конф. молодых ученых и студентов, Екатеринбург, 29–30 апреля 2021 года / Уральский гос. юрид. университет. – Екатеринбург. - 2021. – С. 613–619.

43. Дженакова, Е. В. О классификации субъектов правоотношения по распространению информации / Е. В. Дженакова // Российское право: образование, практика, наука. – 2021. – № 3. – С. 53.

44. Захаров, А. Е. Феномен цифрового права. Возможен ли Цифровой кодекс? // Евразийская адвокатура. – 2025. – № 1. - (72). – С. 154.
45. Колохина, В. М. Информация как объект гражданских прав / В. М. Колохина // Международный журнал гуманитарных и естественных наук. – 2023. – № 6-1. - (81). – С. 74–76.
46. Крюкова, Е. С. Врачебная тайна в аспекте охраны генетической информации / Е. С. Крюкова // Правовое государство: теория и практика. – 2021. – С. 11–25.
47. Кузнецов, М. Н. Влияние цифровизации на некоторые руководящие начала гражданского судопроизводства / М. Н. Кузнецов // Вестник Московского городского педагогического университета. Сер. «Юридические науки». - 2020. - № 2. - С. 58-67.
48. Кузьмин, К. А. Ответственность за нарушение лицензионного договора / К. А. Кузьмин // Право и государство: теория и практика. – 2022. – № 6. - (210). – С. 46-48.
49. Котилко, В. В. Влияние биометрии на результативность экономики: проблемы безопасности / В. В. Котилко // Вестник Восточно-Сибирской Открытой Академии. – 2024. – № 54. - (54).
50. Коробкина, П. С. Правовые особенности заключения лицензионного договора в сети интернет / П. С. Коробкина // Международный журнал гуманитарных и естественных наук. – 2023. – № 5-2. - (80). – С. 218-221.
51. Логунова, Н. Ю. Информация как объект коммерческого использования и распространения в отраслевой экономической системе / Н. Ю. Логунова, А. Г. Татьянок, К. А. Кочнев // Форум. Серия: Роль науки и образования в современном информационном обществе. – 2024. – № S1-3. - (32). – С. 79-83.
52. Мартыненко, Н. Э. Уголовно-правовые средства охраны информации и противодействия информационным угрозам / Н. Э. Мартыненко // Труды Академии управления МВД России. – 2022. – № 4. - (64).

– С. 66–75.

53. Мещерякова, М. А. Конституционное право на тайну коммуникации: понятие и содержание / М. А. Мещерякова // Юридическая наука и правоохранительная практика. – 2020. – № 3. - (53). – С. 127–137.

54. Нуриддинов, Структура и содержание информационного обеспечения кадастра недвижимости / Д. Р. Нуриддинов // Основные принципы развития землеустройства и кадастров: материалы XVIII Всерос. науч.-практ. конф., Новочеркасск, 27–29 апреля 2021 года. – Новочеркасск: ДонГАУ. - 2021. – С. 181–184.

55. Панова, С. М. Биометрия: содержание биометрии и ее применение в России / С. М. Панова // Экономика и инновации: сб. статей участников межвузовской науч.-практ. конф. – Москва: РЭУ им. Г.В. Плеханова. - 2024. – С. 176–180.

56. Рожкова, М. А. О различиях между лицензионным договором и пользовательским соглашением / М. А. Рожкова // Журнал Суда по интеллектуальным правам. – 2024. – № 4. - (46). – С. 121–133.

57. Ромашкина, Н. А., Задремайлова, В. Г. Эволюция политики КНР в области информационной безопасности / Н. А. Ромашкина, В. Г. Задремайлова // Пути к миру и безопасности. – 2020. – С. 122.

58. Русецкая, И. А. NDA как инструмент обеспечения конфиденциальности информации / И. А. Русецкая // Информационная безопасность: вчера, сегодня, завтра: сб. статей по материалам III Междунар. науч.-практ. конф. – Москва: РГГУ. - 2020. – С. 40–44.

59. Санникова, Л. В., Харитонова, Ю. С. Цифровые активы: правовой анализ: монография. / Л. В. Санникова, Ю. С. Харитонова // М.: 4 Принт. - 2020. – С. 57.

60. Савиных, В. А. Информация как объект гражданских прав / В. А. Савиных // Моя профессиональная карьера. – 2025. – Т. 1. - № 72. – С. 324-329

61. Светова, Е. К. Тенденции развития института административной ответственности за правонарушения в информационной сфере / Е. К. Светова

// Юридическая ответственность за правонарушения в информационной сфере: вопросы теории и практики: сб. материалов Междунар. науч.-практ. конф., Санкт-Петербург, 21 октября 2021 года. – СПб.: Центр «Астерион». - 2022. – С. 257–263.

62. Старкова, А. Г., Королева, В. В. Проблемы защиты информации правовыми средствами / А. Г. Старкова, В. В. Королева // Актуальные проблемы современной юридической науки и практики : сб. трудов, посвященный 90-летию АГУ и 25-летию юр. факультета. – Астрахань. - 2022. – С. 139–142.

63. Стеблина, Е. К., Попов, В. В. Юридические особенности исключительной лицензии. Защита прав сторон такого лицензионного договора / Е. К. Стеблина, В. В. Попов // Вестник науки. – 2024. – № 6. - (75), т. 1. – С. 722–728.

64. Тухватулина, А. Г. Информация как объект гражданских прав / А. Г. Тухватулина // Вестник молодых ученых и специалистов Самарского университета. – 2020. – № 2. - (17). – С. 245–250.

65. Титоренко, С. К. Правовое регулирование режима коммерческой тайны при корпоративных конфликтах / С. К. Титоренко // Юридические исследования. – 2024. – № 6. – С. 30-43.

66. Усванова, Д. Р. Роль биометрии в повышении уровня безопасности аутентификации / Д. Р. Усванова // Научный Альманах ассоциации France-Kazakhstan. – 2024. – № 6. – С. 293-295.

67. Фастович, Г. Г., Шитова, Т. В. К вопросу о формировании правовых режимов информации в Российской Федерации / Г. Г. Фастович, Т. В. Шитова // Аграрное и земельное право. – 2021. – № 10. - (202). – С. 7–9.

68. Хмелевская, А. С., Кукарцева, А. Н. Защита интеллектуальной собственности в условиях цифровой трансформации экономики / А. С. Хмелевская, А. Н. Кукарцева // Экономика и управление инновациями. – 2024. – № 1. - (28). – С. 27–38.

69. Цзя. Шаосюе. Обзор законодательства и практики КНР в области развития современного цифрового права / Шаосюе. Цзя // RUDN Journal of

Law. – 2024. – Т. 28. - № 3. – С. 528–545.

70. Шарофзода, Р. Ш. Информация как объект юридического научного познания и правового воздействия / Р. Ш. Шарофзода, Г. А. Шокиров // Правовая жизнь. – 2021. – № 3. - (35). – С. 5-22.

Источники на электронных носителях

71. Рожкова, М. А. «Общедоступная информация», «открытые данные» и «персональные данные, разрешенные субъектом для распространения» – что это такое и как они между собой связаны? [Электронный ресурс] // URL: https://zakon.ru/blog/2021/1/13/obschedostupnaya_informaciya_otkrytye_dannye_i_personalnye_dannye_razreshennye_subektom_dlya_raspros (дата обращения: 11.07.2025).