

Национальная безопасность / nota bene

Правильная ссылка на статью:

Дубень А.К. — Теоретико-методологические основы информационной безопасности // Национальная безопасность / nota bene. – 2023. – № 2. DOI: 10.7256/2454-0668.2023.2.40068 EDN: ALNSVX URL: [https://nbpublish.com/library\\_read\\_article.php?id=40068](https://nbpublish.com/library_read_article.php?id=40068)

## Теоретико-методологические основы информационной безопасности

Дубень Андрей Кириллович

Научный сотрудник Института государства и права Российской академии наук

119019, Россия, Москва область, г. Москва, ул. Знаменка, 10

✉ k.duben@mail.ru



[Статья из рубрики "Доктрина"](#)

**DOI:**

10.7256/2454-0668.2023.2.40068

**EDN:**

ALNSVX

**Дата направления статьи в редакцию:**

24-03-2023

**Дата публикации:**

31-03-2023

**Аннотация:** Статья посвящена теоретическим и методологическим основам обеспечения информационной безопасности государства. Информационные войны в мировом информационном пространстве стали актуальной угрозой безопасности и суверенитету России. Статья посвящена анализу теоретических основ и методологии изучения механизма обеспечения информационной безопасности, раскрытию сущностных признаков и особенностей, структуры очерченной категории. Раскрывая сущностные аспекты информационной безопасности, исследуется уровень ее обеспечения в России. Целью работы является оценка эффективности государственного программно-целевого планирования в области информационной безопасности, выявление проблемных зон в этой сфере. В статье выполнен обзор нормативно-правовых документов, регулирующих вопросы информационной безопасности. Особым вкладом в исследовании автора считается то, что специфика системы специальных методов в исследуемой теме проявляется в комплементарности регулирования, определенной ключевыми векторами. При этом ключевой методологической функцией информационного права является формирование совокупности инструментов, целенаправленно предназначенных для

регулирования отношений в информационной сфере в соответствии с объективными закономерностями динамического развития глобального информационного общества и существующей государственной политики цифровизации. Вместе с тем совокупность правовых методов регулирования общественных отношений в связи с противодействием угрозам и вызовам безопасности личности, общества и государства в информационной среде, основываясь на методах, трансформируются исходя из специфики предметной области.

**Ключевые слова:**

информационное право, методология, теория права, информационная безопасность, цифровизация, законодательство, угрозы и риски, правовое регулирование, правовое обеспечение, информационное общество

Противоправное использование информации становится актуальной проблемой в ХХI веке, когда уровень информатизации общества, если не достиг своего пика, то имеет несоизмеримо высокие показатели в сравнении с прошлым веком. В связи с этим был принят Указ Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы», в котором информационная безопасность была указана в качестве одного из направлений развития российских информационных и коммуникационных технологий [\[1\]](#). Все эти аспекты ставят перед законодателем, правоприменителями и учеными новые вопросы, для разрешения которых, возможно, стоит пересмотреть некоторые положения существующей концепции информационной безопасности, а также переосмыслить значение определенных теоретико-правовых явлений и понятий в рамках науки и отрасли информационного права.

Право в области обеспечения информационной безопасности, будучи подотраслью в рамках информационного права, занимает особое место в системе норм указанной правовой отрасли [\[2, с. 4\]](#). Если еще в XX и начале ХХI века можно было вести дискуссии о наличии отрасли информационного права в рамках системы российского права, то в настоящий момент существование указанной отрасли уже является объективной данностью и в целом уже не требует столь широкого обсуждения [\[3, с. 13\]](#). Тем не менее это не мешает некоторым авторам, не признавая существование сложившейся и уже сформированной отрасли информационного права, утверждать лишь о процессе ее зарождения и формирования в настоящий момент [\[4, с. 47\]](#).

Фактором, обусловившим самостоятельность отрасли информационного права является особый характер информационных правоотношений [\[5, с. 140\]](#). Отношения, возникающие в рамках информационного права и составляющие его предмет, по мнению А.А. Чеботаревой, обладают следующими специфическими признаками:

- 1) они возникают, изменяются и прекращаются при обращении информации;
- 2) данные отношения складываются по поводу обладающих определенной спецификой объектов, к которым относятся информация, информационные объекты, информационные технологии, а явления, на которые направлены информационные права и обязанности» [\[6, с. 30\]](#).

Согласно позиции И.Л. Бачило, в состав предмета информационного права входят отношения, выраженные в:

- 1) информации при разнообразии форм ее проявления и формируемых на этой основе информационных ресурсах;
- 2) средствах и технологиях работы с информацией (информационных технологиях - потенциал ИКТ);
- 3) средствах и технологиях коммуникации информации по сетям связи» [\[7, с. 23\]](#).

Как можно заметить, предмет информационного права не ограничивается отношениями, связанными лишь с самой информацией, а предполагает более широкий перечень отношений, в состав которого входят, в том числе отношения, выраженные в информационных системах, предназначенных для работы с информацией, а также в иных объектах, на которые направлены информационные права и обязанности.

Комплексный характер информационного права предопределил двойственность информационных правоотношений, включающих в себя как частноправовой, так и публично-правовой аспекты. Удельный вес частноправового аспекта информационных правоотношений, как может показаться, был снижен в связи с исключением информации из перечня объектов гражданских прав, закрепленного в ст. 128 ГК РФ [\[8\]](#). Однако множество иных статей ГК РФ неоднократно упоминают информацию в качестве, если не объекта гражданского права, то отдельной правовой категории, объекта правоотношения. Так, в ст. ст. 726, 727 ГК РФ регламентируется порядок передачи информации заказчику, а также режим конфиденциальности, полученной сторонами информации. В ст. 1045 ГК РФ упоминается право стороны договора простого товарищества на информацию. Кроме того, в п. 1 ст. 1465 ГК РФ понятие одного из объектов средств индивидуализации (секрета производства) раскрывается как «сведения любого характера (производственные, технические, экономические, организационные и другие)», что согласуется с понятием информации, закрепленном в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: сведения (сообщения, данные) независимо от формы их представления [\[9\]](#). Таким образом, гражданско-правовой аспект информационных правоотношений состоит в использовании информации в рамках договорных и иных гражданско-правовых отношений (в том числе в объектах интеллектуальной собственности) между субъектами гражданского права. Субъекты права вступают в указанные правоотношения на диспозитивных началах, то есть на основе юридического равенства и свободы волеизъявления. В связи с этим подобные правоотношения можно назвать горизонтальными (координационными).

Публично-правовой аспект информационных правоотношений состоит в применении административно-правовых методов регулирования для обеспечения гарантий осуществления информационных прав и свобод. В рамках указанного аспекта реализуется государственно-управленческое воздействие на информационные правоотношения путем примененияластных предписаний и запретов, призванных обеспечить надлежащее соблюдение и охрану прав субъектов информационного права, а также укрепление суверенитета государства в информационном пространстве.

Рассматривая методологическую основу, можно отметить, что проблема метода правового регулирования информационной безопасности явилаась предметом исследования многих ученых, большинство из которых рассматривают классические методы регулирования в контексте публично-правовых отношений [\[10, с. 105\]](#). Некоторые ученые отмечают, что особенности правоотношений в связи с обеспечением

информационной безопасности, определяясь интересами многих субъектов, детерминируются влиянием специфики обеспечения безопасности и в других сферах на правовое регулирование, в частности посредством применения технических и организационных мер. Для правового обеспечения информационной безопасности как подотрасли информационного права характерен комплексный метод правового регулирования, интегрирующие элементы императивного и диспозитивного способов регламентации. Однако несложно заметить, что информационно-правовые отношения в области информационной безопасности в значительной степени обладают публично-правовыми признаками, нежели частноправовыми, так как непосредственно затрагивают отношения в области охраны и защиты объектов информационного права. Так, в Законе о персональных данных применены нормы как императивного, так и диспозитивного характера. Диспозитивное регулирование, как было указано выше, к примеру, применено в ст. 6 этого Закона. Метод императивного регулирования использован во множестве норм Закона о персональных данных, включая положения ст. 14, устанавливающей основания ограничения права субъекта на доступ к его данным [\[11\]](#).

Тем не менее в рамках правового обеспечения информационной безопасности имеет место и применение диспозитивного метода правового регулирования. Так, в ч. 3 ст. 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» оператор персональных данных имеет право поручить процессы обработки персональных данных другому лицу. Однако реализация данного права ставится в зависимость от согласия субъекта персональных данных. Следовательно, можно заключить, что в рамках правового обеспечения информационной безопасности используются общепринятые в науке информационного права методы диспозитивного и императивного регулирования с превалированием последнего [\[12, с. 21\]](#).

Стоит отметить, что отношения, возникающие в сфере информационной безопасности, носят многообразный характер, что обуславливает возможность применения множества методов правового регулирования, используемых в различных отраслях российского права. Так, при создании объектов интеллектуальной собственности (например, ноу-хау) применяются гражданско-правовые методы, при защите персональных данных работника применяются методы трудового права, а при государственном контроле (надзоре) за обработкой персональных данных используются методы административного права.

Гораздо реже имеет место рекомендательный метод правового регулирования. Обычно данный метод используется при установлении рекомендуемых образцов (форм) документов. Одним из примеров его использования в рамках права в области обеспечения информационной безопасности является рекомендуемый образец сертификата соответствия средства защиты информации [\[13\]](#).

Правоотношения в сфере информационной безопасности составляют в первую очередь предмет регулирования Закона об информации, однако данным нормативно-правовым актом перечень источников права в области информационной безопасности не исчерпывается. Нормы, связанные с регулированием информационной безопасности, содержатся в ст. 16 данного закона, которая именуется как «защита информации». Между тем следует сделать акцент на том, что понятия «информационная безопасность» и «защита информации» являются далеко не тождественными, так как второе является частным случаем первого. Как мы ранее отмечали, обусловлено это многообразием отношений, включенных в предмет информационного права.

Вместе с тем совокупность правовых методов регулирования общественных отношений в

связи с противодействием угрозам и вызовам безопасности личности, общества и государства в информационной среде, основываясь на методах, трансформируются исходя из специфики предметной области, образуя уникальный, взаимосвязанный и взаимообусловленный массив приемов и методов, характерных для правового обеспечения информационной безопасности как комплексного и межотраслевого образования, направленного на достижение национальных интересов в информационной сфере в современных условиях цифровизации [\[14, с. 92\]](#).

Таким образом, специфика системы специальных методов в исследуемой теме проявляется в комплементарности регулирования, определенной ключевыми векторами. При этом ключевой методологической функцией информационного права является формирование совокупности инструментов, целенаправленно предназначенных для регулирования отношений в информационной сфере в соответствии с объективными закономерностями динамического развития глобального информационного общества и существующей государственной политики цифровизации.

## Библиография

1. Указ Президента РФ от 9 мая 2017 года № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.
2. Ловцов Д.А. Теоретические основы системологии информационного права // Информационное право. 2014. № 2. С. 4–13.
3. Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России: Дисс. ... д-ра юрид. наук: 12.00.14 / Полякова Татьяна Анатольевна. М.: Рос. правовая акад. М-ва юстиции РФ, 2008. – 438 с.
4. Арямов А.А., Руева Е.О. Цифровое право как объект уголовно-правовой охраны // Российская юстиция. 2020. № 1. С. 45–47.
5. Информационное право: Учебное пособие для студентов вузов, обучающихся по специальности 021100 «Юриспруденция» / под ред. И.Ш. Килясханова. М.: ЮНИТИ-ДАНА, Закон и право, 2004. – 335 с.
6. Чеботарева А.А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе: Дисс. ... д-ра юрид. наук: 12.00.13 / Чеботарева Анна Александровна. М.: ИГП РАН, 2017. – 472 с.
7. Бачило И. Л. Информационное право: учебник для академического бакалавриата / И. Л. Бачило. — 5-е изд., перераб. и доп. — М.: Издательство Юрайт, 2017. – 419 с.
8. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Российская газета, № 238-239, 08.12.1994.
9. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета, № 165, 29.07.2006.
10. Бачило И.Л. Информационное право: Учебник. 2-е изд., перераб. и доп. М.: Юрайт, 2011. – 522 с.
11. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (ч. 1). Ст. 3451.
12. Городов О.А. Информационное право: Учебник. М.: Проспект, 2007. – 242 с.
13. Приказ ФСТЭК России от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации» (Зарегистрировано в Минюсте России 11.05.2018 № 51063) // Официальный интернет-портал правовой информации

<http://www.pravo.gov.ru>, 14.05.2018.

14. Минбалаев А.В. Характеристика метода правового регулирования (на примере метода информационного права) // Вестник Южно-Уральского государственного университета. Серия: Право. 2013. № 2. Т. 13. С. 91-94.

## **Результаты процедуры рецензирования статьи**

*В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.*

*Со списком рецензентов издательства можно ознакомиться [здесь](#).*

**Предмет исследования.** Представленная на рецензирование статья, подготовленная на тему: "Теоретико-методологические основы информационной безопасности", в качестве предмета исследования имеет анализ теоретико-методологических основ института информационной безопасности как части информационного права.

**Методология исследования.** В ходе выполнения работы применялись современные методы научного познания, как общенаучные, так и частные. Методологический аппарат статьи составили следующие элементы анализа: диахронное и синхронное, внутреннее и внешнее сравнение, формально-юридический метод, а также диалектические методы научного познания: анализ, абстрагирование, индукция, дедукция, гипотеза, аналогия, синтез, исторический и теоретико-прогностический.

**Актуальность исследования.** Вопросы информационной безопасности как компоненты национальной безопасности государства весьма актуальны на современном этапе. Институт информационной безопасности призван обеспечивать сохранение государственной, военной и других тайн Российской Федерации, защищать информационно-телекоммуникационную инфраструктуру, информационные технологии и информационные системы от киберпреступности, стимулировать необходимый уровень научно-технических разработок. По этим причинам правильный теоретико-методологический подход будет способствовать эффективности различных мер, обеспечивающих информационную безопасность.

**Научная новизна.** Нельзя сказать, что тема статьи является новой для правовой науки. Вопросами информационной безопасности занимались многие специалисты в области информационного права: Ю.М. Батурина, И.Л. Бачило, Т.А. Полякова, П.У. Кузнецова, В.Б. Наумова, А.А. Смирнова, А.В. Минбалаева, А.А. Стрельцова и др. В аспекте изучения теоретико-методологических основ информационной безопасности есть публикации Ю.А. Белевской и А.П. Фисуна. Не на всех указанных ученых ссылается автор рецензируемой статьи. Однако нельзя отрицать, что работа, проделанная автором этой статьи, содержит отдельные элементы научной новизны.

**Стиль, структура, содержание.** Работа написана научным стилем. Использована специальная юридическая терминология, как из общей теории права, так и из информационного права. Однако, автор допускает грамматические и стилистические ошибки в своей работе: например, в абзаце "Гораздо реже имеет место рекомендательный метод правового регулирования. Обычно данный метод используется при установлении рекомендуемых образцов (форм) документов. Одним из примеров его использования в рамках права в области обеспечения информационной безопасности является рекомендуемый образец сертификата соответствия средства защиты информации" 2 раза повторяется прилагательное рекомендуемый и 1 раз рекомендательный, т.е. по одному разу в каждом предложении этого абзаца. Автор использует термин "нормативно-правовой акт" вместо "нормативный правовой акт" и др. Статья логически структурирована, хотя нет формального деления на отдельные части. Введение следует доработать, обосновать актуальность, показать практическую

значимость и научную новизну именно этой выбранной автором темы. По содержанию тема раскрыта не полностью. Так, если "методологические основы" проанализированы, то про вторую составляющую "теоретические основы" информационной безопасности содержатся лишь фрагментарные упоминания в статье. Непонятно, что имеет ввиду автор написав "концепция информационной безопасности", хотелось бы узнать его мнение. А также неплохо бы показать как соотносятся категории "концепция" и "теоретико-методологические основы" информационной безопасности. Далее, вызывает сомнение уместность в этой статье длительные рассуждения автора о самостоятельности информационного права как отрасли права.

**Библиография.** Можно сделать замечание, что автором не изучены публикации последних лет по теме. Последняя работа в списке библиографии датирована 2020 годом. Что явно вызывает вопрос у читательской аудитории: актуальна ли тема? Библиографические источники оформлены с нарушением требований ГОСТ.

**Апелляция к оппонентам.** В статье есть обращения к оппонентам. Автор предпринимает попытку аргументировать свою позицию, критически относясь к противоположным мнениям (в частности, о самостоятельности информационного права). Можно заметить, что есть отдельные отрасли права, которые "отпочковались" уже давно, но дискуссии о их самостоятельности или зависимости не прекращаются до сих пор (например, семейное право). Хотелось бы увидеть в статье аргументы в пользу позиции самого автора. Задействования в статье оформлены ссылками на источник опубликования.

**Выводы, интерес читательской аудитории.** Статья "Теоретико-методологические основы информационной безопасности" нуждается в доработке, отвечает не всем требованиям, предъявляемым к научным публикациям. Тема актуальная, поэтому в принципе может представлять интерес для читательской аудитории.