Дата поступления рукописи в редакцию: 30.11.2025 г. DOI: 10.24412/2782-3830-2025-11-595-600
Дата принятия рукописи в печать: 17.12.2025 г.

БАРЫШНИКОВ Марат Юрьевич,
кандидат юридических наук,
доцент кафедры гражданского и предпринимательского права
Всероссийского государственного университета юстиции
(РПА Минюста России),
e-mail: marat210374@yandex.ru

УСМАНОВА Камилла Руслановна,
магистр, преподаватель Института сервисных технологий
ФГБОУ ВО «РГУТИС»,
Российский государственный университет туризма и сервиса,
e-mail: bsoul1@bk.ru

ЧЕЛЯПИНА Ольга Ивановна,
кандидат технических наук,
доцент Института сервисных технологий
Российского государственного университета туризма и сервиса,
город Подольск,
e-mail: olga-chelyapina@mail.ru

ЧАСТНОПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *В настоящей научной статье автор рассматривает особенности частноправовых аспектов обеспечения информационной безопасности. Автор исследования кратко отмечает, что эффективное обеспечение информационной безопасности как таковой доступно только через грамотное сочетание публично-правовых и частноправовых способов защиты. Автор анализирует более детально некоторые частноправовые инструменты: договорные конструкции, локальное правовое регулирование, а также иные, перечисляет ряд публично-правовых способов защиты. В заключении настоящей научной статьи автор также отмечает, что в дальнейшем правовой инструментарий обеспечения информационной безопасности продолжит свое развитие, для чего сегодня есть все необходимые предпосылки.* ***Объектом исследования являются*** *особенности частноправовых аспектов обеспечения информационной безопасности.* ***Целью исследования является*** *комплексный, последовательный анализ особенностей частноправовых аспектов обеспечения информационной безопасности.* ***Методы исследования:*** *формально-юридический, компаративистский, сравнительный анализ, диалектический, обобщение, конкретизация, систематизация и системный метод, дедукция, иные методы теоретического и практического уровней научного познания.* ***Научная новизна исследования*** *заключается в подготовке комплексного исследования, формировании авторских выводов относительно особенностей частноправовых аспектов обеспечения информационной безопасности. Данная научная статья, таким образом, будет полезна теоретикам, практикам, обучающимся и профессорско-преподавательскому составу гуманитарных и иных направлений подготовки, а также более широкому кругу читателей, интересующихся особенностями развития частноправовых аспектов обеспечения информационной безопасности в современной экономической и правовой практике.*

Ключевые слова: *информационная безопасность, правовое регулирование, современное состояние, кибербезопасность, обеспечение безопасности, частноправовой аспект, обеспечение информационной безопасности.*

BARYSHNIKOV Marat Yuryevich,
Candidate of Law, Associate Professor,
Department of Civil and Entrepreneurial Law,
All-Russian State University of Justice
(RPA Ministry of Justice of Russia),

USMANOVA Kamilla Ruslanovna,
Master's Degree, Lecturer, Institute of Service Technologies,
Federal State Budgetary Educational Institution of Higher Education
"Russky State University of Tourism and Service",
Russian State University of Tourism and Service,

CHELYAPINA Olga Ivanovna,
Candidate of Technical Sciences,
Associate Professor, Institute of Service Technologies,
Russian State University of Tourism and Service,
Podolsk,

PRIVATE LAW ASPECTS OF INFORMATION SECURITY

Annotation. *In this research article, the author examines the specifics of the private law aspects of information security. The author briefly notes that effective information security as such is only possible through a competent combination of public and private law protection methods. The author analyzes in more detail certain private law instruments, including contractual structures, local legal regulation, and others, and lists a number of public law protection methods. In the conclusion of this research article, the author also notes that legal instruments for information security will continue to develop in the future, for which all the necessary prerequisites exist today. The object of this research is the specifics of the private law aspects of information security. The purpose of this research is a comprehensive, consistent analysis of the specifics of the private law aspects of information security. Research methods include formal legal, comparative, and dialectical analysis, generalization, specification, systematization, and the systemic method, deduction, and other methods of theoretical and practical scientific inquiry. The research's scientific novelty lies in the comprehensive nature of the study and the author's conclusions regarding the specifics of private law aspects of information security. This research article will therefore be useful to theorists, practitioners, students, and faculty in the humanities and other fields of study, as well as to a wider audience interested in the development of private law aspects of information security in modern economic and legal practice.*

Key words: *information security, legal regulation, current state, cybersecurity, security, private law aspect, information security.*

Обеспечение информационной безопасности в современных условиях приобретает стратегическое значение ввиду того, что информационная безопасность выступает составляющей национальной безопасности всего государства в целом. Учитывая темпы цифровизации, ее постоянное развитие и возникновение новых технологий и инструментов, вопрос об эффективном обеспечении информационной безопасности становится едва ли не ключевым. Очевидно, что в дальнейшем данная тенденция только усилится.

Утверждение Президентом РФ в 2021 г. документов стратегического планирования в области национальной и международной информационной безопасности свидетельствует об актуальности и потребности укрепления информационного суверенитета государства и усилении его роли на международной арене [3].

Качественное обеспечение информационной безопасности определены как одна из задач реализации Доктрины информационной безопасности РФ, принятой в 2016 г. и действующей в настоящее время. Документ предусматривает совокупность публично-правовых и частноправовых инструментов, с помощью которых предполагается достижение высоких результатов. Кратко перечислим основные публично-правовые способы обеспечения информационной безопасности:

– разработка нормативно-правовой базы, регулирующей информационную безопасность, ее отдельные составляющие;

– создание профильных органов государственной исполнительной власти, а также наделение соответствующими полномочиями органов государственной и муниципальной власти;

– разработка и реализация совокупности контрольно-надзорных мероприятий органами государственной исполнительной власти;

– формирование судебной и правоприменительной практики на основе рассмотренных дел, кейсов, обобщения и анализа материалов судов и т.д.;

– иное [6].

Таким образом, публичный аспект в вопросе обеспечения информационной безопасности занимает существенное значение, что выража-

ется, главным образом, в функционировании профильных публичных участников правоотношений, а также в целом в реализации государством своих публично-правовых функций.

Одновременно на итоговую эффективность обеспечения информационной безопасности влияет и применение частноправового инструментария. Рассмотрим отдельные частноправовые способы более детально.

Во-первых, это защита персональных данных. Профильный ФЗ № 152-ФЗ был принят в 2006 г., и с тех пор тенденция к повышению степени защищенности персональных данных все более усиливалась. Рассматриваемым документом не только был введен терминологический аппарат, но также оказались сформулированы ключевые тезисы относительно реализации инструментов защиты персональных данных.

Например, субъект персональных данных правомочен в любой момент отказаться от передачи персональных данных оператору персональных данных, даже если ранее он уже дал согласие на это. Кроме того, при формулировании конкретных пунктов об обращении со своими персональными данными, субъект персональных данных имеет право согласовать или не согласовать какие-то из них. Например, дать согласие на передачу персональных данных, но запретить их распространение, либо разрешить распространение ограниченного рода информации. По общему правилу согласие на передачу персональных данных или их распространение действует до момента, пока сам субъект не оформит отзыв такого согласия.

Обратим внимание, что в данном примере мы наблюдаем распространенную ситуацию, когда частноправовой защитный инструментарий действует в совокупности с публично-правовым. Так, за нарушение законодательства о персональных данных предусмотрена юридическая ответственность вплоть до уголовной. Поэтому персональные данные оказываются защищены одновременно с двух позиций: с одной стороны, субъект персональных данных сам правомочен производить ряд действий по их защите, с другой, даже если это произведено не было или полномочий субъекта персональных данных недостаточно, государство может содействовать в обеспечении информационной безопасности.

Когда ФЗ № 152-ФЗ только был принят, отношение операторов персональных данных и других участников рассматриваемых правоотношений еще не было столь серьезным, как в настоящее время. Однако за 20-летнюю историю применения данного документа уже сформировалась эффективная система обеспечения защищенности персональных данных – как в целом, так и в отдельных составных частях.

Во-вторых, договорные конструкции. В массовом и частном обращении с информацией и связью во многом содействуют эффективной защите заключаемые договоры. К примеру, это абонентский договор на обслуживание, который заключает абонент сотовой связи – сложно сегодня найти человека, не участвующего в таких правоотношениях. Помимо общих положений, такие документы предусматривают также и определенный защитный инструментарий [7].

Так, к примеру, договор может содержать специальный раздел, посвященный условиям соблюдения конфиденциальности. По общему правилу, это касается установления запрета участникам соглашения на распространение информации, ставшей им известной в ходе реализации данного договора. Нередко договором может быть установлен запрет на распространение любых данных и информации, которая будет сочтена стороной договора нежелательной. Данный пункт договора вариативен и может варьироваться в зависимости от характеристик самого договора.

Важно, что нарушение информационной безопасности в подобной ситуации влечет не только, к примеру, административную или уголовную ответственность, но также и гражданско-правовые санкции, которые могут быть выражены, например, в выплате неосновательного обогащения или компенсации морального вреда. Иными словам, информация как объект правоотношений находится под защитой сразу нескольких разновидностей юридических санкций [6].

В-третьих, к актуальным частноправовым методам следует отнести также локальное правовое регулирование, поскольку в этой области организации обладают всей полнотой функционала. Фактически если федеральное законодательство, регламентирующее правоотношения в сфере информации и связи, не регулирует какие-либо проблемные вопросы, субъекты предпринимательской деятельности вправе урегулировать это на локальном уровне, однако такое регулирование не должно противоречить нормам федерального законодательства. Поэтому в данном отношении субъекты предпринимательства в полной мере вольны самостоятельно определять, как именно и в каком порядке осуществлять защиту информации.

Приведем примеры локальных актов, принимаемых организациями в данной области:

– план мероприятий по обеспечению информационной безопасности;

– инструкция о порядке действий при осуществлении контроля использования сотрудниками сети Интернет;

– приказ «Об обеспечении информационной безопасности в организации»;

– иные [2; 4].

Кроме того, важной составляющей являются локальные источники, регламентирующие защиту персональных данных – к примеру, это Политика в отношении обработки персональных данных, Положение об обработке персональных данных, Правила рассмотрения запросов субъектов персональных данных, а также ряд других документов.

И здесь в контексте эффективности применения частноправовых инструментов мы можем наблюдать двойственное положение. С одной стороны, ряд правовых источников локального уровня организации обязаны разработать и принять во исполнение федерального законодательства, с другой же, некоторые организации сами становятся инициатором принятия тех или иных локальных документов ввиду их высокой актуальности. Поэтому на локальном уровне может быть сформулирована самостоятельная правовая база, регламентирующая вопросы обеспечения информационной безопасности. На практике можно наблюдать, как некоторые организации подходят к данному вопросу довольно ответственно, ведь потенциальная опасность для субъектов предпринимательства в современных реалиях по-прежнему остается серьезной (*диаграмма 1*).

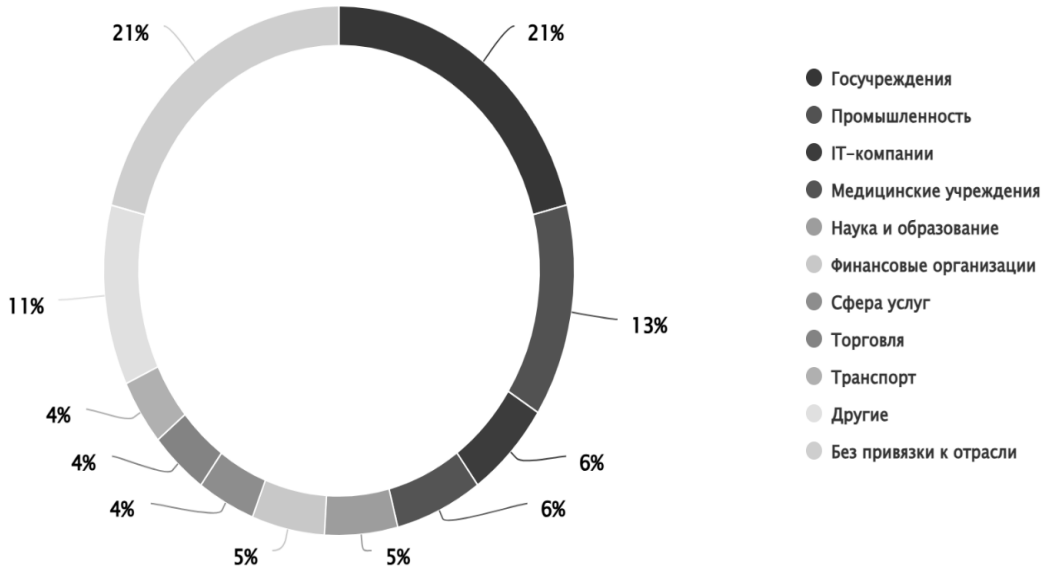


Диаграмма 1. Наиболее подверженные киберугрозам и атакам сектора предпринимательской деятельности (по материалам «Positive Technologies», за первое полугодие 2025 г.)

Важно, что на данном примере можно отчетливо наблюдать, как частноправовые инструменты включают в свое содержание международно-правовые нормы. Сегодня наиболее значимыми международными стандартами в области обеспечения информационной безопасности выступают ISO/IEC 27001 и NIST SP 800-серии, которые лежат в основе практически каждого локального источника правового регулирования. В контексте именно частноправовых аспектов можно отметить следующие важные пункты указанных документов:

ISO/IEC 27001: обязанность разработки внутри организации политики информационной безопасности, на основе которой в дальнейшем базируется все обеспечение информационной безопасности в организации; эффективная оценка существующих и потенциальных рисков; разработка плана контрольных мероприятий и т.д.;

NIST SP 800-серии: оценка рисков и эффективное управление ими; применение на локальном уровне отдельных технических инструментов обеспечения информационной безопасности; ориентация на повышение доступности, целостности, конфиденциальности данных и информации, а также иное [9].

Кроме того, при разработке локального регулирования используются и другие международные нормы.

В-четвертых, значимой составляющей обеспечения информационной безопасности выступает повышение правовой и финансовой грамотности в контексте процессов цифровизации. К примеру, сегодня широко распространено использование разного рода банковских прило-

жений, причем каждая кредитная организация ввиду высокого уровня конкуренции стремится сделать такое приложение все более всеобъемлющим и многофункциональным. Поэтому на практике обычное приложение банка, изначально предназначенное для совершения банковских операций, может содержать крайне широкий перечень информации о пользователе, и получение несанкционированного доступа к таким данным крайне опасно для клиента банка.

Несмотря на высокий уровень защищенности, который стараются обеспечить банки, тем не менее, случаи получения неправомерного доступа к информации о пользователях довольно распространены – в уголовно-правовой практике это один из наиболее часто встречающихся видов мошеннических действий. В большинстве случаев проблема возникает по вине самого пользователя, который либо предпринимает недостаточные меры для обеспечения должного уровня защищенности информации, либо не предпринимает их вовсе [3; 5]. Кроме того, часто встречается «добросовестное заблуждение»: ситуация, когда пользователь банально не обладает должным уровнем компьютерной грамотности (правовой, финансовой), чтобы эффективно обеспечить собственную информационную безопасность.

Помимо изложенного выше по тексту, одной из актуальных проблем в информационной сфере в современных условиях является также нарастание рисков распространения информации, представляющей опасность для несовершеннолетних, в связи с чем важное значение в этой области приобрело в т.ч. формирование информационно-правовой культуры и цифровой грамотности [3].

Отметим также, что большинство из рассмотренных в данном контексте частноправовых инструментов защиты информации носят технический характер.

Перечислим далее некоторые иные частноправовые инструменты обеспечения информационной безопасности:

– использование и санкционирование использования разного рода технических средств для защиты;

– применение правовых режимов коммерческой тайны, конфиденциальной информации, иных;

– применение инструментов защиты интеллектуальной собственности, т.к., к примеру, к объектам интеллектуальной собственности относятся базы данных, программы ЭВМ и другие схожие по своим характеристикам источники информации;

– иное.

Таким образом, мы наблюдаем, что эффективное обеспечение информационной безопасности достигается через грамотное сочетание публично-правовых и частноправовых инструментов, и здесь необходимо отметить их тесную связь и взаимную зависимость. Так, без наличия в государстве профильных органов государственной исполнительной власти не была бы в должной мере реализована контрольно-надзорная функция, а значит, фактически отсутствовал бы квалифицированный, узкопрофильный субъект правоотношений, весь функционал которого связан с обеспечением информационной безопасности. Сегодня такие субъекты присутствуют на всех уровнях государственной и муниципальной власти.

Отметим также, что правовой инструментарий обеспечения информационной безопасности сегодня постоянно развивается и совершенствуется – как в публично-правовом, так и в частноправовом аспектах [8].

Кратко обозначим ключевые выводы по результатам проведенного научного исследования.

Сегодня вопросы обеспечения информационной безопасности в любых выражениях имеют высокий уровень практической значимости. Процессы цифровизации развиваются буквально ежедневно, современные технологии реагируют на эти вызовы довольно оперативно, и поэтому в настоящее время мир находится в глобальной цифровой трансформации, происходящей всегда и повсеместно.

Соответственно, на перемены обязан реагировать законодатель. Достижение эффективного обеспечения информационной безопасности в правовом аспекте предусматривает совокупность частноправовых и публично-правовых инструментов.

В работе перечислены некоторые актуальные публично-правовые инструменты, а именно:

– разработка нормативно-правовой базы, регулирующей информационную безопасность, ее отдельные составляющие, в т.ч. их правовой статус;

– создание профильных органов государственной исполнительной власти, а также наделение соответствующими полномочиями органов государственной и муниципальной власти;

– разработка и реализация совокупности контрольно-надзорных мероприятий органами государственной исполнительной власти;

– иное [4].

Более детально уделяется внимание именно частноправовым способам, среди которых, в частности, автор анализирует наиболее распространенные на практике:

– защита персональных данных;

– договорные конструкции;

– локальное правовое регулирование;

– повышение правовой и финансовой грамотности в контексте процессов цифровизации;

– иное.

Предполагается, что достижение высокого уровня эффективности обеспечения информационной безопасности доступно только при грамотном сочетании публично-правовых и частноправовых способов, а также постоянном повышении собственного уровня правовой, цифровой культуры, развитии [3; 10].

Как видно из представленного анализа, отечественные законодатель, правоприменитель уделяют повышенное внимание вопросам правового регулирования обеспечения информационной безопасности, и это дает предположить, что в дальнейшем правовой инструментарий продолжит развиваться.

Список литературы:

[1] Дурницын, И. Развитие права в сфере информационной безопасности // ГАРАНТ. URL: https://www.garant.ru/ia/opinion/author/durnicyn/1420282/

[2] Дубень, А.К. Правовое обеспечение информационной безопасности в системе информационного права в Российской Федерации: дисс. к.ю.н.: 5.1.2. / Дубень, Андрей Кириллович. – М., 2023. – 245 с.

[3] Дубень, А.К. Отдельные аспекты правового обеспечения информационной безопасности в Российской Федерации // Закон и право. – 2022. – № 10. – С. 66-74.

[4] Колесников, Ю.А., Худякова, Н.В. Обеспечение информационной безопасности как институт современного российского права // Вестник юридического факультета Южного федерального университета. – 2022. – № 13. – С. 19-27.

[5] Правовые аспекты информационной безопасности // URL: https://ropkip.ru/content/uploads/20220124/1643038889_b22536ec7fdaa3acdd9536d07dec761e.pdf

[6] Редкоус, В.М. Законодательное закрепление мер поддержки и развития в сфере кибербезопасности (российский и зарубежный опыт) // Государственная служба и кадры. – 2022. – № 13. – С. 18-27.

[7] Сергун, П.П., Герасимов, Ю.С. Информационная безопасность в Российской Федерации: отдельные аспекты правового регулирования // Вестник РПА. – 2020. – № 2. – С. 112-117.

[8] Туликов, А.В. Публично-правовые и частноправовые аспекты обеспечения информационной безопасности // URL: https://www.sovremennoepravo.ru/m/articles/view/Публично-правовые-и-частноправовые-аспекты-обеспечения-информационной-безопасности

[9] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Собрание законодательства РФ. 12.12.2016. № 50. Ст. 7074.

[10] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 24.06.2025) «Об информации, информационных технологиях и о защите информации». Парламентская газета. № 126-127. 03.08.2006.

References:

[1] Durnitsyn, I. Development of Law in the Sphere of Information Security // GARANTEE. URL: https://www.garant.ru/ia/opinion/author/durnicyn/1420282/

[2] Duben, A.K. Legal Support of Information Security in the System of Information Law in the Russian Federation: diss. candidate of legal sciences: 5.1.2. / Duben, Andrey Kirillovich. - M., 2023. - 245 p.

[3] Duben, A.K. Certain Aspects of Legal Support of Information Security in the Russian Federation // Law and Right. - 2022. - No. 10. - P. 66-74.

[4] Kolesnikov, Yu.A., Khudyakova, N.V. Ensuring Information Security as an Institution of Modern Russian Law // Bulletin of the Law Faculty of the Southern Federal University. – 2022. – No. 13. – P. 19-27.

[5] Legal aspects of information security // URL: https://ropkip.ru/content/uploads/20220124/1643038889_b22536ec7fdaa3acdd9536d07dec761e.pdf

[6] Redkous, V.M. Legislative consolidation of support and development measures in the field of cybersecurity (Russian and foreign experience) // Civil Service and Personnel. – 2022. – No. 13. – P. 18-27.

[7] Sergun, P.P., Gerasimov, Yu.S. Information security in the Russian Federation: certain aspects of legal regulation // RPA Bulletin. – 2020. – No. 2. – P. 112-117.

[8] Tulikov, A.V. Public-law and private-law aspects of ensuring information security // URL: https://www.sovremennoepravo.ru/m/articles/view/Public-law-and-private-law-aspects-of-ensuring-information-security

[9] Decree of the President of the Russian Federation of 05.12.2016 No. 646 “On Approval of the Information Security Doctrine of the Russian Federation”. Collected Legislation of the Russian Federation. 12.12.2016. No. 50. Art. 7074.

[10] Federal Law of 27.07.2006 No. 149-FZ (as amended on 24.06.2025) “On Information, Information Technologies and the Protection of Information”. Parliamentary Newspaper. No. 126-127. 03.08.2006.