

ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ИНФОРМАЦИОННОЙ СФЕРЕ

DOI: 10.17803/1994-1471.2026.189.8.081-093

К. К. Краулин*

Обязанность операторов цифровых сервисов по противодействию компьютерным атакам: частноправовой аспект

Аннотация. В статье исследуется влияние компьютерных атак на договорные отношения по предоставлению цифровых сервисов между их операторами и клиентами (пользователями). Автором выявлена и обоснована тенденция в российском законодательстве к возложению на операторов цифровых сервисов обязанности по противодействию компьютерным атакам и сформулировано шесть юридически значимых признаков таких атак, которые влияют на их оценку в контексте гражданско-правовой ответственности за вызванное ими нарушение обязательств. Рассматриваются позиции в доктрине и судебной практике по вопросам квалификации компьютерных атак как обстоятельств непреодолимой силы и обосновывается целесообразность дифференцированного подхода к такой квалификации в зависимости от интенсивности (мощности) атаки. По результатам анализа применения института договорного ограничения ответственности при компьютерных атаках предложено учитывать нормы публичного права, устанавливающие требования к информационной безопасности цифрового сервиса, в качестве критериев стандарта должной осмотрительности оператора цифрового сервиса при его предоставлении третьим лицам. Отдельное внимание уделено обязанностям в сфере кибербезопасности операторов цифровых сервисов, связанных с выпуском и обменом цифровых финансовых активов, и операторов товарных посреднических цифровых платформ (маркетплейсов).

Ключевые слова: компьютерные атаки; цифровые платформы; оператор информационных систем, в которых осуществляется выпуск цифровых финансовых активов; оператор обмена цифровых финансовых активов; оператор посреднической цифровой платформы; оператор маркетплейса; обстоятельства непреодолимой силы; договорное ограничение ответственности; маркетплейс; информация

Для цитирования: Краулин К. К. Обязанность операторов цифровых сервисов по противодействию компьютерным атакам: частноправовой аспект // Актуальные проблемы российского права. — 2026. — Т. 21. — № 8. — С. 81–93. — DOI: 10.17803/1994-1471.2026.189.8.081-093

Благодарности. Исследование выполнено за счет гранта Российского научного фонда № 24-18-00618.

© Краулин К. К., 2026

* Краулин Константин Константинович, ведущий специалист Центра правовых исследований цифровых технологий Государственного академического университета гуманитарных наук
Мароновский пер., д. 26, г. Москва, Российская Федерация, 119049
kraulin.konstantin@yandex.ru

The Obligation of Digital Service Operators to Counter Cyberattacks: A Private Law Perspective

Konstantin K. Kraulin, Leading Specialist at the Centre for Legal Studies of Digital Technologies of the State Academic University for the Humanities, Moscow, Russian Federation
kraulin.konstantin@yandex.ru

Abstract. The paper examines the impact of computer attacks on contractual relationships concerning the provision of digital services between service operators and their customers (users). The author identifies and substantiates a trend in Russian legislation towards imposing on digital service operators a duty to counter computer attacks. Six legally significant characteristics of such attacks are formulated, which affect their assessment in the context of civil liability for breaches of obligations caused thereby. The paper reviews doctrinal and judicial approaches to the classification of cyber-attacks as force majeure and substantiates the desirability of a differentiated approach depending on the intensity (severity) of the attack. Based on an analysis of the application of contractual limitations of liability in the event of computer attacks, it is proposed that public law rules establishing information-security requirements for digital services be taken into account as criteria for determining the applicable standard of due care expected of a digital service operator when providing services to third parties. Particular attention is given to the cybersecurity obligations of operators of digital services related to the issuance and exchange of digital financial assets, as well as operators of digital intermediary platforms for goods (marketplaces).

Keywords: cyberattacks; digital platforms; operator of information systems in which digital financial assets are issued; digital financial asset exchange operator; intermediary digital platform operator; marketplace operator; force majeure; contractual limitation of liability; marketplace; information

Cite as: Kraulin KK. The Obligation of Digital Service Operators to Counter Cyberattacks: A Private Law Perspective. *Aktual'nye problemy rossijskogo prava*. 2026;21(8):81-93. (In Russ.). DOI: 10.17803/1994-1471.2026.189.8.081-093

Acknowledgments. The study was supported by a grant from the Russian Science Foundation (Grant No. 24-18-00618).

Введение

В Стратегии национальной безопасности Российской Федерации, утвержденной в 2021 г.¹ (п. 50), и Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.² (п. 15) констатировалось увеличение числа компьютерных атак на российские государственные и частные информационные ресурсы. По оценкам провайдеров решений в

сфере информационной безопасности, в 2025 г. количество хакерских атак на бизнес выросло на 46 % и в абсолютном значении превысило 100 тыс., при этом каждая пятая атака могла привести к недоступности сервисов и многомиллионным убыткам³.

Объектом атак часто становятся операторы цифровых сервисов⁴, под которыми для целей статьи предлагается понимать операторов цифровых платформ и иных информационных

¹ Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (ч. II). Ст. 5351.

² Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

³ Более 105 000 с начала 2025-го: число кибератак на бизнес в России выросло почти вдвое // URL: <https://www.comnews.ru/content/242214/2025-11-06/2025-w45/1009/bolee-105-000-nachala-2025-go-chislo-kiberatak-biznes-Rossii-vyroslo-pochti-vdvoe> (дата обращения: 01.03.2026).

⁴ Россия под атакой. Хакеры поменяли стиль и нацелились на уничтожение ИТ-инфраструктуры страны // URL: https://www.cnews.ru/news/top/2025-12-24_hakery_pomenyali_stil_i_pereshli (дата обращения: 01.03.2026).

систем, доступ к функционалу которых предоставляется пользователям через сеть Интернет (например, в сфере цифровых финансов, электронной торговли и пр.), а также лиц, оказывающих облачные и телекоммуникационные услуги (операторы связи, провайдеры хостинга и др.). В таких случаях ущерб причиняется не только самой компании, но и ее контрагентам, например приобретателям цифровых финансовых активов, партнерам-продавцам и пользователям-покупателям на товарных посреднических цифровых платформах (маркетплейсах), поскольку сервис становится для них недоступным, что порождает их требования о возмещении убытков к его оператору.

Поэтому наряду с предложениями по ужесточению уголовной ответственности для хакеров⁵ не менее важным видится формирование доктринального представления об обязанности операторов цифровых сервисов по противодействию компьютерным атакам с точки зрения частного права, что и является целью статьи. Для этого дана характеристика компьютерных атак

через их юридически значимые признаки, рассмотрены законодательство о противодействии таким атакам и его развитие, а также исследованы вопросы о возможности квалификации компьютерных атак в качестве обстоятельства непреодолимой силы и об эффективности договорного ограничения ответственности в таких случаях.

1. Юридически значимые признаки компьютерной атаки

Компьютерные атаки в законодательстве определяются как «целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты... в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации»⁶. В доктрине встречаются также термины «хакерские атаки»⁷ и «кибератаки»⁸, однако по своему содержанию они очень близки к приведенному определению.

01.03.2026) ; Более 105 000 с начала 2025-го: число кибератак на бизнес в России выросло почти вдвое ; Эксперты назвали самые атакуемые хакерами сферы в России // URL: <https://www.rbc.ru/rbcfreeneews/69455f539a79473ded3514cf> (дата обращения: 01.03.2026).

⁵ См., например: законопроект № 1071997-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях (в части установления административной ответственности за нарушение правил эксплуатации объектов критической информационной инфраструктуры Российской Федерации)» // СОЗД ГАС «Законотворчество». URL: <https://sozd.duma.gov.ru/bill/1071997-8> (дата обращения: 01.03.2026) ; Минюст предлагает расширить уголовную ответственность за DDoS-атаки // URL: <https://www.vedomosti.ru/society/articles/2025/05/19/1111078-ugolovnuyu-otvetstvennost-ddos-ataki> (дата обращения: 01.03.2026).

⁶ П. 4 ст. 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ. 2017. № 31 (ч. I). Ст. 4736. См. также сходные определения: п. 2.3 Методики расчета показателя «снижение времени реагирования по блокировке распространения фишинговых сайтов, имитирующих работу сайтов органов государственной власти», утв. приказом Минцифры России от 28.02.2022 № 143 // СПС «КонсультантПлюс» ; п. 3.11 ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», утв. и введен в действие приказом Ростехрегулирования от 27.12.2006 № 374-ст // СПС «КонсультантПлюс».

⁷ Образование и занятость: правовые вопросы новой цифровой реальности : монография / Н. С. Волкова, О. Ю. Еремина, О. В. Моцная [и др.] ; отв. ред. Н. С. Волкова, Н. В. Путило ; Институт законодательства и сравнительного правоведения при Правительстве РФ. М. : Юриспруденция, 2025. С. 160.

⁸ См., например: Государство, общество и личность: пути преодоления вызовов и угроз в информационной сфере : монография / Н. С. Волкова, А. А. Ефремов, С. М. Зырянов [и др.] ; отв. ред. Л. К. Терещенко. М. :

Можно выделить следующие юридически значимые признаки компьютерной атаки⁹. Во-первых, это внешний характер: такая атака не связана с действиями или волей оператора цифрового сервиса. Исключение могут составлять только тестирования устойчивости сервисов компании «белыми» хакерами¹⁰.

Во-вторых, умышленный характер действий: компьютерная атака возникает из-за умышленных противоправных действий третьих лиц, целью которых являются причинение вреда атакуемому лицу и его контрагентам и (или) причинение вреда экономике государства в целом и создание напряженности в обществе (при атаке на B2C или государственные сервисы). Такие действия в определенной степени можно назвать террористическим актом¹¹.

В-третьих, сопряженность с риском парализации бизнес-процессов компании — объекта атаки. Так, например, атака на ИТ-инфраструктуру авиакомпании «Аэрофлот» привела к отмене более 100 рейсов и убыткам свыше 200 млн руб.¹²

В-четвертых, возможность минимизации риска компьютерных атак при «должной осмотрительности» в организации информационной безопасности: чем выше уровень информаци-

онной безопасности у оператора цифрового сервиса, тем больше атак он сможет отразить без влияния на его функционирование.

В-пятых, невозможность абсолютной защиты от любых компьютерных атак. Некоторые атаки являются непредотвратимыми ввиду сверхвысокой мощности, опережающей возможности даже передовых ИБ-решений. Если продолжить аналогию с террористическими актами, то даже при высокоэффективной организации системы охраны правопорядка и перманентной охране всех социально значимых объектов гарантировать полную антитеррористическую защищенность невозможно.

В-шестых, отсутствие прямой обязанности по противодействию таким атакам в законодательстве для большинства операторов цифровых сервисов. Помимо общих требований по обеспечению информационной безопасности и конфиденциальности информации, предусмотренных Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»¹³ и Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»¹⁴, в нормативных правовых актах долгое время отсутствовали требования о противодействии компьютерным атакам.

Инфотропик Медиа, 2024. С. 19 ; Швырев Б. А., Тищенко Ю. Ю. Кибератаки: иммерсионная образовательная среда и ее формирование // Уголовно-исполнительная система: право, экономика, управление. 2024. № 1. С. 30–33.

⁹ Некоторые из них были ранее сформулированы автором применительно к DDoS-атакам: Краулин К. К. Сбой на сайте из-за DDoS-атаки. Можно ли взыскать убытки? // Шортрид. URL: <https://shortread.ru/sboj-na-sajte-iz-za-ddos-ataki-mozhno-li-vzyskat-ubytki/> (дата обращения: 01.03.2026).

¹⁰ Жижина М. В., Завьялова Д. В. Личность субъекта преступлений в сфере компьютерной информации как системообразующий элемент криминалистической характеристики (по материалам российских и зарубежных источников) // Актуальные проблемы российского права. 2022. № 5. С. 152.

¹¹ Компьютерные атаки отнесены к разновидностям терроризма, в частности, в пп. «в» п. 37 Концепции противодействия терроризму в Российской Федерации, утв. Президентом РФ 5 октября 2009 г. (Российская газета. 2009. № 198). См. также о кибертерроризме: Кудинов В. В., Минаев А. В. Кибертерроризм: основные угрозы и проблемы правового регулирования национальной безопасности Российской Федерации // Конституционное и муниципальное право. 2022. № 4. С. 53–56.

¹² Россия под атакой. Хакеры поменяли стиль и нацелились на уничтожение ИТ-инфраструктуры страны.

¹³ СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

¹⁴ СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.

2. Тенденция возложения на операторов цифровых сервисов обязанности по противодействию компьютерным атакам в российском законодательстве

Формирование представления об обязанности оператора по противодействию компьютерным атакам на его цифровые сервисы на государственном уровне происходило постепенно. Соответствующие требования впервые появились только в 2017 г. — в приказе ФСТЭК России от 25.12.2017 № 239, в котором устанавливалась обязанность владельцев значимых объектов критической информационной инфраструктуры по предотвращению компьютерных атак¹⁵.

В 2020 г. были приняты первые специальные нормативные правовые акты, возлагающие обязанности по противодействию компьютерным атакам на операторов отдельных цифровых сервисов. Так, на оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, в специальном Законе была возложена обязанность обеспечить «бесперебойность и непрерывность функционирования информационной системы, в том чис-

ле наличие и надлежащее функционирование дублирующих (резервных) технологических и операционных средств»¹⁶. Одновременно предусмотрена и ответственность в виде полного возмещения убытков пользователям, если они возникнут из-за технических сбоев и пр.¹⁷

Уже через год на таких субъектов наряду с операторами обмена цифровых финансовых активов Банк России возложил дополнительные обязанности в области обеспечения информационной безопасности, в том числе по анализу трафика сетевого взаимодействия¹⁸. Аналогичные требования одновременно были установлены и для операторов финансовых платформ¹⁹.

В 2023 г. внимание законодателя привлекла деятельность операторов других цифровых сервисов — провайдеров хостинга. Для них установили обязанность соблюдать требования о защите информации²⁰, полномочия по определению которых были возложены на Минцифры России. В первом проекте таких требований в числе прочего содержалась обязанность «обеспечить устойчивость к распределенным атакам, направленным на отказ в обслуживании (DDoS-атакам)»²¹, и «принимать меры по обнаружению

¹⁵ П. 22 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утв. приказом ФСТЭК России от 25.12.2017 № 239 // СПС «КонсультантПлюс».

¹⁶ П. 2 ч. 1 ст. 6 Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2020. № 31 (ч. I). Ст. 5018.

¹⁷ См. подробнее все основания ответственности оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов: ст. 9 Закона о цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации.

¹⁸ П. 3.3 положения Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» // Вестник Банка России. 2021. № 42.

¹⁹ Ч. 1 ст. 12 Федерального закона от 20.07.2020 № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы» // СЗ РФ. 2020. № 30. Ст. 4737.

²⁰ П. 3 ст. 1 Федерального закона от 31.07.2023 № 406-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации” и Федеральный закон “О связи”» // СЗ РФ. 2023. № 32 (ч. I). Ст. 6138.

Указанным Законом была введена часть 2 ст. 10.2-1 Закона об информации, информационных технологиях и о защите информации.

²¹ Проект приказа Минцифры России «Об утверждении требований о защите информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно

вторжений»²². Фактически эти положения обязывали отражать любые компьютерные атаки. После длительных обсуждений проекта между представителями бизнеса и отраслевыми регуляторами с учетом технической невозможности предотвращения всех возможных компьютерных атак приведенные положения были заменены на компромиссный вариант: «с целью обеспечения контроля и фильтрации входящего и исходящего сетевого трафика провайдер хостинга *при наличии технических средств* должен принимать меры по обнаружению и предотвращению вторжений *в случае их обнаружения*»²³ (курсив наш. — К. К.). Однако саму попытку закрепить столь строгую обязанность можно рассматривать как подтверждение намерений государства ужесточить требования в области противодействия компьютерным атакам.

В 2024–2025 гг. введены новые требования о защите информации в государственных информационных системах²⁴, в том числе в области противодействия атакам, направленным на от-

каз в обслуживании²⁵. Кроме того, в 2025 г. после ряда массированных DDoS-атак на интернет-провайдеров, которые привели к многочасовой недоступности Интернета на территориях целых кварталов Москвы, Роскомнадзор выступил с инициативой нормативно закрепить требования по противодействию компьютерным атакам на сети операторов связи²⁶.

Изложенное свидетельствует о формировании тенденции возложения на операторов цифровых сервисов обязанности по противодействию компьютерным атакам в российском законодательстве. При этом некоторые виды цифровых сервисов пока продолжают функционировать без каких-либо специальных требований к их бесперебойности. Так, маркетплейсы Ozon и Wildberries всё чаще становятся объектом компьютерных атак²⁷, но даже в Федеральном законе от 31.07.2025 № 289-ФЗ «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации»²⁸ этот вопрос остался без внимания²⁹.

подключенной к сети “Интернет”» (по состоянию на 9 октября 2023 г.) (подготовлен Минцифры России, ID проекта 02/08/09-23/00141794) // СПС «КонсультантПлюс».

См.: п. 7 Требований в проекте приказа Минцифры России «Об утверждении требований о защите информации...».

²² См.: п. 6 Требований в проекте приказа Минцифры России «Об утверждении требований о защите информации...».

²³ П. 6 приказа Минцифры России от 01.11.2023 № 936 «Об утверждении требований о защите информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети “Интернет”» // СПС «КонсультантПлюс».

²⁴ См.: приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» // СПС «КонсультантПлюс».

²⁵ Под атаками, направленными на отказ в обслуживании, понимаются в том числе DDoS-атаки.

²⁶ РКН: законодательство РФ нужно усовершенствовать для борьбы с DDoS-атаками // URL: <https://tass.ru/obschestvo/23501547> (дата обращения: 01.03.2026).

²⁷ Россияне массово жалуются на сбои в работе популярного маркетплейса // URL: <https://news.ru/society/rossiyane-massovo-zhaluyutsya-na-sboi-v-rabote-populyarnogo-marketplejsa> (дата обращения: 01.03.2026); Кибератака или инсайдер: почему произошел сбой в работе Wildberries // URL: <https://www.forbes.ru/biznes/459557-kiberataka-ili-insajder-pocemu-proizosel-sboj-v-rabote-wildberries> (дата обращения: 01.03.2026).

²⁸ СЗ РФ. 2025. № 31. Ст. 4643.

²⁹ За исключением общей обязанности соблюдать законодательство об информации и о персональных данных, которая дублируется в пп. «г» п. 4 ч. 1 ст. 4 Закона об отдельных вопросах регулирования плат-

3. Компьютерная атака как обстоятельство непреодолимой силы

Вместе с тем касательно отнесения компьютерных атак, которые могут вызвать такие сбои, к форс-мажору в юридической науке и правоприменительной практике единая позиция отсутствует, что обуславливает необходимость более глубокого исследования данного вопроса.

Так, в деле № А15-1085/2022 суд освободил от ответственности по государственному контракту исполнителя, который нарушил сроки отпуска на автозаправочных станциях из-за DDoS-атаки на инфраструктуру его оператора связи, признав ее форс-мажором применительно к обязательствам по контракту³⁰. Однако предмет договора, нарушение которого возникло из-за компьютерной атаки, не был связан с информационными технологиями, а объектом компьютерной атаки была инфраструктура не исполнителя, а его интернет-провайдера.

Применительно к обязательствам именно операторов цифровых сервисов суды в основном занимают более строгую позицию. По мнению некоторых судов, «сама по себе хакерская атака, учитывая современный уровень развития

информационно-компьютерных услуг и технологий, не отвечает признаку неотвратимости и неизбежности»³¹, а соответствующие риски являются «обычными коммерческими рисками», которые «в современных условиях хозяйственного оборота относятся к рискам, характерным для предпринимательской деятельности в сфере IT и телекоммуникаций»³². Несмотря на рациональность сформулированных судами тезисов, приведенные дела имеют один существенный недостаток: суды никак не исследовали технические параметры конкретной компьютерной атаки, послужившей причиной разбирательства, а основывались на абстрактных представлениях о них как социально-экономическом явлении в целом, что видится неверным. Поэтому далее предлагается дать такую оценку самостоятельно.

Оценивая возможность квалификации того или иного события как форс-мажора, необходимо проверять его на соответствие обязательным признакам обстоятельств непреодолимой силы³³, сформулированным Пленумом Верховного Суда РФ: непредотвратимости — невозможности избежать наступления этого обстоятельства или его последствий для любого участника оборота³⁴ — и чрезвычайности — исклю-

форменной экономики в Российской Федерации, хотя оператор посреднической цифровой платформы и так обязан соблюдать соответствующее законодательство как оператор информационной системы и оператор персональных данных.

³⁰ Постановление Шестнадцатого арбитражного апелляционного суда от 15.08.2023 № 16АП-1758/2023 по делу № А15-1085/2022.

³¹ Решение Арбитражного суда г. Москвы от 14.12.2012 по делу № А40-104765/10-98-918 (оставлено без изменения постановлением Девятого арбитражного апелляционного суда от 12.04.2013 № 09АП-7660/2013-ГК).

³² Решение Арбитражного суда г. Санкт-Петербурга и Ленинградской области от 01.06.2025 по делу № А56-85885/2024 (на дату написания статьи это решение было отменено постановлением Тринадцатого арбитражного апелляционного суда от 27.10.2025, дело находится на рассмотрении в кассационной инстанции).

³³ См. о признаках форс-мажора, например: *Байбак В. В.* Непреодолимая сила (форс-мажор) как основание освобождения от договорной ответственности (сравнительно-правовой очерк) // Закон. 2025. № 6. С. 166–180 ; *Курбатов А. Я.* Обстоятельства непреодолимой силы: разграничение со смежными понятиями // Законы России: опыт, анализ, практика. 2025. № 1. С. 56–57.

³⁴ П. 8 постановления Пленума Верховного Суда РФ от 24.03.2016 № 7 «О применении судами некоторых положений Гражданского кодекса Российской Федерации об ответственности за нарушение обязательств» // Бюллетень Верховного Суда РФ. 2016. № 15.

чительности рассматриваемого обстоятельства, наступление которого не является обычным в конкретных условиях.

Многочисленные публикации СМИ свидетельствуют, что за последние несколько лет все цифровые сервисы на какое-то время становились недоступными из-за DDoS-атак, включая сервисы ФНС³⁵, «Честный знак» и портал «Госуслуги»³⁶, в которых вопросам информационной безопасности уделяется особое внимание ввиду их значимости для государства. Это может свидетельствовать о том, что компьютерные атаки высокой интенсивности (мощности) являются непредотвратимыми, на что обращали внимание даже, например, спецслужбы Великобритании³⁷.

Переходя к признаку чрезвычайности, необходимо отметить, что хакеры как явление и их атаки давно стали «одной из классических угроз безопасности интернет-сайта»³⁸. Поэтому компьютерные атаки сами по себе уже не носят чрезвычайного характера — как ранее утратили свою чрезвычайность пандемия COVID-19³⁹ и санкции иностранных государств⁴⁰. Между тем, как и в случае с критерием непредотвратимости, видится не совсем верным пытаться дать категоричную квалификацию всем компьютерным атакам в целом без учета их многообразия. Атаки, существенно превышающие мощности

предыдущих атак или технические возможности доступных на российском рынке ИБ-решений, уже позволяют говорить об их чрезвычайности.

В свете изложенного любые категоричные суждения о том, что все компьютерные атаки являются обстоятельством непреодолимой силы⁴¹ или, наоборот, в любом случае не могут признаваться таковыми⁴², едва ли учитывают специфику этого явления. Представляется, что компьютерная атака по умолчанию не должна признаваться форс-мажором, однако в исключительных случаях, когда оператор цифрового сервиса принял меры по обеспечению информационной безопасности, установленные в отношении него законом для противодействия таким внешним воздействиям (если предусмотрены), или разумно ожидаемые от него меры исходя из обычаев делового оборота для такого рода сервисов (в отсутствие законодательных требований), но интенсивность (мощность) компьютерной атаки позволила ей обойти такие меры и выделяется из общей статистики подобных атак, такая компьютерная атака в конкретном споре может быть признана обстоятельством непреодолимой силы.

Вероятно следуя той же логике, В. В. Байбак и А. Г. Карапетов допускают квалификацию в качестве форс-мажора «масштабной цифровой атаки на российскую банковскую систему»⁴³, где клю-

³⁵ ФНС подверглась масштабной кибератаке // URL: <https://www.kommersant.ru/doc/7736483> (дата обращения: 01.03.2026).

³⁶ Минцифры сообщило о DDoS-атаках на «Госуслуги» со стороны Украины // URL: https://www.rbc.ru/technology_and_media/23/06/2022/62b43ea09a79471246251381 (дата обращения: 01.03.2026).

³⁷ Telegraph: спецслужбы Великобритании не могут полностью защитить страну от кибератак РФ // URL: <https://tass.ru/mezhdunarodnaya-panorama/5148364> (дата обращения: 01.03.2026).

³⁸ Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. 3-е изд., перераб. и доп. М. : Статут, 2020. С. 343.

³⁹ Постановление Арбитражного суда Дальневосточного округа от 21.06.2023 № Ф03-1892/2023.

⁴⁰ См., например: решение Арбитражного суда Республики Мордовия от 08.02.2023 по делу № А39-7372/2022 ; решение Арбитражного суда Забайкальского края от 27.02.2023 по делу № А78-11132/2022 и др.

⁴¹ Дадалко В. А., Благодаров Д. Н. Влияние безопасности интернет-банкинга на конкурентоспособность банка // Международное публичное и частное право. 2013. № 4. С. 19–22.

⁴² Савельев А. И. Указ. соч. С. 343.

⁴³ Перемена лиц в обязательстве и ответственность за нарушение обязательства : комментарий к статьям 330–333, 380–381, 382–406.1 Гражданского кодекса Российской Федерации (Электронное издание. Редакция 2.0) / отв. ред. А. Г. Карапетов. М. : М-Логос, 2022. С. 856.

чевым фактором, как видится, является именно ее масштабность. Усилить позицию оператора цифрового сервиса относительно форс-мажорности произошедшей атаки может ссылка на другие компьютерные атаки сопоставимой мощности⁴⁴, которые ранее приводили к сбоям в государственных или финансовых сервисах, а значит, он, обладая существенно меньшими ресурсами, также не смог противостоять такой атаке.

Оценка возможности квалификации компьютерной атаки как обстоятельства непреодолимой силы должна осуществляться судом — как это происходит и при квалификации любых иных событий в качестве таковых — с учетом заключений экспертов и консультаций специалистов в соответствующей области. При этом сдерживающим фактором от уклонения оператором цифрового сервиса от имущественной ответственности станут репутационные риски при ссылках на непредотвратимость для него компьютерных атак.

В то же время сразу в нескольких арбитражных спорах об ответственности оператора цифрового сервиса перед клиентом за инцидент, вызванный компьютерной атакой, суды встали на сторону оператора, мотивировав это не форс-мажорностью атаки, а отсутствием в договоре с клиентом обязательств оператора по защите от неправомерных действий третьих лиц⁴⁵. Возникает вопрос: а не должно ли принятие соответ-

ствующих мер входить в стандарт должной осмотрительности оператора цифрового сервиса?

4. Обязанность по противодействию компьютерным атакам как должная осмотрительность

Операторы цифровых сервисов в отношениях со своими контрагентами широко используют институт договорного ограничения ответственности. Условия, исключающие ответственность оператора цифрового сервиса при недоступности сервиса из-за компьютерных атак, содержатся в офертах крупнейших цифровых сервисов в своей отрасли⁴⁶. Это может говорить как о дисбалансе договорных условий⁴⁷, так и о неготовности операторов таких сервисов гарантировать их бесперебойность.

Однако, как верно замечает М. А. Церковников, «судебная практика по конкретным делам даже при наличии допустимой по п. 4 ст. 401 ГК РФ оговорки об ограничении ответственности может констатировать наличие умысла, если должник значительно отступил от требуемого стандарта поведения»⁴⁸. Рассматривая спор о пределах ответственности исполнителя по договору возмездного оказания услуг, Верховный Суд в 2024 г. сформулировал правило, согласно

⁴⁴ Такие сведения часто публикуют СМИ или сами потерпевшие компании в пресс-релизах по результатам атаки. Без сопоставления технических атак предложенная аргументация видится менее эффективной.

⁴⁵ Постановление Арбитражного суда Московского округа от 08.12.2023 № Ф05-28661/2023 по делу № А40-293189/2022 ; постановление Тринадцатого арбитражного апелляционного суда от 27.10.2025 по делу № А56-85885/2024.

⁴⁶ П. 2.14 Правил информационной системы АО «Альфа-Банк» // URL: https://alfabank.servicecdn.ru/site-upload/7a/6e/7579/pravila_informacionnoi_sistemy_v3_11062025.pdf (дата обращения: 01.03.2026) ; п. 8.1 Пользовательского соглашения сайта оператора финансовой платформы «Финуслуги» в информационно-телекоммуникационной сети «Интернет» и мобильного приложения «Финуслуги» // URL: <https://assets.finuslugi.ru/mp-assets/user-agreement.pdf> (дата обращения: 01.03.2026) ; п. 9.9.10 Оферты о реализации товаров на сайте Wildberries // URL: <https://static-basket-02.wbbasket.ru/vol20/offers/prd/product/88/4a5d9eaa-0fdc-4845-b987-d9426b4cb64f.pdf> (дата обращения: 01.03.2026).

⁴⁷ См. об этом, например: *Зубарев Н. С.* Оферта как инструмент правового регулирования предпринимательской деятельности с использованием маркетплейсов: опыт «Озона» и «Вайлдберриз» // Актуальные проблемы российского права. 2025. Т. 20. № 6. С. 95.

⁴⁸ *Церковников М. А.* Об ограничении ответственности cedenta за недействительность уступаемого права: комментарий к абз. 2 п. 1 ст. 390 Гражданского кодекса РФ // Вестник гражданского права. 2024. № 6. С. 255.

которому «исполнитель... не вправе ссылаться на оговорку об исключении или ограничении ответственности, если выполненные им действия или осуществленная им деятельность были столь упречными (непрофессиональными), что затронули само существо исполняемого обязательства и лишили полезного смысла заключение договора для заказчика»⁴⁹.

Представляется, что, если оператор цифрового сервиса не принял обязательных мер кибербезопасности, которые установлены в отношении его сервиса специальным законодательством, стандарт «минимальной степени заботливости и осмотрительности»⁵⁰ должен считаться невыполненным, а ответственность — наступать в полном объеме⁵¹. В этом смысле публично-правовые нормы информационного законодательства будут влиять на частноправовые отношения, что, по мнению автора, не вызывает противоречий, а, наоборот, способствует большей правовой определенности при прогнозировании «минимально достаточных мер».

И всё же, что, если такие обязанности в отраслевом законодательстве пока отсутствуют (как, например, для посреднических цифровых платформ)? Несомненно, это не может быть интерпретировано как дозволение оператору цифрового сервиса не принимать никаких мер по противодействию компьютерным атакам в принципе, ограничивая свою ответственность договором. Ведь содержание их обязательств перед клиентами включает работоспособность

и доступность предоставляемых сервисов, иное противоречило бы самой сути экономических отношений сторон. В практике арбитражных судов встречается тезис, что «обеспечение компьютерной безопасности организации является обязанностью самой организации, в противном случае риск наступления неблагоприятных последствий в результате такого бездействия несет указанное лицо»⁵². Более того, операторов цифровых сервисов можно считать профессиональными участниками рынка и требовать от них повышенных стандартов кибербезопасности.

Заключение

Как показало исследование, в российском законодательстве прослеживается тенденция возложения на операторов цифровых сервисов обязанности по противодействию компьютерным атакам. Законодатель выбрал путь отраслевого регулирования (по видам сервисов), что вполне оправданно ввиду разной социальной значимости и специфики отдельных сервисов.

Компьютерные атаки, за исключением атак высокой интенсивности (мощности), уже не являются форс-мажором, а стали объективной реальностью и обычным предпринимательским риском для ИТ-рынка. Недостаток и существующей судебной практики, и отдельных доктринальных представлений по вопросам возможности квалификации компьютерных атак как обстоятельств непреодолимой силы — непринятие во внима-

⁴⁹ П. 26 Обзора судебной практики Верховного Суда РФ № 1 (2025), утв. Президиумом Верховного Суда РФ 25 апреля 2025 г. // СПС «КонсультантПлюс».

⁵⁰ Перемена лиц в обязательстве и ответственность за нарушение обязательства... С. 1365–1366. См. также: *Логинов Е. А.* К вопросу о содержании обязательства исполнителя в договоре возмездного оказания услуг. Комментарий к определению Судебной коллегии по экономическим спорам ВС РФ от 13.02.2024 № 305-ЭС23-18507 // Вестник экономического правосудия Российской Федерации. 2024. № 7. С. 12–31.

⁵¹ Абз. 2 п. 7 постановления Пленума Верховного Суда РФ от 24.03.2016 № 7. Важно учитывать, что в договорах с потребителями условие об ограничении ответственности оператора цифрового сервиса при компьютерных атаках будет признано недействительным как ущемляющее права потребителя в силу пп. 4 п. 2 ст. 16 Закона РФ от 07.02.1992 № 2300-1 «О защите прав потребителей» (СЗ РФ. 1996. № 3. Ст. 140).

⁵² Постановление Пятнадцатого арбитражного апелляционного суда от 23.10.2020 № 15АП-15249/2020 по делу № А53-18497/2020 ; решение Арбитражного суда г. Москвы от 21.09.2022 по делу № А40-98900/22-189-752.

ние интенсивности (мощности) конкретной компьютерной атаки. Хотя такая дифференциация видится наиболее справедливой и соответствующей специфике этого явления.

Современные реалии правоприменения свидетельствуют о том, что даже при отсутствии специальных обязанностей по противодействию компьютерным атакам в законодательстве оператор цифрового сервиса всё равно не может не принимать таких мер, ограничив свою ответственность за сбои в сервисе в договоре. Такая обязанность с частноправовой точки зрения будет существовать для него априори в рамках выработанного судебной практикой и доктриной стандарта минимальной степени заботливости и осмотрительности, а ее игнорирование приведет к ничтожности договорных условий об ограничении ответственности при сбоях и инцидентах, которые содержатся практически в каждой оферте крупного цифрового сервиса. В то же время запрет договорного ограничения ответственности за сбои в сервисе в предпринимательских договорах⁵³ будет ущемлять как добросовестного оператора цифрового сервиса,

так и его клиентов — у участников цифрового рынка должна быть возможность согласовывать ограниченную ответственность за счет более низкой цены сервиса.

Публично-правовые по своему характеру нормы, устанавливающие требования к информационной безопасности цифрового сервиса, было бы рационально использовать в качестве критериев упомянутого стандарта должной осмотрительности в договорных отношениях по предоставлению цифрового сервиса его оператором. Такой подход обеспечит большую прозрачность для участников рынка, а отраслевые регуляторы уже обладают необходимыми компетенциями для формирования сбалансированных и конкретных мер по противодействию компьютерным атакам. Отсутствие же соответствующих норм в отношении операторов посреднических цифровых платформ и других субъектов создает правовую неопределенность, предпосылки для противоречивого правоприменения и злоупотреблений как в частноправовом, так и в публично-правовом поле.

БИБЛИОГРАФИЯ

1. Байбак В. В. Непреодолимая сила (форс-мажор) как основание освобождения от договорной ответственности (сравнительно-правовой очерк) // Закон. — 2025. — № 6. — С. 166–180.
2. Государство, общество и личность: пути преодоления вызовов и угроз в информационной сфере : монография / Н. С. Волкова, А. А. Ефремов, С. М. Зырянов [и др.] ; отв. ред. Л. К. Терещенко. — М. : Инфотропик Медиа, 2024. — 352 с.
3. Дадалко В. А., Благодаров Д. Н. Влияние безопасности интернет-банкинга на конкурентоспособность банка // Международное публичное и частное право. — 2013. — № 4. — С. 19–22.
4. Жижина М. В., Завьялова Д. В. Личность субъекта преступлений в сфере компьютерной информации как системообразующий элемент криминалистической характеристики (по материалам российских и зарубежных источников) // Актуальные проблемы российского права. — 2022. — Т. 17. — № 5. — С. 149–158.
5. Зубарев Н. С. Оферта как инструмент правового регулирования предпринимательской деятельности с использованием маркетплейсов: опыт «Озона» и «Вайлдберриз» // Актуальные проблемы российского права. — 2025. — Т. 20. — № 6. — С. 86–96.
6. Кудинов В. В., Минаев А. В. Кибертерроризм: основные угрозы и проблемы правового регулирования национальной безопасности Российской Федерации // Конституционное и муниципальное право. — 2022. — № 4. — С. 53–56.

⁵³ Харитонова Ю. С. Ответственность владельца за некорректную работу цифровой платформы // Законы России: опыт, анализ, практика. 2023. № 12. С. 24.

7. Курбатов А. Я. Обстоятельства непреодолимой силы: разграничение со смежными понятиями // Законы России: опыт, анализ, практика. — 2025. — № 1. — С. 56–61.
8. Логинов Е. А. К вопросу о содержании обязательства исполнителя в договоре возмездного оказания услуг. Комментарий к определению Судебной коллегии по экономическим спорам ВС РФ от 13.02.2024 № 305-ЭС23-18507 // Вестник экономического правосудия Российской Федерации. — 2024. — № 7. — С. 12–31.
9. Образование и занятость: правовые вопросы новой цифровой реальности : монография / Н. С. Волкова, О. Ю. Еремина, О. В. Моцная [и др.] ; отв. ред. Н. С. Волкова, Н. В. Путило ; Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. — М. : Юриспруденция, 2025. — 192 с.
10. Перемена лиц в обязательстве и ответственность за нарушение обязательства : комментарий к статьям 330–333, 380–381, 382–406.1 Гражданского кодекса Российской Федерации (Электронное издание. Редакция 2.0) / отв. ред. А. Г. Карапетов. — М. : М-Логос, 2022. — 1582 с.
11. Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. — 3-е изд., перераб. и доп. — М. : Статут, 2020. — 920 с.
12. Харитонова Ю. С. Ответственность владельца за некорректную работу цифровой платформы // Законы России: опыт, анализ, практика. — 2023. — № 12. — С. 19–24.
13. Церковников М. А. Об ограничении ответственности cedenta за недействительность уступаемого права: комментарий к абз. 2 п. 1 ст. 390 Гражданского кодекса РФ // Вестник гражданского права. — 2024. — № 6. — С. 239–259.
14. Швырев Б. А., Тищенко Ю. Ю. Кибератаки: иммерсионная образовательная среда и ее формирование // Уголовно-исполнительная система: право, экономика, управление. — 2024. — № 1. — С. 30–33.

Материал поступил в редакцию 25 марта 2026 г.

REFERENCES (TRANSLITERATION)

1. Baybak V. V. Nepreodolimaya sila (fors-mazhor) kak osnovanie osvobozhdeniya ot dogovornoy otvetstvennosti (sravnitel'no-pravovoy ocherk) // Zakon. — 2025. — № 6. — S. 166–180.
2. Gosudarstvo, obshchestvo i lichnost: puti preodoleniya vyzovov i ugroz v informatsionnoy sfere: monografiya / N. S. Volkova, A. A. Efremov, S. M. Zyryanov [i dr.]; отв. ред. L. K. Tereshchenko. — M.: Infotropik Media, 2024. — 352 s.
3. Dadalko V. A., Blagodarov D. N. Vliyanie bezopasnosti internet-bankinga na konkurentosposobnost banka // Mezhdunarodnoe publichnoe i chastnoe pravo. — 2013. — № 4. — S. 19–22.
4. Zhizhina M. V., Zavyalova D. V. Lichnost subekta prestupleniy v sfere kompyuternoy informatsii kak sistemoobrazuyushchiy element kriminalisticheskoy kharakteristiki (po materialam rossiyskikh i zarubezhnykh istochnikov) // Aktual'nye problemy rossijskogo prava. — 2022. — T. 17. — № 5. — S. 149–158.
5. Zubarev N. S. Oferta kak instrument pravovogo regulirovaniya predprinimatelskoy deyatel'nosti s ispolzovaniem marketpleysov: opyt «Ozona» i «Vayldberriz» // Aktual'nye problemy rossijskogo prava. — 2025. — T. 20. — № 6. — S. 86–96.
6. Kudinov V. V., Minaev A. V. Kiberterrorizm: osnovnye ugrozy i problemy pravovogo regulirovaniya natsionalnoy bezopasnosti Rossiyskoy Federatsii // Konstitutsionnoe i munitsipalnoe pravo. — 2022. — № 4. — S. 53–56.
7. Kurbatov A. Ya. Obstoyatelstva nepreodolimoy sily: razgranichenie so smezhnymi ponyatiymi // Zakony Rossii: opyt, analiz, praktika. — 2025. — № 1. — S. 56–61.
8. Loginov E. A. K voprosu o sodержanii obyazatelstva ispolnitelya v dogovore vozmezdnoy okazaniya uslug. Kommentariy k opredeleniyu Sudebnoy kollegii po ekonomicheskim sporam VS RF ot 13.02.2024 № 305-ES23-18507 // Vestnik ekonomicheskogo pravosudiya Rossiyskoy Federatsii. — 2024. — № 7. — S. 12–31.

9. Obrazovanie i zanyatost: pravovye voprosy novoy tsifrovoy realnosti: monografiya / N. S. Volkova, O. Yu. Eremina, O. V. Motsnaya [i dr.]; otv. red. N. S. Volkova, N. V. Putilo; Institut zakonodatelstva i sravnitel'nogo pravovedeniya pri Pravitel'stve Rossiyskoy Federatsii. — M.: Yurisprudentsiya, 2025. — 192 s.
10. Peremena lits v obyazatel'stve i otvetstvennost za narushenie obyazatel'stva: kommentariy k statyam 330–333, 380–381, 382–406.1 Grazhdanskogo kodeksa Rossiyskoy Federatsii (Elektronnoe izdanie. Redaktsiya 2.0) / otv. red. A. G. Karapetov. — M.: M-Logos, 2022. — 1582 s.
11. Savelev A. I. Elektronnyaya kommertsiya v Rossii i za rubezhom: pravovoe regulirovanie. — 3-e izd., pererab. i dop. — M.: Statut, 2020. — 920 s.
12. Kharitonova Yu. S. Otvetstvennost vladeltsa za nekorrektnuyu rabotu tsifrovoy platformy // Zakony Rossii: opyt, analiz, praktika. — 2023. — № 12. — S. 19–24.
13. Tserkovnikov M. A. Ob ogranichenii otvetstvennosti tsedenta za nedeystvitelnost ustupaemogo prava: kommentariy k abz. 2 p. 1 st. 390 Grazhdanskogo kodeksa RF // Vestnik grazhdanskogo prava. — 2024. — № 6. — S. 239–259.
14. Shvyrev B. A., Tishchenko Yu. Yu. Kiberataki: immersionnaya obrazovatel'naya sreda i ee formirovanie // Ugolovno-ispolnitelnaya sistema: pravo, ekonomika, upravlenie. — 2024. — № 1. — S. 30–33.