Дата поступления рукописи в редакцию: 31.05.2026 г.
Дата принятия рукописи в печать: 11.07.2026 г.

DOI: 10.24412/2782-3849-2026-7-326-330

БОЗИЕВ Мурат Владимирович,

майор полиции, преподаватель, Северо-Кавказский институт повышения квалификации сотрудников МВД России (филиал) Краснодарского университета МВД России, кафедра специальных дисциплин,

e-mail: mail@law-books.ru

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ВМЕШАТЕЛЬСТВА В ДЕЯТЕЛЬНОСТЬ СУДА И СЛЕДСТВЕННЫХ ОРГАНОВ С ПОМОЩЬЮ ИТ-ИНСТРУМЕНТОВ

Аннотация. *В статье рассматриваются современные проблемы квалификации вмешательства в деятельность суда и следственных органов с использованием информационно-технологических инструментов. Анализируется действующее уголовное законодательство Российской Федерации, в частности положения статьи 294 УК РФ, а также смежные нормы о преступлениях в сфере компьютерной информации. Отмечается, что существующая правоприменительная практика не учитывает специфики цифровых способов воздействия на судебные и следственные процессы. На основе примеров кибератак на государственные ресурсы, включая ГАС «Правосудие» и сайты судов субъектов РФ, выявлены пробелы в законодательстве и сложности доказывания прямого умысла на воспрепятствование осуществлению правосудия. Делается вывод о необходимости совершенствования диспозиции статьи 294 УК РФ, с учётом современных форм цифрового вмешательства, а также выработки методических рекомендаций для следователей и прокуроров по квалификации подобных деяний.*

Ключевые слова: *киберпреступления, вмешательство в правосудие, ст. 294 УК РФ, ИТ-инструменты, цифровое правосудие, кибератаки, квалификация преступлений, информационная безопасность.*

BOZIEV Murat Vladimirovich,

police major, teacher, North Caucasian Institute for Advancement qualifications of employees of the Ministry of Internal Affairs of Russia (branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia, Department of Special Disciplines

PROBLEMS OF QUALIFICATION OF INTERFERENCE IN THE ACTIVITIES OF THE COURT AND INVESTIGATIVE BODIES USING IT TOOLS

Annotation. *The article examines the current issues of classifying interference in the activities of courts and investigative bodies through the use of information technology tools. The research analyzes the criminal legislation of the Russian Federation, particularly Article 294 of the Criminal Code, as well as related provisions concerning cybercrime. It is noted that existing law enforcement practice does not adequately address the specifics of digital methods of influence on judicial and investigative procedures. Using examples of cyberattacks on government information systems, including the State Automated System "Justice" and regional court websites, the paper identifies gaps in legislation and difficulties in proving direct intent to obstruct justice. The author concludes that it is necessary to improve the wording of Article 294 of the Criminal Code, taking into account modern forms of digital interference, and to develop methodological recommendations for investigators and prosecutors regarding the qualification of such acts*.

Key words: *cybercrime, obstruction of justice, Article 294 of the Criminal Code of the Russian Federation, IT tools, digital justice, cyberattacks, criminal qualification, information security.*

Цифровизация правовой системы, внедрение информационно-технологических средств в деятельность судебной и следственной ветвей власти, активное использование интернета, облачных сервисов, удалённого взаимодействия — всё это расширяет не только спектр возможной правозащитной деятельности, но и возможности неправомерного вмешательства. В таком контексте остро встаёт вопрос: как квалифицировать преступления, связанные с вмешательством в деятельность суда и органов предварительного расследования,

если используются ИТ-средства? Действующие нормы УК РФ (в первую очередь ст. 294 и главы о компьютерных преступлениях) в значительной степени обусловлены эпохой докомпьютерной или начальной компьютерной, и реальность порой обходит правовые рамки[1].

Цель исследования — выявить основные пробелы в правоприменительной практике по квалификации вмешательства с применением ИТ-инструментов, оценить сложности доказывания, показать примеры из судебной практики, и предложить проект законодательных и методических изменений, которые позволят повысить точность правовых оценок, защитить законные интересы, не допустить чрезмерной криминализации.

К сегодняшнему дню российские суды и следственные органы переживают активный этап цифровой трансформации: электронные провадження, автоматизированные информационные системы, применение аналитики и ИИ для контроля за преступностью и управления делопотоком. Это меняет не только способы совершения преступлений, но и границы того, что считать «вмешательством» в деятельность органов правосудия и предварительного расследования. При этом уголовно-правовой аппарат, сформированный в эпоху, когда ключевые формы преступлений представлялись бумажными и бытовыми, порой с трудом адаптируется под новые технологические реалии.

Ключевой правовой якорь — ст. 294 УК РФ — довольно емко описывает составы: вмешательство в деятельность суда в целях воспрепятствования осуществлению правосудия и вмешательство в деятельность прокурора, следователя или дознавателя в целях воспрепятствования всестороннему, полному и объективному расследованию. Однако диспозиция сформулирована в общих терминах «вмешательство в какой бы то ни было форме», что порождает широкий простор для толкований, особенно в части ИТ-действий: от DDoS-атак на веб-портал суда до подмены электронных документов, до распространения фальсифицированных протоколов и «ботополот» в медиа-пространстве.

Практическая сторона квалификации обостряется взаимодействием со статьями главы 28 УК РФ «Преступления в сфере компьютерной информации». Так, неправомерный доступ к компьютерной информации, уничтожение или модификация данных, создание угроз — уже описаны в ст. 272 и смежных нормах. Но преступление «вмешательства в деятельность суда/следствия» несет целевой признак — намерение воспрепятствовать правосудию или расследованию — тогда как компьютерные преступления часто рассматриваются через призму технического вреда (ущерб, несанкционированный доступ). На практике это порождает два сценария: (1) одни и те же деяния квалифицируются по «компьютерке» без учёта общеопасного (целевого) аспекта; (2) квалификация по ст. 294 применяется при наличии доказанного целевого мотива, что требует иного набора доказательств (цель, связь деяния с препятствием расследованию). Такая дублированность ведет к правовой неопределенности и различной правоприменительной практике.

Доказательная проблема в данном случае является одной из центральных. Для квалификации по ст. 294 необходимо установить субъект, объект, деяние и, в особенности, цель — намерение воспрепятствовать. ИТ-инструменты вносят сложности: анонимность в сети, использование посредников, георасределенные инфраструктуры, использование легитимных сервисов (облачные хостинги, VPN, мессенджеры), автоматизация и скрипты. Прокурору и следователю приходится доказывать, что конкретная DDoS-кампания или утечка данных преследовала цель помешать следствию — доказательства часто косвенные: синхронность атак с ключевыми процессуальными действиями, целевая рассылка с предупреждениями, связь с фигурантами дела и т.п.[10] В отсутствии прямых доказательств умысла суды склонны квалифицировать по «техническим» составам, что снижает общественную резонансность и иногда — адекватность наказания. Практические обзоры указывают на рост дел, связанных с ИТ-атаками на государственные системы, однако заметна нехватка единообразной практики по ст. 294 в цифровом контексте [2][6].

Еще одна проблема — граница между допустимой процессуальной активностью и преступным вмешательством. Законный доступ к данным, жалобы, публикации и иные формы защиты интересов сторон не должны превращаться в криминализацию защищённых прав. Но цифровые технологии позволяют обострять последствия даже без прямого уголовного умысла: например, массовая публикация чувствительных личных данных свидетелей (doxxing) может непреднамеренно воспрепятствовать показаниям и быть квалифицирована как вмешательство. Тут нужны четкие стандарты оценивания последствий действий, шкала ответственности в зависимости от результата (вред/угроза/реальные препятствия расследованию) и внимания к мотивам. Экспертные публикации отмечают, что без технических критериев и экспертиз

квалификация будет оставаться произвольной. [4][5]

Наконец, институциональные вызовы. Цифровые следы требуют от органов предварительного расследования цифровой экспертизы высокой квалификации: сбор логов, трассировка источников, атрибуция атак — всё это дорого и технически сложно. Межведомственное взаимодействие (полиция, ФСБ, специализированные лаборатории) развивается, однако пока страдает оперативность и стандартизация процедур. Государственные инициативы по повышению кибербезопасности и регламентации (пилотные проекты ГИС, требования по защите информации) идут в ногу с ростом угроз, но это не заменяет необходимости уголовно-правовой ясности при квалификации деяний против правосудия в цифровой среде. [12].

Ярким примером вмешательства в деятельность судов с использованием ИТ-инструментов стала зафиксированная в 2022-2023 гг. хакерская атака на сайты арбитражных судов России. На главных страницах судов Амурской области и др. появились оскорбительные тексты, связанные с политическими событиями, сайты были недоступны некоторое время. Это явно вмешательство в работу судебной системы средствами ИТ — хотя, по публичным источникам, неясно, применялась ли ст. 294 УК РФ к лицам, совершившим атаку. [5]

Отдельного внимания заслуживает инцидент с атаками на ГАС «Правосудие», после которого Верховный суд России заявил, что будет усиливать защиту системы, создавать спецотдел информационной безопасности. Это индикатор того, что управление судебной информационной системой подразумевает риски вмешательства со стороны злоумышленников, и де-юре вмешательство уже было, пусть и не всегда квалифицировано по ст. 294. [11]

Что делать на практике и в теории? Во-первых, правоприменителям и законодателю представляется необходимым прописать технико-юридические ориентиры: примеры типовых форм «вмешательства» через ИТ, критерии установления связи между ИТ-действием и препятствованием расследованию, стандарты оценки последствий. Во-вторых, необходимо усиление цифровой компетенции следствия: создание централизованных экспертных площадок, типовых методик атрибуции и процедур хранения цифровых доказательств. В-третьих, полезно предусмотреть отдельную квалификацию или квалифицирующие признаки за использование высокотехнологичных средств при воспрепятствовании правосудию (аналогично тому, как ст. 294 ч. 3 ужесточает ответственность при служебном положении) — это помогло бы соотнести общественную опасность и санкции. Наконец, важна судебно-правовая практика: систематизация решений высших судов и публикация аналитических обзоров облегчат выработку единых подходов [12][14]..

В связи с изложенным, представляется целесообразным изложить диспозицию ч.1 ст.294 УК РФ в следующей редакции: «Вмешательство в какой бы то ни было форме, в том числе с использованием информационно-технологических средств (путем несанкционированного доступа к информационным системам суда либо органов предварительного расследования, искажения, уничтожения или модификации электронных документов, блокировки/нарушения доступа к цифровым сервисам, публикации, манипуляции с данными в сети), в деятельность суда в целях воспрепятствования осуществлению правосудия…». Аналогичные поправки следует предусмотреть для чч. 2, 3 ст.294 УК РФ, где речь идет о следствии, дознании, прокуроре, и при использовании служебного положения.

Альтернативным вариантом уточнения диспозиции ст.294 УК РФ может стать введение квалифицирующего признака: «если вмешательство приведено с использованием высокотехнологичных средств (кибератаки, автоматизированные бот-сети, программные средства для фальсификации данных)» с установлением более строгого наказания.

Заключение. Цифровая трансформация приносит новые возможности, но и ставит перед уголовным правом задачу реконцептуализации преступлений против деятельности суда и следствия. Существующие нормы (включая ст. 294 УК РФ и главы о компьютерных преступлениях) в целом пригодны, но требуют технической конкретизации, унифицированных процедур доказывания и усиления экспертной поддержки. Без этого правоохранительная практика рискует либо недооценивать современные угрозы (переквалификация на «компьютерку» без учёта целевого компонента), либо чрезмерно криминализировать публичную процессуальную активность. Решение лежит на стыке права и техники: нужно вводить понятия, которые бы позволяли однозначно соотносить ИТ-действия с целью воспрепятствования правосудию и при этом защищать законные способы защиты прав и свободы выражения.

Список литературы:

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 01.07.2025) // Собрание законодательства РФ. — 1996. — № 25. — Ст. 2954.

[2] Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации» // Российская газета. — 2022. — № 289.

[3] Кудрявцев Н. А. Воспрепятствование осуществлению правосудия и производству предварительного расследования: проблемы квалификации и правоприменения // Российский следователь. — 2023. — № 8. — С. 35–42.

[4] Гаврилов Б. Я. Проблемы правовой квалификации преступлений, совершаемых с использованием цифровых технологий // Законность. — 2024. — № 2. — С. 18–26.

[5] Киселёв А. И. Современные подходы к определению вмешательства в деятельность суда и следственных органов в условиях цифровизации // Вестник Волгоградского государственного университета. Серия 5: Юриспруденция. — 2023. — Т. 22, № 4. — С. 77–86.

[6] Обзор судебной практики по ст. 294 УК РФ (воспрепятствование осуществлению правосудия и производству предварительного расследования) // СПС «КонсультантПлюс». — Режим доступа: https://www.consultant.ru (дата обращения: 06.10.2025).

[7] Прокуратура Тамбовской области. Разъяснение о применении статьи 294 УК РФ // Официальный сайт прокуратуры Тамбовской области. — 2024. — Режим доступа: https://epp.genproc.gov.ru (дата обращения: 06.10.2025).

[8] Характеристика субъективной стороны воспрепятствования осуществлению правосудия и производства предварительного расследования // Вестник Московского университета МВД России. — 2022. — № 6. — С. 54–61.

[9] Как российские суды наказывают за киберпреступления // TAdviser. — 2023. — Режим доступа: https://www.tadviser.ru (дата обращения: 06.10.2025).

[10] В УК может появиться наказание за DDoS-атаки // Российская газета. — 2024. — № 112. — Режим доступа: https://rg.ru (дата обращения: 06.10.2025).

[11] Отраслевая судебная практика в области информационной безопасности // itWeek. — 2023. — № 10. — Режим доступа: https://www.itweek.ru (дата обращения: 06.10.2025).

[12] Научно-правовой анализ статьи 294 УК РФ // CyberLeninka. — 2023. — Режим доступа: https://cyberleninka.ru (дата обращения: 06.10.2025).

[13] Тенденция расширения применения статьи 294 УК РФ в современной судебной практике // Юридический мир. — 2024. — № 3. — С. 44–52.

[14] Уголовные дела о неправомерном воздействии на критическую информационную инфраструктуру Российской Федерации // TAdviser. — 2024. — Режим доступа: https://www.tadviser.ru (дата обращения: 06.10.2025).

References:

[1] Criminal Code of the Russian Federation No. 63-FZ dated June 13, 1996 (as amended by 01.07.2025) //Collection of Legislation of the Russian Federation. — 1996. — № 25. - Art. 2954.

[2] Resolution of the Plenum of the Supreme Court of the Russian Federation of December 15, 2022 No. 37 “On some issues of judicial practice in criminal cases of crimes in the field of computer information “//Rossiyskaya Gazeta. — 2022. — № 289.

[3] Kudryavtsev N. A. Obstruction of justice and preliminary investigation: problems of qualification and law enforcement//Russian investigator. — 2023. — № 8. - S. 35-42.

[4] Gavrilov B. Ya. Problems of legal qualification of crimes committed using digital technologies//Legality. — 2024. — № 2. - S. 18-26.

[5] Kiselev A.I. Modern approaches to determining interference in the activities of the court and investigative bodies in the context of digitalization//Bulletin of Volgograd State University. Series 5: Jurisprudence. — 2023. - T. 22, NO. 4. - S. 77-86.

[6] Review of judicial practice under Art. 294 of the Criminal Code (obstruction of justice and preliminary investigation)//SPS “ConsultantPlus.” - Access mode: https://www.consultant.ru (access date: 06.10.2025).

[7] Prosecutor’s Office of the Tambov Region. Clarification on the application of Article 294 of the Criminal Code of the Russian Federation// Official website of the prosecutor’s office of the Tambov region. — 2024. - Access mode: https://epp.genproc.gov.ru (access date: 06.10.2025).

[8] Description of the subjective side of obstruction of justice and preliminary investigation// Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. — 2022. — № 6. - S. 54-61.

[9] How Russian courts punish cybercrimes// TAdviser. — 2023. - Access mode: https://www.tadviser.ru (access date: 06.10.2025).

[10] Punishment for DDoS attacks may appear in the Criminal Code//Rossiyskaya Gazeta. — 2024. — № 112. - Access mode: https://rg.ru (access date: 06.10.2025).

[11] Information Security Industry Litigation Practice//itWeek. — 2023. — № 10. - Access mode: https://www.itweek.ru (access date: 06.10.2025).

[12] Scientific and legal analysis of Article 294 of the Criminal Code of the Russian Federation// CyberLeninka. — 2023. - Access mode: https://cyberleninka.ru (access date: 06.10.2025).

[13] The tendency to expand the application of Article 294 of the Criminal Code of the Russian Federation in modern judicial practice//Legal world. — 2024. — № 3. - S. 44-52.

[14] Criminal cases on unlawful impact on the critical information infrastructure of the Russian Federation//TAdviser. — 2024. - Access mode: https://www.tadviser.ru (access date: 06.10.2025).