ОТЗЫВ

официального оппонента

на диссертацию Аббуда Руслана Ратебовича на тему «Международно-правовое регулирование противодействия киберпреступлениям», представленной на соискание учёной степени кандидата юридических наук по научной специальности 5.1.5. Международно-правовые науки (юридические науки)

По данным Международного союза электросвязи, текущий уровень киберугроз оценивается примерно в 2200 кибератак в мире ежедневно, при этом ежегодно количество кибератак в мире увеличивается на 80%. Схожие данные приводит и Роскомнадзор, указывая на то, что с начала специальной военной операции число компьютерных и DDoS-атак ежегодно увеличивается в среднем на 70%. Только некоторые из кибератак, происходящих по всему миру, предположительно организованы государствами: их число на основе общедоступной информации оценивается в 738 атак за период с 2005 по 2023 год включительно.

Лавинообразное увеличение числа кибер-инцидентов, а также милитаризация т.н. «киберпространства» актуализируют вопросы поиска путей для формирования более безопасной глобальной информационной среды. Одну из ключевых ролей в этом процессе играет международное право. Указ Президента Российской Федерации «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» № 309 от 7 мая 2024 г. относит обеспечение сетевого суверенитета и информационной безопасности в информационно-телекоммуникационной сети «Интернет» к целевым показателям и задачам, выполнение которых характеризует достижение национальной цели «Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы» (п. 8 «л»). В соответствии со Стратегией национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 2 июля 2021 г. № 400, одними из стратегических национальных приоритетов являются оборона страны, государственная и общественная безопасность, информационная безопасность, а также стратегическая стабильность и взаимовыгодное международное сотрудничество. Стратегия научно-технологического развития, утвержденная Указом Президента Российской Федерации 28 февраля 2024 г. № 145, относит новые гибридные внешние угрозы национальной безопасности, в том числе военные и информационные, к наиболее значимым для научно-технологического развития России большим вызовам (п. 15 «ж»).

Российская Федерация занимает активную позицию по всем вопросам международно-правовой повестки в области информационной безопасности. В соответствии с Основами государственной политики Российской Федерации в области международной информационной безопасности 2021 г., целью нашего государства является «продвижение на международной арене российских подходов к формированию системы обеспечения международной информационной безопасности и российских инициатив в области международной информационной безопасности» и «содействие созданию международно-правовых механизмов предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве».

Наблюдаются попытки перехвата и узурпирования инициативы в области формирования онтологических основ универсальной (глобальной) повестки международной информационной безопасности. К ним относится подготовка «Таллинского руководства», которое, несмотря на спонсирование НАТО и основную роль военных и дипломатов из этих стран, позиционируется и продвигается как главный источник «экспертного» знания в области применения международного права к «кибероперациям». Кроме того, большинству государств, которые еще не артикулировали свою позицию в данной сфере, навязывается основанная на применении «военной парадигмы» квалификация вредоносного использования информационно-коммуникационных технологий, что открывает двери как для эскалации, так и для ужесточения политики использования односторонних принудительных мер.

Однако при этом нельзя не отметить прорывного характера подписанной в 2025 году в Ханое новой Конвенции Организации Объединенных Наций против киберпреступности, разработка которой является плодом дипломатических и правовых усилий Российской Федерации.

Вместе с тем, внедрение технологии «искусственного интеллекта» (ИИ) и возросшая автономность (и, следовательно, непредсказуемость) «кибероперацій» постоянно усиливают уязвимость государств перед вредоносными действиями в т.н. «киберпространстве». Можно с определенной долей уверенности предположить, что использование ИИ как государственными, так и негосударственными акторами будет только расширяться.

В свете этих тенденций особое значение приобретает изучение текущего состояния и перспектив сотрудничества государств в области противодействия вредоносному использованию информационно-коммуникационных технологий (далее – ИКТ). Отсюда, диссертационное исследование, подготовленное Р. Р. Аббудом, является актуальным и имеет как теоретическое, так и практическое значение.

Достоверность и новизна результатов диссертации

Достоверность результатов диссертационного исследования подтверждается использованием автором действующих источников международного и внутригосударственного права, судебной практики, доктринальных источников, а также применением положений общего международного права, терминологического аппарата дисциплины, а также методов научного анализа.

Новизна сделанных в диссертации выводов и предложений обусловлена тем, что автор не только систематизирует подходы к противодействию киберпреступлениям, отраженные в различных международных договорах, но предпринимает попытку сформулировать концептуальные положения, касающиеся как круга составов, подпадающих под понятие «киберпреступления», так и форм и видов сотрудничества государств в области противодействия этим деяниям.

В диссертации проанализировано значительное число источников – как правовых, так и доктринальных, – которые ещё не становились предметом досконального научного анализа. Отдельно стоит подчеркнуть стремление автора проиллюстрировать свои теоретические рассуждения примерами из практики национальных и международных судов.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Выводы, рекомендации и предложения, сформулированные в диссертации Р. Р. Аббуда, являются научно обоснованными. Диссертация основана на доктрине позитивизма и применении аналитической юриспруденции. В работе грамотно определены и использованы нормативные, доктринальные, а также эмпирические источники. Вынесенные на защиту положения соответствуют сделанным в диссертации выводам.

Следует согласиться с тезисами автора о проблеме терминологической несогласованности в части обозначения правонарушений, совершаемых с использованием ИКТ (второе положение, вынесенное на защиту), а также о наличии пробелов *ratione materiae* в сфере применения международных договоров, регулирующих сотрудничество государств в области противодействия киберпреступности (третье положение, вынесенное на защиту). Сближение национальных подходов к криминализации и процессуальным действиям в отношении киберпреступлений, действительно, может осуществляться благодаря принятию международных договоров универсального и регионального характера (пятое положение, вынесенное на защиту).

Ценность результатов работы для науки и практики

Теоретическая ценность данного диссертационного исследования состоит в том, что оно вносит вклад в разработку целого ряда аспектов международно-правового регулирования государств в области противодействия киберпреступлениям. Разработка этих положений важна, прежде всего, для международного уголовного права и сотрудничества государств в уголовно-правовой сфере. Практическая составляющая данного диссертационного исследования также достаточно важна и заключается в возможности использования сформулированных автором положений в деятельности правоохранительных органов Российской Федерации.

Подтверждение опубликования основных результатов диссертации в научной печати

Основные результаты диссертации представлены в шести статьях, опубликованных в ведущих рецензируемых научных журналах, индексируемых ВАК.

Замечания

1. В центре представленного диссертационного исследования находится понятие «киберпреступление». Автор даёт собственное определение этому термину, понимая под ним «виновно совершенный, несанкционированный доступ к информационно-коммуникационным технологиям при помощи компьютерных устройств и иных технических средств, с целью нанесения как материального, так и нематериального ущерба и влекущее негативные последствия трансграничного характера неограниченному круг лиц» (второе положение на защиту на стр. 12 и стр. 30 диссертации). Из этого определения становится ясным, что в известном диспуте между сторонниками широкого и узкого подхода автор эксплицитно выбирает последний. Однако, во-первых, это явно идёт вразрез с официальной позицией России, отстаивающей необходимость развития международно-правовой базы для преследования не только преступлений, совершаемых в отношении ИКТ, но и посредством ИКТ (экстремизм, детская порнография и др.). Отсюда, отстаивание узкого подхода, как минимум, требует обоснования и аргументирования. Во-вторых, вызывает вопросы внутренняя логика построения диссертационного исследования в связи с тем, что в тексте работы и в положениях на защиту автор ратует за закрепление в качестве киберпреступлений «кибербуллинга» и «дипфейков» (третье положение на защиту на стр. 13), что логически возможно только при условии отстаивания широкого подхода к понятию «киберпреступлений».

2. Представляется спорным тезис автора данной диссертации об исключительно трансграничном характере киберпреступлений (первое положение, вынесенное на защиту, на стр. 12). Это положение не учитывает двух вариантов ситуаций, когда подпадающее под используемую автором дефиницию деяние произойдет действительно на территории одного государства. Первый вариант связан с существующим разделением между Интернетом как публичной и предназначенной для массового потребителя сетью, и промышленными сетями (на англ.: *Industrial Ethernet*). Второй вариант вытекает из возможности установления «стен», отграничивающих национальный сегмент Интернета, что тестируется или уже используется некоторыми государствами.

3. В качестве одного из составных элементов научной новизны автор диссертации указывает на то, что его «исследование содержит анализ систем искусственного интеллекта (далее – ИИ), что позволило прийти к выводу о том, что посредством установления специального алгоритма, ИИ способен обеспечить надлежащую киберзащиту» (стр. 12 диссертации). Эта же мысль повторяется в четвертом положении, вынесенном на защиту: «Предлагается противостоять киберпреступлениям при помощи ИИ путем разработки исходного кода внутреннего инструмента специального программного обеспечения (далее – ПО), посредством которого разработчики систем ИИ смогут находить риски и тем самым выявлять проблемы кибербезопасности» (стр. 13 диссертации). В то время, как этот вывод не является результатом международно-правового исследования и относится к сфере компьютерных наук, диссертант мог бы продемонстрировать, что именно это означает для международного права в целом и для многостороннего или двустороннего сотрудничества государств в области противодействия киберпреступлениям – в частности. Если автор является приверженцем концепции «регулирования через код», это тоже стоило отразить в работе. Однако этого в тексте работы сделано не было, отсюда данный вывод представляется не имеющим отношения к правовому исследованию, коим и должна была являться диссертация по международно-правовым наукам.

4. В восьмом положении, вынесенном на защиту, автор ссылается на решения Европейского Суда по правам человека по делам *Soering* и *Othman (Abu Qatada)* против Великобритании, обсуждая при этом применение экстрадиции в отношении лиц, совершивших киберпреступления. Однако ни в первое, ни во второе из процитированных решений не касались киберпреступлений. Таким образом, в положение, вынесенное на защиту, закралась ошибка.

5. Седьмое положение, вынесенное на защиту, начинается со слов «доказано», при этом приведенная в первом абзаце информация о содержании Конвенции ООН против преступности 2024 года явно носит дескриптивный, а не эвристический характер.

6. Предложение автора квалифицировать «кибератаку, направленную одним государством против другого», как «акт применения силы», «если данная кибератака нарушает цифровой суверенитет государств и угрожает международной информационной безопасности в целом» (стр. 68 диссертации) представляется необоснованным. Диссертант явно смешивает сферы применения запрета применения силы, а также принципа суверенного равенства, добавляя к этому ещё и политико-правовую концепцию международной информационной безопасности. Высказывая суждение об одном из центральных пунктов дискуссии государств о международно-правовой квалификации вредоносного использования ИКТ в межгосударственных отношениях, диссертант не ссылается на позиции государств в этой области и их острую полемику, не раскрывает официальной позиции Российской Федерации, а также даже не делает обзора палитры мнений, представленной в научной литературе.

   Кроме того, предложение автора расширить компетенцию Международного уголовного суда не совсем ясно сформулировано (стр. 69-70 диссертации). Речь идёт о преступлении агрессии, которая может совершаться, по мнению диссертанта, с использованием ИКТ (что следует из того, что диссертант обсуждает в этой части работы нарушение запрета применения силы), или же о всех составах киберпреступлений? При этом идея «*создать*» «Конференцию по обзору Римского статута» (стр. 69 диссертации) представляется ошибочной: возможно, имелось в виду, что необходимо «созвать» такую конференцию? Не понятно также, что имеется автором в виду под «международными силовыми органами» (стр. 70 диссертации)?

7. На стр. 21-22 диссертации автором указано, что «в главе 28 Уголовного Кодекса Российской Федерации (далее – УК РФ) под киберпреступлением понимаются преступления в сфере компьютерной информации, где приведены виды данного рода преступления и не разъяснено понятие». Эта посылка является ошибочной, так как Глава 28 УК РФ названа «Преступления в сфере компьютерной информации» и термином «киберпреступления» кодекс не оперирует.

Помимо этих замечаний и вопросов, следует также отметить, что текст диссертации в ряде месте не согласован, допущено много стилистических и орфографических ошибок. Не ясно, какого именно стандарта оформления сносок придерживался автор. Кроме того, текст на стр. 74-120 изложен в дескриптивном стиле.

Вместе с тем, представленные выше замечания направлены на приглашение к научной дискуссии и дальнейшее развитие заявленной темы.

Диссертационное исследование представляет собой завершенную научно-квалификационную работу и решает научную задачу, заключающуюся в необходимости концептуальной проработки международно-правового регулирования противодействия киберпреступлениям. Таким образом, диссертационная работа Аббуда Руслана Ратебовича «Международно-правовое регулирование противодействия киберпреступлениям» соответствует требованиям II раздела, в том числе пунктов 9-10 Положения о присуждении учёных степеней, утверждённого постановлением Правительства РФ от 24 сентября 2013 года № 842 в действующей редакции, предъявляемым к кандидатским диссертациям, а её автор заслуживает присуждения учёной степени кандидата юридических наук по специальности 5.1.5. Международно-правовые науки (юридические науки).

Официальный оппонент
Профессор, руководитель департамента международного права факультета права, главный редактор «Журнала ВШЭ по международному праву (HSE University Journal of International Law)», доктор юридических наук, 12.00.10 – Международное право; Европейское право (5.1.5. Международно-правовые науки (юридические науки))

Русинова Вера Николаевна

Организация места работы:
Федеральное государственное автономное образовательное учреждение
высшего образования «Национальный исследовательский университет "Высшая школа экономики"»
Адрес: 109028, Москва, Большой Трехсвятительский переулок, д. 3, каб. 227
Раб. тел.: +7 (495) 772-95-90 доб.: 23066
Официальный сайт: https://pravo.hse.ru/intlaw
Адрес электронной почты: vrusinova@hse.ru

«29» сентября 2025 г.

Подпись заверяю
30. 09. 2025
СПЕЦИАЛИСТ ПО ПЕРСОНАЛУ
ШОСТАК И С