«УТВЕРЖДАЮ»
Проректор по научной работе
федерального государственного
бюджетного образовательного
учреждения высшего образования
«Саратовская государственная
юридическая академия»,
доктор юридических наук, профессор
_____ Белоусов С.А.
«18» сентября 2025 г.

ОТЗЫВ

ведущей организации – федерального государственного бюджетного образовательного учреждения высшего образования «Саратовская государственная юридическая академия» на диссертацию Аббуда Руслана Ратебовича «Международно-правовое регулирование противодействия киберпреступлениям», представленную на соискание учёной степени кандидата юридических наук по специальности 5.1.5. Международно-правовые науки

Тема диссертационного исследования Р.Р. Аббуда актуальна. Киберпреступления нередко не ограничиваются юрисдикцией одного государства: преступные действия, включая хакерские атаки, хищение данных, распространение вредоносного программного обеспечения, атаки на критическую инфраструктуру, часто совершаются из-за рубежа, а их последствия проявляются в разных государствах, что делает невозможным эффективное противодействие исключительно на национальном уровне и актуализирует необходимость международно-правового регулирования в данной сфере. Отсутствие в настоящее время действующих международно-правовых инструментов, имеющих глобальный охват и сбалансированных с точки зрения обеспечения государственного суверенитета и трансграничного доступа к данным, обуславливает фрагментарность и недостаточную эффективность противодействия киберугрозам в мировом масштабе, подтверждая актуальность комплексных научных исследований, направленных на разработку теоретических основ и практических моделей гармонизации национальных правовых систем, поиска новых форм

межгосударственного сотрудничества и выработки принципов, способных обеспечить способных обеспечить эффективное пресечение, раскрытие и расследование киберпреступлений, включая создание действенных механизмов оперативного трансграничного обмена информацией, выдачи преступников и сближения национальных правовых стандартов уголовной ответственности за киберпреступления. В этих условиях обращение российских исследователей к международно-правовым проблемам регулирования противодействия киберпреступности заслуживает одобрения и поддержки.

В целом цель и задачи исследования в достаточной степени отражают ключевые особенности содержания темы с учетом ее актуальности, позволяют раскрыть тему и получить значимые для науки международного права результаты. Отдельные сомнения вызывает постановка одной из задач – «проанализировать алгоритм работы систем искусственного интеллекта в качестве противодействия киберпреступлениям»: данная задача видится не вполне уместной и недостаточно отработанной в тексте диссертации.

Работа структурирована надлежащим образом: структура диссертации соответствует поставленным цели и задачам, отвечает требованиям логики планирования научных исследований и изложения их результатов.

Методологическая основа исследования соответствует требованиям, на практике предъявляемым к диссертациям на соискание ученой степени кандидата юридических наук, выбор методов оправдан.

Положения, выносимые на защиту, обладают необходимой научной новизной, отражают авторскую позицию, имеют обоснование, хотя и вызывают ряд вопросов, изложенных ниже. Диссертация Р.Р. Аббуда имеет определенную теоретическую и практическую значимость, соответствующую уровню диссертацию на соискание степени кандидата юридических наук.

Заслуживает внимания и является ценным в теоретическом плане материал главы 1 дис., посвящённый международно-правовой

характеристике киберпреступлений. Автор делает ряд выводов, основанных на исследовании подходов к определению понятия «киберпреступление» (пар. 1), излагает результаты исследования подходов к классификации киберпреступлений (пар. 2), рассматривает киберпреступления в контексте международно-правового регулирования применения силы (пар. 3).

Новыми и значимыми для науки и практики являются отдельные результаты исследования международно-правового противодействия киберпреступлениям (глава 2 дис.). Подробное рассмотрение содержания международных соглашения в сфере противодействия киберпреступлениям (пар. 1), исследование практических аспектов международного расследования, реализации противодействия и гармонизации национального законодательства государств (пар. 2), обращение к некоторым правовым аспектам значения технологий искусственного интеллекта для сферы кибербезопасности, а также к вопросам юрисдикции, экстрадиции, ответственности государств (пар. 3) позволили автору сделать некоторые обобщения, сравнения, а также рекомендации по совершенствованию международно-правового регулирования в рассматриваемой сфере.

Надлежащий уровень апробации исследования подтверждается результатами его обсуждения на кафедре международного права Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный университет правосудия им. В.М. Лебедева», а также результатами выступлений автора на научных и научно-практических конференциях международного и всероссийского уровня. Основные результаты исследования отражены в опубликованных научных работах, в том числе, в рецензируемых научных изданиях. Опубликованные статьи диссертанта отражают основные положения диссертации. Автореферат в достаточной мере раскрывает содержание диссертации.

Содержание диссертационного исследования свидетельствует о том, что автор на достаточном уровне справился с поставленной целью и

основными задачами. Вместе с тем отдельные положения представленной диссертации нуждаются в дополнительном пояснении, а некоторые – носят весьма спорный характер и вызывают замечания. Кроме того, представляется уместным задать автору отдельные дополнительные вопросы. Основные вопросы и замечания, которые могут быть сформулированы по результатам ознакомления с работой Р.Р. Аббуда, состоят в следующем.

1. Нуждается в дополнительном пояснении авторское понимание содержания понятия киберпреступления. Учитывая, что автор делает существенный акцент на значимости определения данного понятия, к его выработке можно было бы подойти более обстоятельно.

1.1. В диссертации автор отстаивает позицию о трансграничности как неотъемлемой характеристики киберпреступлений.

В положении №1, выносимом на защиту, автор утверждает, что «Киберпреступление является преступлением, обладающее трансграничным характером – происходит на территории двух и более государств». Вопросы относительно трансграничности требуют комментария и в связи с включением данного признака в авторское определение киберпреступления (положение №2, выносимое на защиту). Обращает на себя внимание в связи с этим упоминание автором двух доктринальных подходов к определению содержания понятия киберпреступления в обосновании актуальности на стр. 6 дис.: ни узкое, ни широкое его понимание не включает обязательного признака трансграничности (см. также стр. 20 дис.).

Позиция о трансграничности – одна из главных идей диссертации, но диссертант прилагает недостаточно усилий для ее отстаивания. В ходе публичной защиты ее нужно обосновать и объяснить более основательно.

Не следует упрощать концепцию трансграничности и сводить ее к формуле «происходит на территории двух и более государств». Недостаточно убедительно в контексте киберпреступности и утверждение «трансграничность выражается в появлении иностранного элемента в правоотношениях» (положение №1, выносимое на защиту). Подобными

заявлениями тезис о трансграничности трудно обосновать. Почему не существует киберпреступлений, которые «не происходят на территории двух и более государств»? Почему не существует киберпреступлений, без «появления иностранного элемента»? Может ли считаться киберпреступлением деяние, которое характеризуется тем, что злоумышленник и жертва находятся в одной стране, а для совершения деяния используются локальные ИКТ-платформы или мессенджеры с серверами и иной инфраструктурой, расположенными в данном государстве?

На стр. 24–26 дис. содержится обзор зарубежных доктринальных позиций относительно понятия киберпреступления и делается вывод, что «Таким образом… данное деяние… носит экстерриториальный характер» (стр. 26). Вместе с тем, ни в одной из приведенных зарубежных позиций не упоминается «экстерриториальность» или отдельные ее признаки.

Такими методами диссертант не сможет убедить читателя.

Возможно, позиция Р. Аббуда гораздо глубже, чем кажется на первый взгляд. Автор исходит из того, что «информационное пространство не имеет определенных границ» (стр. 12 дис.), «киберпреступления не знают территориальных границ» (стр. 18 дис.) и т. д.; на стр. 30 дис. он заявляет, что «выработка четкого определения является необходимым фактором для дальнейшей квалификации данного рода правонарушений в сети “Интернет”». То есть гипотетически в представлении автора речь идет либо о некоей «внетерриториальности» киберпреступлений (что вряд ли состоятельно), либо о потенциальной или презюмируемой трансграничности, «заложенной» в самой цифровой среде, и имманентно присущей любому деянию с использованием Интернета.

В таком случае автору непременно нужно раскрыть в контексте содержания понятия «киберпреступление» свое представление о соотношении деяний, совершенных с использованием Интернета и других систем. Например, 15 сентября 2025 г. Председатель ЦИК РФ Э. Памфилова заявила о полной автономности системы «ГАС Выборы 2.0» и отсутствия ее

связи с Интернетом[1]. Может ли, по мнению Р.Р. Аббуда, неправомерное вмешательство в работу данной системы, имеющее все признаки внутреннего деяния (с точки зрения территории и всех иных характеристик), являться киберпреступлением? Имеет ли место какая-либо имманентная транснациональность, экстратерриториальность или «внетерриториальность» такого деяния?

Некоторые исследователи выделяют понятие «транснациональные киберпреступления», а также отмечают, что от 30 % до 70 % киберпреступлений обладают транснациональным характером[2]. Как автор относится к мнениям о том, что лишь некоторые (пусть даже большинство) киберпреступления носят транснациональный характер?

В итоге позицию об определении киберпреступления через признак трансграничности легче не отстаивать, чем отстаивать. Даже если автор считает трансграничность неотъемлемым признаком, нет веских оснований считать ее признаком определяющим. Данный признак не может оказать рационального влияния на правоприменение: автор рискует побудить правоприменителя разграничивать деяния, которые разграничивать не следует с учетом целей международного противодействия киберпреступности; это может привести к злоупотреблениям со стороны государств и снизить с таким трудом достигнутый уровень международного взаимодействия в данной сфере. А вот для обоснования значимости такого взаимодействия и совершенствования его форм вполне разумно рассуждать о трансграничности киберпреступлений или значительного их числа.

1.2. Авторский подход к определению понятия «киберпреступление» вызывает и иные вопросы. Например, почему такие преступления непременно представляют собой «несанкционированный доступ к информационно-коммуникационным технологиям» (положение №2,

---

[1] См.: Памфилова: интернет является «недружественной России паутиной» // Вести.ру. URL: https://www.vesti.ru/article/4687847 (дата обращения: 15.09.2025).

[2] См.: *Пучков Д. В.* Уголовно-правовая модель телекоммуникаций от преступных посягательств: проблемы теории и практики: дис. … канд. юрид. наук. Екатеринбург, 2022. С. 128.

выносимое на защиту; см. также представление автора об объективной стороне киберпреступления на стр. 28 дис.)? Почему нельзя считать киберпреступлениями деяния, совершенные «без несанкционированного доступа»? Например, совершается ли «кибербуллинг» в форме несанкционированного доступа? Еще один наглядный пример: предусмотренное ст. 16 Конвенции ООН против киберпреступности «распространение интимных изображений без согласия… с помощью информационно-коммуникационных систем» – это не обязательно киберпреступление? Оно вполне может быть совершено без какого-либо несанкционированного доступа к чему-либо. Может неслучайно незаконный/неправомерный доступ к соответствующим ресурсам – это лишь одно из целого ряда противоправных деяний, предусмотренных Будапештской конвенцией 2001 г. (ст. 2), упомянутой выше Конвенцией ООН (ст. 7), а также УК РФ (ст. 272)?

1.3. Возможно, теоретической и практической значимостью могло бы обладать авторское объяснение значимости «общепризнанного универсального определения киберпреступления». Проблеме определения уделено значительное внимание в диссертации (положение №1, выносимое на защиту; пар. 1 главы 1). Ни Будапештская конвенция 2001 г., ни Конвенция ООН против киберпреступности не содержат определения данного понятия. Если абстрагироваться от традиционной склонности отечественной правовой науки и законодательной практики к выработке определений, какие конкретные практические проблемы – реальные или гипотетические – порождает отсутствие определения? Может в результате какое-то конкретное деяние «выпадает» из сферы международного внимания к киберпреступности? Если это так, то каким образом авторское определение (будь оно нормативно или доктринально воспринято) позволяет преодолеть эти проблемы?

2. В части предложений о новых «видах киберпреступлений» (см. положение №3, выносимое на защиту; стр. 35–41 дис.) также возникает ряд вопросов.

2.1. На стр. 37 дис. отмечается: «кибербуллинг – это оскорбления в сети “Интернет” с использованием цифровых технологий». Некоторые специалисты наряду с оскорблениями выделают еще целый ряд форм кибербуллинга – домогательство, распространение слухов, использование фиктивного имени, публичное разглашение личной информации, угрозы и т.д.[3] Считает ли автор несостоятельными подобные представления?

2.2. На стр. 38 дис. автор пишет «к одному из современных видов киберпреступлений можно отнести дипфейки. Дипфейк – это генерация изображения или голоса, которая основана на ИИ». Далее описываются возможные общественно опасные способы использования данной технологии, но возникает вопрос: почему можно утверждать, что сама по себе «генерация изображения или голоса, которая основана на ИИ» преступна? Правильно ли назвать дипфейк киберпреступлением (см. положение №3, выносимое на защиту)?

2.3. Интересным будет услышать позицию автора о том, не охватываются ли отдельные новые «виды киберпреступлений» действием положений Конвенции ООН против киберпреступности:

«криптоджекинг» – действием статей 7, 9 и/или 13;

«вещевой кардинг» – действием, например, статьи 13?

3. В целом не вполне понятно отношение автора к Конвенции ООН против киберпреступности. Она упоминается в положении №7, выносимом на защиту, как «разработанная Россией» (кстати, на стр. 23 дис. утверждается иное; а как на самом деле?). Вместе с тем, в обосновании актуальности отмечается «потребность в необходимости выработки на международном уровне конвенции универсального характера» (стр. 7 дис.). В описании

[3] См., например: *Willard N.* An Educator’s Guide to Cyberbullying Cyberbullying and Cyberthreats. URL: https://www.scaet.org/csafety/cbcteducator.pdf (дата обращения: 15.09.2025).

практической значимости исследования предлагается использовать его результаты «в рамках разработки международного договора универсального характера под эгидой ООН» (стр. 16 дис.). Отсутствие «универсальной новой Конвенции» отмечается на стр. 30 дис. На стр. 166 дис. отмечается: «Принятие под эгидой ООН универсальной Конвенции в части регулирования киберпреступлений видится актуальным и необходимым».

Что имеет в виду автор: разработку и принятие еще одной конвенции ООН? Альтернативной той, что была принята в 2024 г. резолюцией Генеральной ассамблеи по инициативе России? Насколько позволяет судить об этом диссертация, Конвенция ООН против киберпреступности, по мнению автора, не решает проблем определения киберпреступления, кибербуллинга, дипфейка и некоторых других. Автор предлагает разработать конвенцию с точечным решением данных проблем? Насколько рациональна или перспективна такая идея, учитывая чувствительность этой сферы для поиска международного консенсуса?

Еще более затрудняет восприятие позиции автора его постоянное обращение к «проекту Конвенции ООН» (от 27 июля 2021 г.) (см. описание правовой основы исследования на стр. 10). При этом уже принятая Конвенция ООН против киберпреступности в правовую основу исследования не включена и не анализируется в диссертации, лишь упоминается. В параграфе 2 главы 1 автор вновь обращается к «проекту Конвенции ООН». Есть ощущение, что автор отождествляет эти два документа: в положении №7, выносимом на защиту, в абзаце о Конвенции ООН против киберпреступности отмечается, что «закрепляется цифровой суверенитет государств над своим информационным пространством»; на стр. 64 утверждается то же самое о «проекте Конвенции ООН». Уверен ли автор, что оба документа закрепляют цифровой суверенитет?

На стр. 23 дис. автор пишет: «для работы над проектом Конвенции ООН был учрежден ad hoc комитет». Это ведь другой проект Конвенции ООН – не «предложенный Россией»? На стр. 24 вновь идет речь о «проекте

Конвенции ООН» в контексте поддержки Россией и другими странами некоего «вышеназванного документа» (видимо, российского проекта). На стр. 61 дис. упоминается «Конвенция ООН», хотя, очевидно, речь идет о российском проекте. На стр. 83 дис. отмечается, что на данный момент ведется «субстантивная работа» над «проектом Конвенции ООН»: это действительно так в 2025 году?

Согласен ли автор со следующим утверждением: Конвенция ООН против киберпреступности, хотя и принята по инициативе, в том числе, России – это не принятый российский «проект Конвенции ООН» 2021 г., а совершенно другой акт? Вызывает сожаление, что автор не проанализировал в сравнительной перспективе эти документы.

Появляются и более общие вопросы.

Считает ли автор целесообразным для России подписать и ратифицировать Конвенцию ООН против киберпреступности, если она настолько несовершенна, что в диссертации предлагается разработать новый договор?

Если предложенный Россией в 2021 г. «проект Конвенции ООН» так хорош, как это оценивается на стр. 63–64 дис., стоит ли нашей стране продолжать продвигать данный проект?

Как три документа – 1) Конвенция ООН против киберпреступности, 2) российский «проект Конвенции ООН» 2021 г. (если он имеет перспективу) и 3) «универсальная новая Конвенция» (о необходимости выработки которой заявляет автор) – будут соотноситься друг с другом? Будут ли дополнять друг друга или взаимозаменять?

4. Автор относит кибератаку «направленную одним государством против другого… к акту применения силы, если данная кибератака нарушает цифровой суверенитет государств» (стр. 68 дис.). Что автор понимает под «цифровым суверенитетом» государства? Почему именно он должен быть нарушен в результате кибератаки, чтобы она составляла акт применения силы?

5. На стр. 73 дис. автор утверждает: «правовые механизмы противодействия киберпреступлениям предусмотрены преимущественно в многосторонних международных соглашениях регионального характера. По большей части эти региональные соглашения содержат нормы jus cogens и являются обязательными для исполнения». Как именно автор понимает термин *jus cogens*, и какие конкретные нормы *jus cogens* содержатся в указанных региональных соглашениях?

6. В положении № 6, выносимом на защиту, отмечается: «Сотрудничество через двусторонние международные договоры между государствами-участниками [ЕАЭС] оказалось малоэффективным, так как киберпреступления нарушают правопорядок более двух государств». В выводах параграфа 1 главы 2 на стр. 121 дис. отмечается «Сотрудничество через двусторонние международные договоры между государствами-участниками не работает». Эти тезисы нуждаются в подтверждении. В материале диссертации на стр. 97–99, где данные договоры упоминаются, какое-либо значимое подтверждение отсутствует.

7. Автор предлагает принять договор, посвященный противодействию киберпреступности, «под эгидой ЕАЭС» и учредить «международный правоохранительный орган в рамках ЕАЭС». Какие положения Договора о ЕАЭС 2014 г. могли бы выступать правовой основой для реализации подобных инициатив?

8. В параграфе 1 главы 2 делается вывод «Исходя из вышеизложенного, ни международные акты обязательного характера, ни международные акты рекомендательного характера, по сути, не играют особую роль в части противодействия преступлениям в сфере ИКТ» (стр. 123 дис.). Что это значит – «не играют особую роль»? Это негативная оценка эффективности инструментов? Какие методы автор использовал для оценки или на какие авторитетные источники полагается?

9. На стр. 123 дис. утверждается «В международном праве киберпреступления относят к преступлениям международного характера».

Далее на стр. 123–124 дис. приводятся позиции ведущих российских ученых о преступлениях международного характера, но не приводится ни одной позиции об отнесении «киберпреступлений к преступлениям международного характера». В итоге делается вывод «Исходя из вышеизложенного, в международном праве киберпреступление является преступлением международного характера». Эти тезисы требуют дополнительного подтверждения. Кто из российских или зарубежных ученых считает, что киберпреступления – это преступления международного характера (подчеркиваю: не «транснациональные киберпреступления», не какие-либо отдельные киберпреступления или категории киберпреступлений, а как таковые «киберпреступления»)? Поскольку данные вопросы связаны с возвращением к дискуссии о транснациональности, для ответа на них достаточно будет подтвердить тезис об отнесении киберпреступлений как собирательного понятия к категории преступлений международного характера ссылкой на любую авторитетную позицию. Аналогичные сомнения возникают в контексте заголовка пар. 3 главы 1 дис. – «Киберпреступление как новый вид международного преступления»: действительно ли автор считает киберпреступление международным преступлением?

10. Немало вопросов возникает в связи с предложениями автора использовать искусственный интеллект (ИИ) для борьбы с киберпреступностью. В диссертации ИИ рассматривается как возможное «средство международно-правовой борьбы», однако эта идея недостаточно ясно и корректно изложена. Материал соответствующей части параграфа 3 главы 2 гораздо «богаче», чем это представлено в положении №4, выносимом на защиту, и содержит ряд выводов, важных и интересных (хотя и не бесспорных) в контексте правовых аспектов взаимосвязи использования ИИ и борьбы с киберпреступлениями. В ходе публичной защиты автору рекомендуется сосредоточиться на международно-правовом измерении этой взаимосвязи, а заявления о противостоянии преступлениям «путем

разработки исходного кода» можно считать оправданным призывом к совершенствованию технических средств противодействия киберпреступности на разных уровнях – международном, национальном, корпоративном.

Содержание работы вызывает много вопросов, однако в поддержку автора можно высказать следующее. Тема достаточно широкая, непростая. Встречаются диссертации, к которым трудно подобрать вопросы и замечания с учетом их заурядности, отсутствия попыток высказать что-то новое, страха соискателя отстаивать свое мнение. Работа Р.Р. Аббуда – не из их числа: автор предлагает новое видение теоретических вопросов, вырабатывает конкретные практические решения, отстаивает собственное видение исследуемых проблем. Некоторые из высказанных замечаний и вопросов носят преимущественно дискуссионный характер, другие – направлены на поощрение автора к проведению дальнейших исследований по выбранной теме, отдельные недостатки можно считать устранимыми при условии представления обстоятельной аргументации в ходе публичной защиты.

В целом диссертационное исследование Р.Р. Аббуда представляет собой завершенную научно-квалификационную работу, в которой содержится решение новой научной задачи, имеющей значение для развития науки международного права. Работа написана автором самостоятельно, имеет теоретическую и практическую значимость, обладает внутренним единством, содержит новые научные результаты и положения, выдвигаемые для публичной защиты. Работа свидетельствует о личном вкладе Р.Р. Аббуда в науку. По своему содержанию рецензируемая диссертация соответствует научной специальности 5.1.5 Международно-правовые науки.

Вывод: диссертационное исследование Аббуда Руслана Ратебовича на тему «Международно-правовое регулирование противодействия киберпреступлениям» соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата юридических наук в соответствии с Положением о присуждении ученых степеней, утвержденным

постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842 «О порядке присуждения ученых степеней» (в текущей редакции), а его автор – Аббуд Руслан Ратебович – заслуживает присуждения ученой степени кандидата юридических наук по специальности 5.1.5 Международно-правовые науки.

Отзыв подготовлен заведующим кафедрой международного права, кандидатом юридических наук, доцентом Д.В. Красиковым, обсужден и одобрен на заседании кафедры международного права федерального государственного бюджетного образовательного учреждения высшего образования «Саратовская государственная юридическая академия» (протокол № 2 от 16 сентября 2025 г.).

Заведующий кафедрой международного права
федерального государственного бюджетного
образовательного учреждения
высшего образования
«Саратовская государственная
юридическая академия»,
кандидат юридических наук, доцент **Д.В. Красиков**

16 сентября 2025 г.

Сведения о ведущей организации:
федеральное государственное бюджетное образовательное учреждение высшего образования «Саратовская государственная юридическая академия».
Почтовый адрес: 410056 г. Саратов, ул. Чернышевского Н.Г., зд. 104, стр. 3.
Тел.: +7 (8452) 299-202;
адрес электронной почты: rector@ssla.ru;
официальный сайт: http://сгюа.рф.

Информация о кафедре международного права федерального государственного бюджетного образовательного учреждения высшего образования «Саратовская государственная юридическая академия»:
почтовый адрес: 410028 г. Саратов, ул. Вольская, дом 16;
тел.: +7 (8452) 299-142;
адрес электронной почты: k_intlaw@ssla.ru;
адрес страницы кафедры в сети Интернет: http://сгюа.рф/dep-europe-law/history.

Подпись Красикова Д.В.
УДОСТОВЕРЯЮ
Начальник управления кадрового и документационного обеспечения федерального государственного бюджетного образовательного учреждения высшего образования Саратовская государственная юридическая академия
М.А. Вагорова

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
УПРАВЛЕНИЕ КАДРОВОГО И ДОКУМЕНТАЦИОННОГО ОБЕСПЕЧЕНИЯ