ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 05.2.001.03, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ДИПЛОМАТИЧЕСКАЯ АКАДЕМИЯ МИНИСТЕРСТВА ИНОСТРАННЫХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ» ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 24 октября 2025 г. № 14

О присуждении Аббуду Руслану Ратебовичу, гражданину Российской Федерации, ученой степени кандидата юридических наук

Диссертация «Международно-правовое регулирование противодействия киберпреступлениям» по специальности 5.1.5. – Международно-правовые науки принята к защите 24 марта 2025 г., протокол № 11, диссертационным советом 05.2.001.03, созданным на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Дипломатическая академия Министерства иностранных дел Российской Федерации» (ведомственная принадлежность: Министерство иностранных дел Российской Федерации; адрес: 119021, г. Москва, Остоженка 53/2, строение 1) на основании Приказа Министерства науки и высшего образования Российской Федерации от 5 октября 2023 г. № 1883/нк. Приказом Минобрнауки России от 2 июля 2025 г. № 667/нк в состав диссертационного совета включен д.ю.н., доцент, профессор кафедры международного права Дипломатической академии МИД России Д.В. Галушко.

Соискатель **Аббуд Руслан Ратебович**, 18 декабря 1992 г. рождения, в 2015 году окончил специалитет Федерального государственного бюджетного образовательного учреждения высшего образования «Московский

государственный университет имени М. В. Ломоносова» по специальности «Юриспруденция», присвоена квалификация «Юрист». В 2022 году окончил аспирантуру Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный университет правосудия» по направлению подготовки «Юриспруденция», присвоена квалификация «Исследователь. Преподаватель-исследователь».

Диссертация выполнена на кафедре международного права Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный университет правосудия имени В.М. Лебедева».

Научный руководитель – доктор юридических наук, профессор, заведующий кафедрой международного права Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный университет правосудия имени В.М. Лебедева», **Нешатаева Татьяна Николаевна.**

Официальные оппоненты:

Русинова Вера Николаевна, доктор юридических наук, профессор, руководитель Департамента международного права факультета права ФГАОУ ВО «Национальный исследовательский университет «Высшая школа экономики»;

Скуратова Александра Юрьевна, кандидат юридических наук, доцент, доцент кафедры международного права ФГАОУ ВО «Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации»,

дали положительные отзывы на диссертацию.

Ведущая организация, **Федеральное государственное бюджетное образовательное учреждение высшего образования «Саратовская государственная юридическая академия»,** в своем положительном отзыве, подписанном заведующим кафедрой международного права, кандидатом юридических наук, доцентом Красиковым Д.В., и утвержденном проректором по научной работе, доктором юридических наук, профессором Белоусовым С.А.,

указала, что диссертация Аббуда Руслана Ратебовича на тему «Международно-правовое регулирование противодействия киберпреступлениям» представляет собой законченное исследование на актуальную тему, результаты которого имеют теоретическое и практическое значение, свидетельствующее о решении важной научной и практической задачи для развития международного права. Работа соответствует критериям, которым должны отвечать диссертации на соискание ученой степени кандидата юридических наук, изложенным в п. 9-10 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842 (ред. от 16.10.2024, с изм. и доп., вступ. в силу с 01.01.2025), а ее автор, Аббуд Руслан Ратебович, заслуживает присуждения ученой степени кандидата юридических наук по специальности 5.1.5. – Международно-правовые науки.

Соискатель имеет 10 опубликованных по теме диссертации работ, в том числе в рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации – 6.

Общий объем публикаций по теме диссертации составляет 6,4 п.л., из них личный вклад соискателя составляет 6,4 п.л. В число публикаций по теме диссертации входят 6 статей в научных журналах, а также тезисы 2 докладов в материалах по итогам международных научных конференций.

К числу основных работ по теме диссертации относятся следующие:

1. Аббуд Р.Р. Киберхалифат: новый неисследованный субъект в международном информационном пространстве // Электронное сетевое издание «Международный правовой курьер». – 2017. - № 1. – С. 61-65. (0,6 п.л.)

2. Аббуд Р.Р. Киберхалифат: нормативное определение и криминологическая характеристика в национальном и международном информационном праве // Вопросы российского и международного права. – 2018. - Том 8 № 8А. – С. 190-197. (1 п.л.)

3. Аббуд Р.Р. Актуальные вопросы международного права в части преступлений в сфере компьютерной информации // Евразийский юридический

журнал. – 2021. - № 2 (153). – С. 43-44. (0,4 п.л.)

4. Аббуд Р.Р. Трансформация форм киберпреступности в условиях пандемии COVID-19 // Юридическая Наука. – 2022. - № 7. – С. 126-129. (0,5 п.л.)

5. Аббуд Р.Р. Международно-правовое регулирование борьбы с киберпреступлениями // Российское правосудие. – 2023. - № 4. – С. 24-30. (0,8 п.л.)

6. Аббуд Р.Р. Международно-правовая классификация новых киберпреступлений // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и Право. – 2024. - № 8. – С. 121-124. (0,5 п.л.)

На диссертацию поступили отзывы:

– **ведущей организации, Федерального государственного бюджетного образовательного учреждения высшего образования «Саратовская государственная юридическая академия»**. Отзыв положительный, имеющий следующие замечания:

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 20» и отсутствия ее связи с Интернетом. 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. 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, 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. 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 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;

– официального оппонента доктора юридических наук, профессора **Русиновой Веры Николаевны.** Отзыв положительный, замечания следующие:

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 Oatada) 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 обо 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;

– официального оппонента **Скуратовой Александры Юрьевны,** кандидата юридических наук, доцента. Отзыв положительный, замечания следующие:

1. В положении № 3, выносимом на защиту, соискателем указывается, что «классификация киберпреступлений, содержащаяся в действующих международных соглашениях, теряет актуальность», в связи с чем предлагается выделить дополнительную (авторскую) классификацию. Однако возникает вопрос, насколько в целом целесообразна классификация преступлений в международных соглашениях? На доктринальном уровне, безусловно, такой подход возможен, и соискатель вполне может предложить свой взгляд на этот вопрос, но насколько необходима «классификация киберпреступлений» на нормативном уровне? В региональных актах, регулирующих сотрудничество государств по противодействию преступлениям в сфере ИКТ, приведен подробный перечень противоправных деяний, подлежащих криминализации, без опоры на

классификацию. Кроме того, в действующих региональных договорах закреплены положения, предусматривающие внесения изменений и дополнений (с учетом динамики преступных угроз в сфере ИКТ) в виде отдельных Протоколов, что предполагает эволюцию данной области регулирования. Будет ли классификация киберпреступлений в международных договорах усиливать эффективность борьбы? Если да, то каким образом? И в какой именно международный договор, по мнению диссертанта, необходимо внести авторские предложения по новым видам преступных деяний в сфере ИКТ? Второй вопрос – выделение, как предложено соискателем, такого отдельного вида киберпреступлений, как, например, «вещевой кардинг». Является ли это преступление по своему характеру чем-то иным, чем уже предусмотренный нормативными актами такой состав, как хищение или мошенничество с использованием информационно-компьютерных технологий?

2. Вывод соискателя в положении № 5, выносимом на защиту, о том, что противоречивые положения национального законодательства приводят к невозможности успешного противодействия преступлениям в сфере ИКТ, выглядит спорным. Даже до принятия универсальной Конвенции под эгидой ООН на региональном уровне уже давно реализуется успешное сотрудничество правоохранительных органов государств в борьбе с преступными угрозами в сфере ИКТ. Пример – взаимодействие в рамках Совета Европы (на основе Конвенции 2001 г.), обусловившее гармонизацию и унификацию законодательства государств, создание специализированных подразделений, предметно занимающихся вопросами борьбы с преступлениями в сфере ИКТ. Иной пример – вполне результативное сотрудничество в рамках Евросоюза (в том числе посредством Европола). Под эгидой ОДКБ на постоянной основе проводится операция «ПРОКСИ», в рамках которой сотрудники силовых ведомств, специальных служб и правоохранительных органов, профильных министерств и ведомств государств – членов Организации сотрудничают в борьбе преступлениям в сфере ИКТ.В отношении универсального уровня правоохранительного сотрудничества можно указать на взаимодействие государств в рамках Интерпола, значимая часть деятельности которого нацелена именно на борьбу с преступлениями в сфере ИКТ

(в том числе посредством созданного под эгидой Интерпола отдельного центра по таким преступлениям в Сингапуре - INTERPOL Global Complex for Innovation). Таким образом, различные правовые системы не являются препятствием к межгосударственному взаимодействию, тезис соискателя о невозможности сотрудничества государств опровергается практикой.

3. Не совсем убедительно, на наш взгляд, выглядит тезис соискателя о целесообразности принятия договора под эгидой ЕАЭС для целей борьбы с киберпреступлениями, равно как и о создании специально правоохранительного органа в рамках ЕАЭС. Любая организация создается с вполне конкретными целями, имеет свою компетенцию; деятельность ЕАЭС ограничена экономическими аспектами (создание условий для развития экономик государств-членов, повышение уровня жизни населения, стремление к формированию единого рынка товаров, услуг, капитала), не связана с борьбой с преступностью. Насколько целесообразно наделять ЕАЭС – организацию в экономической сфере – данным направлением сотрудничества (при всей его актуальности) и создавать в ее рамках отдельную правоохранительную структуру, при том, что члены ЕАЭС не находятся вне правового поля, уже являются сторонами соглашений в области борьбы с преступлениями в рамках ИКТ, активно взаимодействуют в этом направлении.

4. В положении, выносимом на защиту № 7, сделан вывод о целесообразности создания международной правоохранительной организации универсального характера, наделенной компетенцией в части осуществления международной оперативно-розыскной деятельности в целях борьбы с киберпреступлениями. Однако насколько оправданно создавать новую организацию – при том, что все перечисленные соискателем задачи уже осуществляются под эгидой Интерпола? Основную задачу по расследованию выполняют компетентные органы государств и взаимодействие по линии Интерпола (действующего с 1956 г. наряду с адаптацией к новым вызовам и угрозам, коими являются преступления в сфере ИКТ) уже налажено, отработано и доказывает свою эффективность. Есть ли смысл в дублировании структур?

5. Вывод соискателя о том, что киберпреступление является международным

преступлением в увязке с идеей о потенциальном создании специального трибунала ad hoc по международным киберпреступлениям требует определенной конкретизации. Киберпреступления, по его мнению, являются собирательным понятием (отсюда и попытка классифицировать, уточнить их перечень), и международными они становятся в силу того, что приобретают трансграничный характер. В этом случае есть основания их квалифицировать как преступления международного характера, что соискатель и делает. Однако далее в тексте диссертации на определенном этапе происходит «переход» киберпреступлений в другую категорию – международных преступлений, т.е. деяний, стоящих в одном ряду с агрессией, геноцидом, военными преступлениями. Хотелось бы, чтобы в процессе защиты соискатель уточнил, относится ли киберпреступления к категории международных, которые предполагают возможность осуществления международной уголовной юрисдикции? Если да, то какое именно из нормативно закрепленного перечня преступлений? Или же в данном случае термин «кибер» будет означать средство, с помощью которого может быть осуществлено преступление, например агрессия, и в этом случае отдельного, нового состава международного преступления нет? При таком подходе более понятным становится тезис, что новым киберпреступлением стала, например, реабилитация нацизма (с. 33). Учитывая, что выводы соискателя в данном аспекте противоречивы, было бы уместно прояснить позицию; отметим, что МУС в подготовленном Офисом Прокурора в 2025 г. Проекте политики Суда в отношении киберпреступлений в соответствии с Римским статутом (и потенциальном распространении на них юрисдикции МУС) высказался по данному вопросу вполне определенно.

На автореферат поступили отзывы:

– **Глотовой Светланы Владимировны,** доцента кафедры международного права юридического факультета ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», кандидата юридических наук. Отзыв положительный, содержит следующее замечание.

1. Следует обратить внимание на некоторую неточность. Диссертант указывает, что «в современном мире положения правовых норм, противоречащих друг другу, приводят к коллизиям национальных законов, и как следствие, к невозможности их регулирующего действия на территории разных государств, так и реализаций наказаний за их нарушение» (вывод 5, стр. 11). В связи с изложенным делается вывод о механизме сближения национальных правовых систем посредством международных договоров. Полагаем, что коллизий между национальным законодательством различных государств не может существовать в силу принципа суверенного равенства, самостоятельности при построении собственной национальной правовой системы. Видится, что в указанном случае речь корректнее вести о разнообразных национальных законодательных подходах к регулированию противодействия киберпреступлениям.

2. Также диссертант предлагает развивать сотрудничество в части противодействия киберпреступлениям в рамках Евразийского экономического союза (далее – ЕАЭС). В частности, отмечается, что «видится необходимым принятие договора под эгидой ЕАЭС, который сможет обеспечить безопасность информационного пространства путем обмена информацией, взаимной помощью в части расследования киберпреступлений, а также запросах о выдаче преступников» (вывод 6, стр.12). Необходимо отметить, что сотрудничество в рассматриваемой области осуществляется в рамках Содружества Независимых Государств, о чем упоминает автор, отмечая, в том числе, что «в рамках СНГ существует многостороннее соглашение в части противодействия преступлениям в сфере информационных технологий. Кроме того, в рамках данной международной организации функционирует Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств - участников СНГ» (стр. 21). В связи с изложенным представляется перспективным определить особенности и уникальные механизмы регулирования противодействия киберпреступлениям в рамках ЕАЭС по сравнению с подходами, которые сложились в рамках СНГ.

– **Пузыревой Юлии Владимировны,** кандидата юридических наук, ученый секретарь диссертационного совета 03.2.006.01 Московского университета МВД России имени В.Я. Кикотя. Отзыв положительный, содержит следующие замечания. *Во-первых*, в первом положении, выносимом на защиту, диссертант утверждает, что киберпреступление носит трансграничный характер, проявляющийся в том, что такие противоправные деяния не ограничены территориальными границами одного государства и в них возможно появление иностранного элемента (С. 9). Вместе с тем, в п. 2 ст. 3 Конвенции ООН против транснациональной организованной преступности 2000 г. определены базовые признаки преступлений транснационального характера. В ходе публичной защиты хотелось бы уточнить у диссертанта о том, как соотносятся его авторские критерии «трансграничности» киберпреступлений с выработанными конвенционными признаками, позволяющими квалифицировать те или иные преступные деяния как «транснациональные». *Во-вторых*, во втором положении, выносимом на защиту, автор отмечает, что международных соглашения» отсутствует общепризнанное универсальное определение «киберпреступления», что связано с несогласованностью терминологии в международных документах (С. 9-10). Хотелось бы уточнить целесообразность закрепления в международно-правовых актах единого определения данного термина, выступающего собирательным и родовым понятием для конкретных преступных деяний, так или иначе связанных с ИКТ-средой и непосредственно самим ИКТ, криминализация которых через детальную характеристику и закрепляемый специальный состав будет обеспечивать повышение эффективности и результативности предупреждения киберпреступности и борьбы с ней, а также позволит укрепить международное сотрудничество в предупреждении киберпреступности и борьбе с ней. Свою точку зрения диссертант может обосновать в ходе публичной защиты. *В-третьих*, в § 1.3. диссертант рассуждает о возможности квалификации киберпреступлений как нового вида международных преступлений с последующем развитием идеи о необходимости создания специального трибунала ad hoc по международным

киберпреступлениям в целях осуществления эффективного международного уголовного правосудия (С. 17-
18). Исходя из такого новаторского и весьма дискуссионного авторского подхода, речь скорее всего идет о потенциально-новом органе международной уголовной юстиции (ОМУЮ) и о перспективах развития системы ОМУЮ. Учитывая, что в практике международного права выработаны и апробированы
определенные модели учреждения и функционирования ОМУЮ, требует уточнения авторское предложение о международно-правовых механизмах создания специального трибунала ad hoc по международным киберпреступениям;

- **Козловой Татьяны Сергеевны,** кандидата юридических наук, директора Департамента по корпоративному управлению и документационному обеспечению Некоммерческой организации «Фонд развития Центра разработки и коммерциализации новых технологий» (Фонд «Сколково»). Отзыв положительный, замечаний не содержит;

- **Мысливского Павла Петровича**, кандидата юридических наук, советника судьи Суда Евразийского экономического союза. Отзыв положительный, замечаний не содержит.

- **Колосова Александра Викторовича,** кандидата юридических наук, доцента кафедры международного права и сравнительного правоведения Юридического института ФГБОУ ВО «Иркутский государственный университет». Отзыв положительный, содержит следующие замечания: в автореферате указывается на возможность квалификации киберпреступления как акта агрессии. Какими критериями, по мнению диссертанта, следует руководствоваться международному сообществу для разграничения «акта применения силы» и «акта агрессии» в цифровом пространстве;

Все отзывы на диссертацию и автореферат положительные, в них сделан вывод о том, что работа соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата юридических наук, закрепленным в Положении о присуждении ученых степеней, утвержденном Постановлением Правительства Российской Федерации от 24.09.2013 № 842 (ред.

от 16.10.2024, с изм. и доп., вступ. в силу с 01.01.2025), а ее автор, Аббуд Руслан Ратебович, заслуживает присуждения ученой степени кандидата юридических наук по специальности 5.1.5. – Международно-правовые науки.

Выбор официальных оппонентов обосновывается их высоким профессиональным уровнем, специализацией и сферой научных интересов, соответствующих теме и профилю представленного на защиту диссертационного исследования. В частности, В.Н. Русинова является ведущим учёным-правоведом в области международного права, в сферу интересов которого входят такие важнейшие аспекты диссертационного исследования Р.Р. Аббуда, как международное уголовное право, право международной безопасности, права человека, право мирного разрешения международных споров. А.Ю. Скуратова является специалистом в области международного права, исследуя, в частности, международно-правовые аспекты сотрудничества государств по борьбе с преступностью, международное уголовное правосудие.

Компетентность официальных оппонентов в соответствующей отрасли науки подтверждается, прежде всего, следующими публикациями:

Русинова В.Н., Сушков С.П. Вменение государству использования информационно-коммуникационных технологий // Журнал зарубежного законодательства и сравнительного правоведения. – 2024. Т. 20. - № 5. – С. 74-84; Русинова В.Н. Международно-правовая квалификация вредоносного использования информационно-коммуникационных технологий: в поисках консенсуса// Московский журнал международного права. – 2022. - № 1. – С. 38-51; Русинова В.Н., Ассаф А.Н., Мошников Д.К. Спор о суверенитете в киберпространстве: содержание, пределы и перспективы развития позитивистского дискурса // Международное правосудие. – 2020. - № 3. С. 55-66; Капустин А. Я., Русинова В. Н., Шинкарецкая Г. Г., Касенова М. Б. Проблемы международного сотрудничества в области применения добровольных, необязательных норм ответственного поведения государств в ИКТ-среде и предложения по их решению // В кн. : Международная безопасность в среде информационно-коммуникационных технологий. / Под общ. ред.: А. А. Стрельцов, А. Я.

Капустин, Т. А. Полякова, А. С. Марков, Б. Н. Мирошников. М.: Национальная Ассоциация международной информационной безопасности, – 2023. Гл. 2. С. 26-36; Стрельцов А. А., Капустин А. Я., Полякова Т. А., Шинкарецкая Г. Г., Русинова В. Н. Международная безопасность в среде информационно-коммуникационных технологий / Под общ. ред.: А. А. Стрельцов, А. Я. Капустин, Т. А. Полякова, А. С. Марков, Б. Н. Мирошников. М.: Национальная Ассоциация международной информационной безопасности, – 2023. Гл. 2. – С. 26-36; Скуратова А.Ю. Обязательство «aut dedere, aut judicare»: современные проблемы международно-правового содержания // Международное уголовное право и международная юстиция. – 2020. - № 2. – С. 3-7; Скуратова А.Ю. Принцип ex post facto в международном уголовном праве: соблюдать нельзя нарушить? // Международное уголовное право и международная юстиция. – 2024. - № 3. – С. 2-7; Скуратова А.Ю. Актуальные проблемы реализации принципа ne bis in idem в международном уголовном праве // Право и управление. XXI век. – 2024. - № 2. – С. 29-44; Скуратова А.Ю. Особенности содержания и применения принципа законности в международном уголовном праве // Российский юридический журнал. – 2024. - № 1. – С. 7-24; Вылегжанин А.Н., Лобанов С.А., Скуратова А.Ю. Международно-правовые основания противодействия преступлениям, посягающим на безопасность стационарных платформ в акваториях Российской Федерации // Всероссийский криминологический журнал. – 2020. - № 2 (14). – С. 313-326; Синякин И.И., Скуратова А.Ю. Специальный трибунал по Ливану и прогрессивное развитие международного уголовного права // Правоприменение. – 2021. - № 4 (5). – С. 226-236; Вереина Л.В., Синякин И.И., Скуратова А.Ю. Критерии идентификации обязательств erga omnes // Государство и право. – 2023. - № 9. – С. 180-188.

Выбор ведущей организации, Федерального государственного бюджетного образовательного учреждения высшего образования «Саратовская государственная юридическая академия», обосновывается тем, что базе сложилась одна из ведущих российских научных школ в области международного права, в рамках деятельности которой осуществляются научные исследования по

актуальным проблемам международного уголовного права, международного уголовного правосудия, цифрового права, международно-правовых аспектов сотрудничества государств по борьбе с преступностью, являющимся предметом диссертационного исследования, что подтверждается следующими публикациями сотрудников кафедры по теме диссертации:

Красиков Д. В. Развитие концепции цифрового суверенитета в правовой политике Европейского Союза // Бизнес. Образование. Право. – 2021. - № 4 (57). – С. 255-259; Липкина Н. Н. Принципы установления экстратерриториальной юрисдикции государств в киберпространстве в контексте правовых позиций Европейского Суда по Правам Человека // Правовая политика и правовая жизнь. – 2021. - № 2. – С. 153-160; Красиков Д. В. Влияние Пандемии COVID-19 на политико-правовое восприятие принципа суверенитета в киберпространстве // Вестник Саратовской государственной юридической академии. – 2021. - № 6 (143). – С. 57-63; Липкина Н. Н. Определение параметров реализации принципа государственного суверенитета в киберпространстве в контексте принципа свободы усмотрения // Бизнес. Образование. Право. – 2021. - № 4 (57). – С. 232-235; Красиков Д. В. Применимость международного права к поведению государств в киберпространстве: проблемы достижения консенсуса // Вестник Саратовской государственной юридической академии. – 2020. - № 6 (137). – С. 86-95; Красиков Д. В., Липкина Н. Н. Принцип территориального суверенитета и концепция делимитации юрисдикции государств в киберпространстве: монография. – Саратов: ИЦ «Наука», 2021. – 153 с; Красиков Д. В. Проблемы использования технологий искусственного интеллекта для разрешения международных споров // Право, цифровые технологии и искусственный интеллект: сборник статей. Сер. «Правоведение». М.: ИНИОН РАН, 2021. С. 171–185; Красиков Д.В. Проблемы реализации суверенитета государств киберпространстве в условиях повышения рисков в связи с распространением новой коронавирусной инфекции (COVID-19) // Защита общественных интересов в эпоху глобальных вызовов и трансформаций: международно-правовое, международное частноправовое и сравнительно-правоведческое измерение:

Сборник по материалам Международной научно-практической конференции в рамках Саратовского международного юридического форума, посвященного 90-летию Саратовской государственной юридической академии / под ред. Д.В. Красикова, Н.Н. Липкиной. – Саратов: Изд-во СГЮА, 2021 – С. 9–11; Красиков Д. В. Проблемы трансграничной территориальности в праве интеллектуальной собственности в эпоху Интернета // Право будущего: интеллектуальная собственность, инновации, интернет: Ежегодник. сер. «Правоведение» Ин-т науч. информ. по обществ. наукам РАН, Центр. соц. науч.-информ. исслед., предпринимательского права МГУ им. М.В. Ломоносова; отв. ред. Афанасьева Е.Г. – М.: ИНИОН РАН, 2020 – 138–144.

Диссертация отвечает критериям, установленным п.п. 9-10 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842 (ред. от 16.10.2024, с изм. и доп., вступ. в силу с 01.01.2025).

В диссертации отсутствуют недостоверные сведения об опубликованных соискателем ученой степени работах, в которых изложены основные научные результаты исследования.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- **выявлено** отсутствие в международных соглашениях общепризнанного универсального определения киберпреступления, что связано с несогласованностью терминологии в международных документах, а также с отсутствием в доктринах единого понятия киберпреступления, в связи с чем диссертантом предлагается авторское определение данного понятия;

- **доказано**, что киберпреступление является преступлением, обладающее трансграничным характером – происходит на территории двух и более государств;

- **аргументировано**, что в настоящий момент, учитывая стремительное развитие технологий в эпоху цифровизации, классификация киберпреступлений, содержащаяся в действующих международных соглашениях, не является исчерпывающей, в связи с чем автором предлагается выделить дополнительную

классификация киберпреступлений;

- **установлено**, что средством борьбы с киберпреступлениями может выступить ИИ, в связи с чем автором предлагается противостоять киберпреступлениям при помощи ИИ путем разработки исходного кода внутреннего инструмента специального программного обеспечения, посредством которого разработчики систем ИИ смогут находить риски и тем самым выявлять проблемы кибербезопасности;

- **выявлено**, что современная множественность национальных правовых систем свидетельствует о невозможности координации регулирования противодействия киберпреступлениям на национальном уровне;

- **обосновано**, что сближение национальных правовых систем в части криминализации во внутреннем законодательстве деяний, совершенных с использованием компьютерных технологий, а также включения в национальный уголовный процесс норм о процессуальных действиях, специфических для расследования и судебного разбирательства по делам о киберпреступлениях осуществимо через международные договоры универсального и регионального характера;

- **установлено**, что на сегодняшний день в рамках Евразийского экономического союза отсутствует многостороннее соглашение в части противодействия киберпреступлениям;

- **обоснована** необходимость принятия договора под эгидой ЕАЭС, который сможет обеспечить безопасность информационного пространства путем обмена информацией, взаимной помощью в части расследования киберпреступлений, а также запросах о выдаче преступников;

- **доказано**, что принятие на универсальном уровне международного соглашения, регламентирующего усовершенствованные формы сотрудничества и усиление превентивных мер в части оказания противодействия киберпреступлениям, является актуальным;

- **аргументирована** важность создания в будущем международной правоохранительной организации универсального характера, наделенной

компетенцией в части осуществления международной оперативно-розыскной деятельности в целях выявления, пресечения или раскрытия наиболее тяжких киберпреступлений, а также международных расследований на досудебных стадиях уголовного судопроизводства;

- **установлено**, что экстрадиция по-прежнему остается одним из традиционных механизмов сотрудничества в части борьбы с киберпреступлениями;

- **обосновано**, что если государство по каким-либо причинам отказывается в выдаче, то оно обязано само осуществить правосудие.

Теоретическая значимость исследования заключается в том, что оно имеет фундаментальный характер для науки международного права, поскольку является первым в отечественной юридической науке комплексным исследованием, в котором осуществлен анализ регулирования противодействия киберпреступлениям с точки зрения международного публичного права. В исследовании автором сформулировано понятие, выявлены характеристики, а также определена новая классификация киберпреступлений, не содержащаяся в международных договорах. Проанализированы институциональные и договорные формы сотрудничества между государствами в целях противодействия киберпреступлениям и аргументирована позиция в отношении того, какие акты (*hard law vs soft law*) являются наиболее эффективными в части регулирования данной проблемы.

Предложенные выводы выступают полезным источником для дальнейших исследований и разработки эффективных международно-правовых механизмов, соответствующих современным реалиям, вносят вклад в научные разработки в области международного права.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

– полученные выводы могут выступить в качестве методологического и практического материала в процессе дальнейшего развития международно-

правового регулирования противодействия киберпреступлениям, в том числе в рамках переговорных процессов по исследуемой тематике;

– предложения, сформулированные в результате исследования, могут служить рекомендательной базой или концептуальной основой для совершенствования международной, а также внутригосударственной правотворческой деятельности и правоприменительной практики;

– научные результаты и выработанные рекомендации могут быть могут быть применены правоохранительными органами Российской Федерации в части уголовного преследования за совершение киберпреступлений. Более того, результаты проведенного исследования могут быть использованы в рамках разработки международного договора на глобальном, региональном, многостороннем и двустороннем уровнях в части сотрудничества Российской Федерации с иностранными государствами по вопросам противодействия киберпреступлениям;

– разработанные положения способствуют совершенствованию международно-правового регулирования сотрудничества в области противодействия киберпреступлениям, а также могут быть использования в преподавательской деятельности, при подготовке учебных пособий и чтении учебных курсов по международно-правовым наукам в профильных образовательных организациях высшего образования;

– результаты исследования внедрены в учебный процесс при разработке рабочих программ, учебно-методической документации, при чтении лекций и проведении семинарских занятий на юридическом факультете ФГБОУ ВО «Российский государственный университет правосудия имени В.М. Лебедева», что подтверждается соответствующими справками и актом о внедрении.

Достоверность и объективность настоящей работы подтверждается:

– применением соответствующих объекту и предмету исследования общенаучных (анализ, синтез, обобщение, аналогия, индуктивный и дедуктивный методы, диалектический и системный метод, формально-логический метод) и специализированных методов (историко-правовой метод,

сравнительно-правовой метод, формально-юридический метод и метод интерпретации) юридической науки;

– привлечением широкой нормативно-правовой базы, значительного количества российских и зарубежных научных трудов и специальной литературы, информационно-аналитических материалов, способствующим в своей совокупности комплексному и объективному изучению различных аспектов темы диссертации.

Научная новизна диссертации определяется тем, что диссертантом в комплексном виде осуществлен сравнительно-правовой анализ международных соглашений, регулирующих отношения государств в области противодействия киберпреступлениям. При изучении сущности киберпреступления в диссертационном исследовании были не только выявлены характеристики данного противоправного деяния, но и сформулировано автором исследования его понятие, а также определена новая классификация киберпреступлений, не содержащаяся в международных договорах. В исследовании проанализированы институциональные и договорные формы сотрудничества между государствами в целях противодействия киберпреступлениям и аргументирована позиция в отношении того, какие акты (*hard law vs soft law*) являются наиболее эффективными в части регулирования данной проблемы. Доказано, что нормы мягкого права, носящие рекомендательный характер, являются наиболее приоритетными, и содержатся в специальных источниках - актах органов международных организаций, стандартах, регламентах, рекомендациях, кодексах, инструкциях, разработанных в целях регулирования киберпреступлений, а также обеспечения кибербезопасности. Более того, исследование содержит анализ систем искусственного интеллекта (ИИ), что позволило прийти к выводу о том, что посредством установления специального алгоритма, ИИ способен обеспечить надлежащую киберзащиту.

Научная новизна исследования заключается, помимо прочего, в предложенных автором практических и теоретических рекомендациях в целях

содействия прогрессивному развитию международного права и его кодификации в исследуемой области.

Теоретические и практические рекомендации в совокупности с положениями, выносимыми на защиту, отражают **личный вклад** автора в науку международного права. Он также выражается в оригинальном подходе к обработке, интерпретации и анализу значительного объема источниковедческой базы, включающей разноплановые научные и нормативные документы, что позволило существенно расширить научное представление по исследуемой проблематике.

В диссертационном исследовании соблюден принцип внутреннего единства, работа отличается концептуальной целостностью, что проявляется в четко выстроенной структуре, согласованной методологической базе и логичной связности полученных результатов.

Работа содержит теоретические положения, разработанные на основе исследований соискателя, которые имеют существенное значение для развития науки международного права и в своей совокупности способствовали проведению комплексного исследования международно-правового регулирования противодействия киберпреступлениям. Внедрение со стороны профильных ведомств и их подразделений научно обоснованных автором идей может содействовать прогрессивному развитию международного права и его кодификации в исследуемой области, а также совершенствованию международно-правового регулирования противодействия киберпреступлениям.

Диссертация является оригинальным, законченным, самостоятельно проведенным исследованием, в котором отсутствуют заимствованные материалы без ссылок на авторов и источники заимствования.

Диссертационный совет пришел к выводу, что диссертация представляет собой научно-квалификационную работу, которая соответствует требованиям Положения о присуждении ученых степеней, утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842 (ред. от 16.10.2024, с изм. и доп., вступ. в силу с 01.01.2025).

На заседании 24 октября 2025 г. диссертационный совет принял решение присудить Аббуду Руслану Ратебовичу ученую степень кандидата юридических наук.

При проведении тайного голосования диссертационный совет в количестве 9 человек, из них 8 докторов юридических наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 12 человек, входящих в состав совета, проголосовали: за – 9, против – 0, недействительных бюллетеней – 0.

Председатель
диссертационного совета Данельян Андрей Андреевич

Ученый секретарь
диссертационного совета Комендантов Сергей Васильевич

27 октября 2025 г.

Подлинность руки
удостоверяю
Начальник отдела
документационного обеспечения
Дипломатической академии МИД России