В диссертационный совет 24.2.320.07,
созданный на базе федерального
государственного бюджетного образовательного
учреждения высшего образования
«Кубанский государственный университет»
350000, г. Краснодар, ул. Октябрьская, 25,
каб. 203

ОТЗЫВ

официального оппонента на диссертацию Лихачева Никиты Александровича на тему «Уголовно-правовое противодействие преступлениям в сфере обеспечения информационной безопасности: законодательный, правоприменительный и доктринальный аспекты», представленную на соискание ученой степени кандидата юридических наук по специальности 5.1.4. Уголовно-правовые науки (юридические науки)

Диссертация Н.А. Лихачева выполнена на максимально актуальную в нынешних криминологических условиях тему. Растущие масштабы информатизации общества и цифровизации социальных процессов неминуемо привели к проникновению криминальных угроз в информационно-телекоммуникационное пространство. В начале третьего десятилетия XXI века в России сложилась такая ситуация, в которой вся преступная деятельность, которая в принципе допускает возможность применения сети Интернет для подготовки или совершения общественно опасных деяний, вторглась в информационно-телекоммуникационное пространство.

По итогу 2023 года в России было зарегистрировано 676 951 преступление, совершенное с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, удельный вес таких деяний в структуре преступности составил 34,8%. В 2024 году рост «цифровых» преступлений продолжился. По итогу первого квартала текущего года было совершено 179 228 деяний, что на 17,6% превышает показатель, зафиксированный в аналогичном периоде прошлого года. Доля преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в общем объеме зарегистрированных преступлений составила 37,9%.

Согласно сведениям, представленным Центральным банком РФ в «Обзоре операций, совершенных без согласия клиентов финансовых организаций», в 2023 году объем операций без согласия клиентов увеличился по сравнению с 2022 годом на 11,5% на фоне роста объема денежных переводов с использованием карт (+10,5%, до 136,38 трлн руб.). Кредитные организации возвратили клиентам всего 8,7% от всего объема операций по переводу денежных средств, совершенных без согласия клиентов.

Современная ситуация дает основания утверждать, что любой государственный орган или частная организация, которые так или иначе сталкиваются к проблемой совершения преступлений в сфере

информационно-телекоммуникационных технологий, отмечают неблагоприятные тенденции в указанной сфере. К сожалению, деятельность субъектов профилактики ощутимого эффекта не приносит. Закономерным следствием этого стала необходимость модернизации средств противодействия преступности, основным из которых является уголовное законодательство.

Масштабы и сложность проблемы осознаются руководством страны и правоохранительных органов. Выступая на расширенном заседании коллегии МВД России 2 апреля 2024 года, Президент России В.В. Путин констатировал, что в 2023 году «почти на 30 процентов выросло число преступлений с использованием информационных технологий. Их совершено порядка 680 тысяч, а ущерб превысил 156 миллиардов рублей. Нужно серьёзно совершенствовать механизмы борьбы с правонарушениями в этой сфере, работать на опережение». В свою очередь, Министр внутренних дел Российской Федерации В.А. Колокольцев отметил, что «реализуются меры, направленные на повышение эффективности борьбы с киберпреступностью. Необходимо отметить, что значительная угроза исходит из-за рубежа, прежде всего с территории Украины. В прошлом году с учётом положений законодательства заработали механизмы противодействия сокрытию или подмене номера абонента. Осуществлены оргштатные мероприятия. Общее количество сотрудников, задействованных на данной линии, за прошедший год возросло на 15 процентов, в основном за счёт формирования на местах оперативных подразделений по борьбе с противоправным использованием информационно-коммуникационных технологий».

Несмотря на предпринимаемые шаги, вопросы противодействия преступности, связанной с применением информационных технологий, в том числе и уголовно-правовыми средствами, сохраняют свою социальную значимость. Все указанные обстоятельства убедительно подтверждают высокую актуальность темы диссертации Н.А. Лихачева. Любые попытки совершенствования механизма уголовно-правовой охраны информационной безопасности в настоящее время соответствуют насущным потребностям уголовно-правовой науки, а также важны для практики противодействия преступности.

В основу работы положен широкий круг нормативных и теоретических источников. Содержание диссертации показывает, что она основывается на обширном фундаменте многочисленных исследований отечественных и зарубежных ученых в области теории государства и права, информационного права, уголовного права, криминологии, уголовно-процессуального права, теории национальной безопасности, международного права и международного уголовного права. При подготовке работы был использован практически весь объем актуальных уголовно-правовых научных трудов, затрагивающих проблемы противодействия преступным посягательствам на информационную безопасность.

Автором корректно и точно определены объект, предмет, цель и задачи диссертационного исследования.

Нельзя не отметить качественную методологическую основу работы, которая была обеспечена комплексным применением общенаучных и частнонаучных методов: всеобщего диалектического метода научного познания изучаемых социально-правовых явлений, а также системного, формально-логического, структурно-функционального, формально-юридического, сравнительно-правового, исторического, социологического, статистического и метода аналогии. Умелое комбинирование названных методов позволило Н.А. Лихачеву обеспечить теоретико-практическую обоснованность, объективность, достоверность результатов, способствовало всесторонней разработке уголовно-правовых проблем противодействия преступлениям в сфере обеспечения информационной безопасности.

Работа отличается обширной эмпирической базой. В качестве источников научной информации были использованы статистические данные ГИАЦ МВД России за период 2018–2023 гг., определения Конституционного Суда РФ, постановления Пленума Верховного Суда РФ, 207 приговоров по уголовным делам о преступлениях, так или иначе связанных с негативным воздействием на информационную безопасность, вынесенных судами г. Москвы, г. Екатеринбурга, Республики Крым, г. Краснодара, г. Красноярска, Нижегородской области и др. Автором было проведено анкетирование по различным проблемам исследования 138 практических работников – 56 федеральных судей и 82 следователей МВД России и Следственного комитета России.

Оппонируемая работа обладает несомненной научной новизной, что подтверждается авторскими результатами. Соискателю удалось получить значительный объем качественно нового научного знания, дополняющего и развивающего теоретические основы уголовно-правового противодействия посягательствам на информационную безопасность, и разработать на этой основе пути совершенствования отдельных направлений уголовно-правовой политики в указанной сфере.

Научную новизну диссертационного исследования убедительно подтверждают следующие конкретные результаты:

предложено доктринальное определение информации как объекта уголовно-правовой охраны;

сформирован комплекс действий, направленных на обеспечение информационной безопасности уголовно-правовыми средствами, который может быть положен в основу совершенствования уголовно-правовой политики в исследуемой сфере;

обоснован новый подход к классификации деяний, посягающих на информационную безопасность, в основу которого положено то обстоятельство, что информация может рассматриваться не только как предмет противоправного посягательства, но и способна выступать признаком объективной стороны;

внесены предложения по внедрению в отечественную систему уголовно-правовой охраны информационной безопасности передового зарубежного опыта;

сформулирован ряд важных дефиниций, в числе которых «кибератака», «информационная война», «киберпространство», «информационное

пространство» и др., которые как дополняют уголовно-правовую доктрину, так и имеют перспективу отражения в уголовном законодательстве;

обоснован вывод о том, что киберпространство в настоящее время приобретает все более осязаемые черты криминальной среды со своей контркультурой, а также отличительными, присущими только ему признаками, что в перспективе дает возможность определять его как новую форму реальности, а следовательно, – место совершения преступления;

сформирован комплекс доктринальных положений и основанных на них законотворческих предложений, направленных на совершенствование норм действующего уголовного законодательства, в частности, статей 272 – 274^1 УК РФ.

Научную новизну диссертационного исследования, решение поставленных задач убедительно подтверждает и содержание основных положений, выносимых на защиту.

Диссертация Н.А. Лихачева обладает несомненной теоретической значимостью. Полученные соискателем результаты вносят существенный вклад в развитие уголовного права, расширяя научные представления о механизме уголовно-правового обеспечения информационной безопасности. Материалы исследования могут послужить основой для дальнейших научных изысканий в области познания феномена преступлений, посягающих на информационную безопасность, и разработки уголовно-правовых средств, охраняющих соответствующие общественные отношения.

Следует отметить и высокую практическую значимость диссертационного исследования. Полученные автором результаты могут быть успешно использованы в законотворческом процессе при совершенствовании уголовного законодательства, регламентирующего ответственность за посягательства на информационную безопасность. Разработанный Н.А. Лихачевым терминологический аппарат и авторские рекомендации по квалификации преступлений, посягающих на информационную безопасность, могут использоваться в правоприменительной деятельности, а также при формировании правовых позиций Верховного Суда РФ для обеспечения единообразной следственно-судебной практики. Материалы диссертации могут использоваться в учебном процессе образовательных организаций при преподавании дисциплин уголовно-правового профиля. Также их целесообразно применять в рамках повышения квалификации действующих сотрудников правоохранительных органов и судей, что позволит сформировать у них компетенции, необходимые для верной квалификации незаконных действий, посягающих на информационную безопасность.

Избранные автором методологическая, теоретическая и нормативная основы исследования, эмпирическая база, применение широкого объема источников получения научной информации подтверждают высокую степень обоснованности и достоверности результатов диссертационного исследования. Автором были строго соблюдены требования методологии уголовно-правовой науки, применены апробированные общенаучные и частнонаучные методы познания. Основные результаты диссертационного исследования докладывались и обсуждались на международных и

всероссийских научно-практических конференциях. По теме диссертации автором опубликовано 7 научных статей, 4 из которых – в изданиях, рекомендованных ВАК при Минобрнауки России. Автореферат и опубликованные по теме диссертации работы отражают ее основное содержание.

Диссертация имеет стройную и логически выверенную структуру, состоит из введения, трех глав, объединяющих двенадцать параграфов, заключения, списка используемых источников и приложений.

Во введении автор обосновывает актуальность темы, характеризует степень ее научной разработанности, определяет объект, предмет, цель и задачи исследования, описывает методологическую, теоретическую, нормативную и эмпирическую основы, раскрывает его научную новизну, теоретическую и практическую значимость, оценивает степень достоверности полученных результатов, описывает их апробацию, формулирует основные положения, выносимые на защиту.

Первая глава диссертации структурно разделена на четыре параграфа и содержит описание общетеоретических, уголовно-правовых и сравнительно-правовых аспектов обеспечения информационной безопасности. В первом параграфе первой главы Н.А. Лихачев проводит исторический анализ возникновения дефиниции «информация», появления и развития теории информации и системы информационной безопасности, их места и значения в федеральном, в том числе уголовном законодательстве. Результатом этой части исследования является авторская дефиниция информации, а также описание комплекса действий, направленных на обеспечение информационной безопасности уголовно-правовыми средствами. Второй параграф первой главы посвящен анализу подходов к определению преступлений в сфере информационной безопасности, разграничению понятия «компьютерные преступления» с иными сходными терминами. Разработана авторская классификация преступлений, посягающих на информационную безопасность. В третьем параграфе первой главы автор анализирует проблемы международно-правового обеспечения информационной безопасности уголовно-правовыми средствами. Констатируется отсутствие унифицированной системы международного уголовно-правового обеспечения информационной безопасности, обозначаются перспективы ее будущей архитектуры. Четвертый параграф первой главы посвящен анализу уголовно-правовой практики противодействия преступлениям, направленным против информационной безопасности, в зарубежных государствах. На основе такого анализа автор оценивает перспективы рецепции зарубежных уголовно-правовых норм в УК РФ.

Во второй главе диссертации, состоящей из трех параграфов, автор оценивает состояние и перспективы современной уголовно-правовой политики России в сфере обеспечения информационной безопасности. В первом параграфе второй главы Н.А. Лихачев анализирует развитие процесса регламентации уголовно-правовой охраны информационных отношений, криминализации соответствующих деяний, уголовно-правовое регулирование

киберпространства, специфику преступлений, направленных против информационной безопасности, оценивает перспективы уголовно-правовой оценки деятельности по реализации программ, созданных с использованием технологий искусственного интеллекта, определяет уголовно-правовой статус киберпространства и информационного пространства. Второй параграф второй главы посвящен рассмотрению специфики современной киберпреступности. Предлагается авторское доктринальное определение кибератаки и оцениваются перспективы закрепления определения и характеристик информационной войны в теории уголовного права. В третьем параграфе второй главы автор исследует составы преступлений, содержащие криминообразующий или квалифицирующий признак в виде использования информационно-телекоммуникационных сетей (включая сеть «Интернет»). Соискатель приходит к выводу о целесообразности расширения перечня обстоятельств, отягчающих наказание, за счет включения аналогичного обстоятельства.

В третьей главе диссертации, включающей в себя пять параграфов, подробно рассмотрена уголовно-правовая характеристика посягательств на безопасность компьютерной информации (статей 272–274^2 УК РФ). Каждый из параграфов включает характеристику объективных и субъективных признаков отдельных составов преступлений, закрепленных в главе 28 УК РФ. Н.А. Лихачев оценивает достоинства и недостатки конструкции составов преступлений, анализирует судебную практику их применения, приводит теоретические позиции ученых. В результате предлагаются корректировки статей в виде изменения признаков основных составов преступлений, модернизации и дополнения квалифицирующих признаков, включения в статьи примечаний, разъясняющих содержание отдельных дефиниций.

В заключении автор последовательно и содержательно формулирует общие итоги исследования, основные выводы и положения.

Работа включает два приложения. В первом приложении представлены предлагаемые автором редакции статей 272–274^1 УК РФ. Во втором приложении содержатся обобщенные результаты анкетирования судей и следователей по различным вопросам, касающимся исследуемой темы.

Принимая во внимание актуальность темы диссертации, высокий уровень ее научной новизны, несомненную теоретическую и практическую значимость полученных результатов, можно заключить, что Н.А. Лихачев достиг поставленной цели и полностью решил задачи исследования.

Положительно оценивая диссертационное исследование, следует отметить, что в работе присутствуют выводы и суждения, способные вызвать критические замечания, стать предметом научной дискуссии и требующие пояснений в ходе публичной защиты.

1. В положении №9, выносимом на защиту, автор утверждает, что сравнительно-правовое исследование положений зарубежного уголовного законодательства привело его к выводу о перспективности заимствования опыта ФРГ по криминализации противоправной записи непубличных разговоров с последующей передачей ее третьим лицам, особенно если указанные действия повлекли за собой наступление тяжких последствий, а

также распространения сведений, полученных преступным путем. Там же указано, что «представляет интерес использование “мошенничества” как признака, характеризующего способ совершения преступления: получение доступа к охраняемой законом информации посредством обмана и злоупотребления доверием».

На стр. 88-89 указано, что «с необходимостью криминализации записи непубличных разговоров с последующей передачей ее третьим лицам, если указанные действия повлекли за собой наступление тяжких последствий, распространения компьютерной информации, полученной преступным путем, получения доступа к охраняемой законом информации посредством обмана и злоупотребления доверием согласилось большинство (76%) опрошенных следователей МВД России, СК РФ, судей федеральных судов общей юрисдикции». Действительно, в приложении 2 содержится информация о доле положительно ответивших на этот вопрос. Однако подобное авторское решение вызывает ряд критических замечаний:

– вопрос №10 анкеты составлен с методической ошибкой. Фактически респондентов спрашивали о необходимости криминализации одновременно трех самостоятельных действий. Выразить свое согласие либо несогласие с необходимостью криминализации только одного или двух из них опрошенные специалисты не могли;

– не подвергнут анализу опыт применения предлагаемых к рецепции норм зарубежного законодательства, до конца не ясно значение используемых там терминов («непубличные разговоры», «третьи лица», «тяжкие последствия»);

– ни одно из предлагаемых для криминализации деяний не получило воплощения в виде конкретных уголовно-правовых норм.

2. В действующей редакции ч. 3 ст. 274^1 УК РФ установлена ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации. В положении №10, выносимом на защиту, приложении 1 к диссертации, а также на стр. 181-182 работы Н.А. Лихачев предлагает свою редакцию ст. 274^1 УК РФ, в которую названное деяние по каким-то причинам не вошло. Никаких аргументов в пользу необходимости его декриминализации в работе нет, фактически действующая часть 3 из предлагаемой автором редакции статьи 274^1 УК РФ просто-напросто пропала.

3. Нельзя в полной мере поддержать авторское определение кибератаки, отраженное в положении №7, выносимом на защиту, как «виновно совершаемых противоправных общественно опасных деяний по массовому

воздействию на компьютеры, компьютерные сети и системы, их блокированию, повреждению, уничтожению, получению удаленного доступа к ним в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроз совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями». Тем более, что Н.А. Лихачев говорит перспективах дальнейшей криминализации подобного деяния. Дело в том, что в предлагаемом автором определении отчетливо прослеживаются террористические цели – дестабилизация деятельности органов власти или международных организаций либо воздействия на принятие ими решений. Такая же формулировка цели преступления нашла отражение в ст. 205 УК РФ. Сущность кибератаки в привычном лексическом значении этого слова гораздо шире – это любое противоправное воздействие на информационную систему с целью повредить её, получить или ограничить доступ к ней, собрать конфиденциальные данные. Схожее определение, например, содержится в англоязычной Википедии. Сам же автор на стр. 117 отмечает, что «в большинстве случаев кибератаки совершаются частными лицами, напрямую не связанными ни с органами государственной власти, ни со службами специального назначения». Представляется, что даваемое Н.А. Лихачевым определение больше подходит под термин «кибертерроризм», тем более, что на стр. 79 диссертации приводится позиция Д. Дэннинга, согласно которой «кибертерроризм – это осуществление противозаконных компьютерных атак на государственные информационные системы для запугивания или понуждения правительства или общества к совершению определенных действий и достижения преступных целей политического или социального характера». Перенос террористических целей на все без исключения кибератаки приведет к еще большей терминологической неопределенности.

4. Критические замечания и вопросы, требующие пояснений в ходе публичной защиты, вызывает содержание и технико-юридическое воплощение предложенных автором диссертации квалифицирующих признаков в статьях 272, 273, 274, 274^1 УК РФ:

– в частях 3 статей 272 и 273 УК РФ предложено установить квалифицирующий признак в виде совершения деяния с трансграничной передачей компьютерной информации, содержащей персональные данные, и (или) трансграничным перемещением носителей, содержащих такие данные. Единственным обоснованием этого предложения являются результаты экспертного опроса, который, правда, касался только ст. 272 УК РФ. На стр. 151 диссертации указано, что такое решение «видится обоснованным». По сути это единственный аргумент автора. Почему трансграничное перемещение именно персональных данных или носителей, содержащих такие данные, а не, например, сведений, составляющих государственную тайну, должно влечь более строгое наказание? Не повлечет ли такое законодательное решение усиление рисков объективного вменения из-за незнания преступником мест локализации облачных серверов, на которые копируются данные?

– каким образом возможно осуществить неправомерный доступ к охраняемой законом компьютерной информации и последующее ознакомление с ней (ч. 1 ст. 272 УК РФ) да еще и так, чтобы это деяние сопровождалось трансграничной передачей компьютерной информации, содержащей персональные данные, и (или) трансграничным перемещением носителей, содержащих такие данные, для наступления ответственности по ч. 3 ст. 272 УК РФ? Как трансграничное перемещение компьютерной информации может стать следствием ознакомления с ней?

– не ясно чем вызвана необходимость помещения в разные части статей 272, 273, 274, 274^1 УК РФ квалифицирующих признаков в виде совершения преступления группой лиц по предварительному сговору и организованной группой. Обоснования этого авторского решения в работе нет;

– в действующих ч. 4 ст. 272, ч. 3 ст. 273, ч. 2 ст. 274 УК РФ усиление ответственности происходит при наступлении тяжких последствий или в случае создания угрозы их наступления. В предлагаемых автором ч. 4 ст. 272 УК РФ и ч. 4 ст. 273 УК РФ ответственность усиливается только в случае фактического наступления тяжких последствий, про угрозу их наступления не сказано ничего. Обоснования такого авторского решения в работе нет;

– в предлагаемых автором п. «а» ч. 2 ст. 274 УК РФ и п. «а» ч. 3 ст. 274^1 УК РФ в качестве общественно опасных последствий, влекущих усиление ответственности, указано прекращение работы предприятия на срок более суток, в п. «а» ч. 3 ст. 274 УК РФ и п. «а» ч. 4 ст. 274^1 УК РФ – прекращение работы предприятия на срок более недели. Из работы не ясно, почему автор выбрал именно такие сроки прекращения работы предприятий для конструирования квалифицирующих и особо квалифицирующих признаков. Почему, например, не последовать православным традициям и не указать в качестве квалифицирующих и особо квалифицирующих признаков прекращение работы предприятий на срок девять дней и сорок дней соответственно?

Наконец, столь кардинальное изменение основных составов преступлений, предусмотренных статьями 272, 273, 274, 274^1 УК РФ, и их квалифицирующих признаков, пробуждает интерес к авторскому видению границ пенализации предлагаемых норм. Как наказания по различным частям предлагаемых редакций статей будут соотноситься с действующими санкциями соответствующих норм?

5. Нельзя согласиться с авторской трактовкой термина «распространение» применительно к объективной стороне ст. 273 УК РФ (стр. 165). Н.А. Лихачев под распространением вредоносных компьютерных программ предлагает понимать «их умышленную передачу, продажу, предоставление в пользование, дарение неограниченному кругу лиц». Между тем уголовно-правовая доктрина, как и правоприменительная практика, к распространению вредоносных компьютерных программ относят предоставление их хотя бы одному конкретному лицу. Неограниченность круга потенциальных получателей программы не обязательна для квалификации деяния по ст. 273 УК РФ. Об этом говорит и пункт 11 Постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О

некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"», согласно которому распространение вредоносных компьютерных программ или иной вредоносной компьютерной информации состоит в предоставлении доступа к ним конкретным лицам или неопределенному кругу лиц любым способом, включая продажу, рассылку, передачу копии на электронном носителе либо с использованием сети «Интернет», размещение на серверах, предназначенных для удаленного обмена файлами.

6. Автор предлагает включить в диспозицию ст. 273 УК РФ дополнительный функциональный признак вредоносной компьютерной программы – «осуществление слежения за компьютерным устройством». Также предлагается дополнить аналогичными признаками ч. 1 и ч. 2 ст. 274^1 УК РФ, установив ответственность за создание, приобретение, распространение и (или) использование компьютерной программы либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для … **отслеживания информации, содержащейся в ней** *… (выделено мной – В.С.)*, а также неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ с целью … **отслеживания информации, содержащейся в ней** *(выделено мной – В.С.)*. В связи с этим возникает вопрос, что же автор предлагает понимать под слежением за компьютерным устройством и отслеживанием информации, содержащейся в критической информационной инфраструктуре Российской Федерации? Как соотносится предлагаемое автором понятие «ознакомление с информацией» с понятием «отслеживание информации»?

Вместе с тем указанные замечания имеют во многом частный и дискуссионный характер, не ставят под сомнение, безусловно, высокую научную состоятельность, актуальность, новизну диссертации, обоснованность и достоверность сформулированных выводов и положений.

Диссертация Лихачева Никиты Александровича «Уголовно-правовое противодействие преступлениям в сфере обеспечения информационной безопасности: законодательный, правоприменительный и доктринальный аспекты» является научно-квалификационной работой, в которой содержится решение научной задачи, имеющей значение для науки уголовного права, представляет собой актуальное самостоятельное научное исследование, которое имеет завершенный вид, основано на качественной эмпирической базе, что обеспечивает его достоверность; содержащиеся в нем выводы и предложения обоснованы, обладают научной новизной, теоретической и практической значимостью.

Оппонируемая диссертация в полной мере соответствует критериям, установленным пп. 9 – 14 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842, а ее автор – Лихачев Никита Александрович – заслуживает присуждения искомой ученой степени кандидата юридических наук по научной специальности 5.1.4. Уголовно-правовые науки (юридические науки).

Официальный оппонент:
начальник кафедры уголовного права и криминологии
Краснодарского университета МВД России
кандидат юридических наук,
доцент Соловьев Владислав Сергеевич

3 июня 2024 г.

Подпись Соловьева В.С.
ПОДТВЕРЖДАЮ
Начальник отдела кадров

Сведения об официальном оппоненте:
Соловьев Владислав Сергеевич – кандидат юридических наук (диссертация защищена по научной специальности 12.00.08 – уголовное право и криминология; уголовно-исполнительное право), доцент по научной специальности 5.1.4. Уголовно-правовые науки (юридические науки); начальник кафедры уголовного права и криминологии Краснодарского университета МВД России.

Сведения о месте работы:
Наименование организации: Федеральное государственное казенное образовательное учреждение высшего образования «Краснодарский университет Министерства внутренних дел Российской Федерации».
Сокращенные наименования: Краснодарский университет МВД России, КрУ МВД России.
Почтовый адрес: Российская Федерация, 350005, Краснодарский край, г. Краснодар, ул. Ярославская, д. 128.
Адрес официального сайта в сети Интернет: https://крду.мвд.рф
Адрес электронной почты: post_krdu@mvd.ru
Телефон: 8 (861) 258-47-08.

С отзывом ознакомлен Соловьев В.С. 05.06.2024г.