«УТВЕРЖДАЮ»
Проректор по научной работе ДВФУ
_____ В.А. Нелюб
«_____» _____ 2024 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ
федерального государственного автономного образовательного учреждения высшего образования «Дальневосточный федеральный университет» (ДВФУ) на диссертационную работу Лихачева Никиты Александровича по теме: «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

Актуальность темы диссертационного исследования обусловлена существенными изменениями, происходящими в общественных отношениях, вызванными цифровизацией всех аспектов жизни российского общества. Поэтому уголовно-правовое противодействие преступлениям в сфере обеспечения информационной безопасности становится все более востребованным и требует своего дальнейшего анализа и развития.

Обосновывая актуальность темы диссертационного исследования, автор указывает, что любые передовые технологии практически сразу начинают использоваться в преступной деятельности. Статистические показатели совершаемых уголовно-правовых деликтов в сфере информационных и компьютерных технологий стали расти, а законодательство и правоохранительные органы зачастую не успевают реагировать на стремительно меняющуюся структуру общественных отношений. Очевидно, что информационная безопасность в ближайшее время станет одним из важнейших объектов уголовно-правовой охраны. Коммуникационная

индустрия стремительно развивается, ее доля в общественных процессах, в экономике и социальной жизни занимает ключевую роль.

Научная новизна диссертационного исследования Н.А. Лихачева заключается в том, что автором впервые с учетом дополнений, внесенных в УК РФ Федеральным законом от 14 июля 2022 г. № 260-ФЗ, осуществлено комплексное исследование преступлений в сфере обеспечения информационной безопасности и защиты информации. Проведенная систематизация преступлений, в рамках которых информация рассматривается не только как предмет противоправного посягательства, но и может выступать признаком объективной стороны, привела к обоснованию нового подхода к классификации исследуемых деяний, формированию определения информации как предмета информационных отношений, выступающих объектом уголовно-правовой охраны.

В своем исследовании диссертант определяет направления дальнейшей криминализации соответствующих деяний, позволяющее выявить наиболее уязвимую и незащищенную сферу правового регулирования в исследуемой области, определить специфические особенности новых составов преступлений: экстерриториальность, широкий, практически неограниченный круг потерпевших, самораспространяемость и изменчивость, крайне высокий уровень латентности.

Также достаточно новым является обоснованный автором тезис о том, что киберпространство может рассматриваться как место совершения преступления. Сравнительно-правовое исследование позволило диссертанту сформировать положения, представляющие интерес для возможной последующей имплементации в отечественное законодательство.

Результаты проведенного исследования позволили выработать комплекс как доктринальных положений, так и основанных на них законотворческих предложений, направленных на совершенствование норм действующего уголовного законодательства и правоприменительной практики в соответствующей их части.

Анализ проведенного Н.А. Лихачевым исследования позволяет сделать вывод о том, что автор достиг намеченной цели и решил поставленные задачи. Диссертант интересно и творчески подходит к решению сложных теоретических проблем исследуемой темы, по-новому рассматривает некоторые традиционные и устоявшиеся положения криминологической и уголовно-правовой доктрины применительно к предмету исследования.

Теоретическая значимость диссертационного исследования. Представленная диссертационная работа направленна на разрешение одной из актуальных проблем построения современного информационного общества – уголовно-правовое противодействие преступлениям в сфере обеспечения информационной безопасности.

Основные положения диссертационного исследования позволят расширить теоретические знания, касающиеся проблем уголовно-правового обеспечения информационной безопасности. Работа вносит определенный вклад в развитие доктрины уголовного права в соответствующей ее части. Сформулированные автором идеи и положения могут послужить катализатором развития и прогресса уголовно-правовой науки, они подготавливают почву для дальнейших исследований в указанной области научного познания.

Практическая значимость диссертационного исследования Н.А. Лихачева подтверждается возможностью использования полученных результатов, выводов и предложений, содержащихся в работе, для повышения квалификации сотрудников правоохранительных органов, специализирующихся на профилактике, расследовании и раскрытии преступлений и иных противоправных посягательств в сфере информационной безопасности.

Предложения нормотворческого характера и обоснованная автором правовая модель построения уголовно-правовых норм, содержащихся в Главе 28 УК РФ, могут быть использованы в процессе дальнейшего совершенствования уголовного законодательства, регламентирующего

ответственность за посягательства на информационную безопасность, а разработанный автором терминологический аппарат и рекомендации по квалификации указанных преступлений – в правоприменительной деятельности, а также при формировании правовых позиций Верховного Суда РФ.

Диссертация имеет необходимую и достаточную эмпирическую, теоретическую и нормативную основы. *Эмпирическую базу* исследования составляют: статистические данные, подготовленные ГИАЦ МВД РФ за период 2018–2023 гг.; определения Конституционного Суда РФ; постановления Пленума Верховного Суда РФ; приговоры, вынесенные по уголовным делам о преступлениях, так или иначе связанных с негативным воздействием на информационную безопасность (Симоновского районного суда г. Москвы, Кировского районного суда г. Екатеринбурга, Судакского городского суда Республики Крым, Ленинского районного суда г. Краснодара, Бабушкинского районного суда г. Москвы, Свердловского и Кировского районных судов г. Красноярска, Саровского городского суда Нижегородской области и др., всего изучено 207 приговоров); обобщенные результаты проведенного автором анкетирования 138 практических работников – 56 федеральных судей и 82 следователя.

Нормативная база исследования представлена Конституцией Российской Федерации, нормами международного и отечественного уголовного права, рядом федеральных конституционных законов, федеральных законов, указов Президента РФ, постановлений Правительства РФ, корреспондирующими нормами уголовного законодательства некоторых зарубежных стран – Белоруссии, Германии, Казахстана, Китая, Киргизии, Молдавии, США, Таджикистана, Туркменистана, Узбекистана.

Результаты исследования прошли необходимую апробацию на международных, всероссийских и региональных научных и научно-практических конференциях, круглых столах, проведенных автором учебных занятиях. Основные положения диссертационного исследования нашли

отражение в 7 научных работах, в числе которых 4 статьи в рецензируемых научных изданиях, включенных в перечень ВАК при Министерстве науки и высшего образования РФ.

Структура и содержание диссертационного исследования отвечают заявленной теме и концептуальным подходам автора к изучению обозначенной в диссертации проблематики. Работа состоит из введения, трех глав, двенадцати параграфов, заключения, списка использованных источников, приложения.

Во введении обоснована актуальность и степень разработанности темы, цели и задачи исследования, методологическая и теоретическая основа, нормативная и эмпирическая база, научная новизна диссертационного исследования и положения, выносимые на защиту.

Первая глава посвящена анализу общетеоретических, уголовно-правовых и сравнительно-правовых аспектов обеспечения информационной безопасности.

В первом параграфе первой главы дается анализ истории возникновения дефиниции «информация», появления и развития теории информации и системы информационной безопасности, их места и значения в федеральном, в том числе уголовном, законодательстве.

Проанализировав различные мнения и подходы к пониманию информации и информационной безопасности, соискатель резюмирует отсутствие доктринального единства научных позиций.

При этом автор постулирует, что информация рассматривается и как объект информационных отношений, и как объект передачи данных, однако требует конкретизации соответствующего понятия, встречающегося в различных интерпретациях более чем в 18 кодексах российского права. Автор предлагает следующее доктринальное определение информации – это подлежащие уголовно-правовой охране сведения конфиденциального характера, содержащие персональные данные или относящиеся к любой разновидности тайны, порядок допуска к которым, в том числе ознакомление

с ними, их распространение, копирование, изменение, уничтожение, а также порядок и форма хранения, подлежит императивному правовому регулированию, нарушение которого влечет уголовную ответственность (с. 43).

Второй параграф первой главы посвящен анализу уголовно-правового обеспечения информационной безопасности в Российской Федерации.

Исследовав российское законодательство в сфере обеспечения информационной безопасности, автор приходит к обоснованному выводу, что правовое регулирование информационной сферы – это комплексная сложная и многоаспектная задача, представляющая собой синергию различных отраслей науки. При решении правовых коллизий, восполнении пробелов в уголовном законодательстве следует учитывать научные достижения и опыт информологии, журналистики, лингвистики, психологии, программирования, информатики, физики, политологии. Однако, прежде всего, приоритетной задачей на краткосрочную перспективу должно стать формирование устойчивого понятийно-категориального аппарата как для ряда статей УК РФ, так и для федерального законодательства, непосредственно направленного на обеспечение информационной безопасности государства.

Третий параграф первой главы посвящен анализу проблем международно-правового обеспечения информационной безопасности.

В работе выявлено отсутствие унифицированной системы международного уголовно-правового обеспечения информационной безопасности, отмечена тенденция на его сегментирование и регионализацию, что продиктовано политико-экономическими причинами поляризации современных международных отношений.

Диссертант аргументированно обосновывает, что в настоящее время на международном уровне происходит активное формирование будущей архитектуры правового обеспечения информационной безопасности. Уголовно-правовые аспекты в данном случае играют ключевую роль, так как количество информационных операций и кибератак растет в геометрической

прогрессии, они становятся более разнонаправленными, и их классификация усложняется. Отсутствие единого международного договора, определяющего кибератаки, механизм уголовно-правовой борьбы с ними, позволяет их использовать в качестве инструмента политического воздействия.

Вторая глава диссертационного исследования посвящена анализу современной уголовно-правовой политики России в сфере обеспечения информационной безопасности.

В первом параграфе второй главы проводится исследование развития процесса уголовно-правовой регламентации охраны информационных отношений, криминализации соответствующих деяний, уголовно-правовых аспектов регулирования киберпространства, специфики преступлений, направленных против информационной безопасности.

Диссертант приходит к обоснованному выводу, что анализ современного уровня уголовно-правовой охраны информационных отношений позволяет констатировать наличие тенденции модернизации уголовного закона в связи с появлением качественно новых общественных отношений и их информатизацией, формированием системы защиты информации, построением информационно-коммуникационной инфраструктуры.

Автор отмечает разрозненность норм, направленных на охрану информационных отношений, содержащихся в Особенной части УК РФ, что препятствует, в том числе, эффективному процессу правоприменения. Также диссертант аргументированно доказывает необходимость криминализации таких деяний, как неправомерное собирание и хранение персональных данных физических лиц, незаконный оборот персональных данных физических лиц. Автор постулирует, что в ближайшем будущем возникнет необходимость уголовно-правовой оценки деятельности по реализации программ, созданных в рамках технологий искусственного интеллекта.

Во втором параграфе второй главы «Общая характеристика современной информационной преступности и отдельных ее видов»

рассматривается современная киберпреступность, ее специфика и особенности.

Соискатель приходит к выводу, что в теории уголовного права должны найти закрепление дефиниция и характеристика информационной войны, так как на международном уровне она уже получила свое официальное нормативное определение. Для уголовно-правового противодействия информационным войнам требуется установление критериев противоправности соответствующих деяний, обоснование уровня их общественной опасности и последствий.

Необходимо рассматривать информационную безопасность не только в контексте преступлений в сфере компьютерной информации, но и тех уголовно-правовых деликтов, которые связаны с распространением информации различного свойства и содержания как способом их совершения.

Автор дает свое определение кибератаки. Предлагая понимать ее как виновно совершаемое противоправное общественно опасное деяние 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 угрозу совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями (с. 123). Такую позицию следует поддержать.

Третий параграф второй главы посвящен вопросу ИТС «Интернет» как квалифицирующего признака деяния.

Автор отмечает, что за последнее десятилетие в закон введен ряд новых составов, отличительной чертой которых является наличие следующего квалифицирующего признака – «использование информационно-телекоммуникационных сетей (включая ИТС «Интернет»).

Диссертант справедливо подчеркивает, что любое, по сути, преступление, при подготовке или совершении которого использовались

ресурсы или возможности ИТС «Интернет», должно квалифицироваться с учетом данного признака. Тем не менее не все необходимые статьи УК РФ содержат указание на такое обстоятельство, поэтому соискатель приходит к выводу о целесообразности расширения перечня обстоятельств, отягчающих наказание, за счет его включения.

Третья глава диссертационного исследования посвящена рассмотрению уголовно-правовой характеристики посягательств на безопасность компьютерной информации в Российской Федерации: (ст. 272–274^2 УК РФ).

В первом параграфе третьей главы автор излагает свое видение содержания состава и проблем квалификации преступления, указанного в ст. 272 УК РФ.

Выявив достоинства и недостатки конструкции состава названного преступления, осуществив краткий обзор судебной практики, анализ теоретических позиций ученых, автор отмечает, что согласно ст. 1 УК РФ, уголовное законодательство РФ состоит исключительно из Уголовного кодекса. Вместе с тем сущностные характеристики общественно опасных последствий, напрямую влияющих на квалификацию, строгость и вид наказания за совершение преступления, предусмотренного ст. 272 УК РФ, содержатся в постановлении Пленума Верховного Суда РФ, что вряд ли оправдано. В результате рассмотрения диссертантом предложена скорректированная редакция ст. 272 УК РФ.

Во втором параграфе третьей главы пристальное внимание диссертанта сосредоточено на содержании состава и вопросах квалификации деяния, криминализованного в ст. 273 УК РФ, а также соответствующие теоретические изыскания, касающиеся данного преступления.

В результате диссертант предлагает свою редакцию ст. 273 УК РФ.

Здесь же представлена авторская дефиниция вредоносной компьютерной программы – это программа, созданная на языке программирования и заведомо предназначенная для неправомерного доступа

к компьютерным устройствам и воздействия на них в целях уничтожения, повреждения, модификации, копирования компьютерной информации, ознакомления с ней, осуществления слежения за компьютерным устройством, ограничения доступа к информационно-телекоммуникационным ресурсам в сети «Интернет», нейтрализации средств защиты компьютерной информации.

Третий параграф третьей главы ставит под вопрос необходимость существования ст. 274 УК РФ.

Автором отмечается, что решение об установлении уголовной ответственности за данное преступление является дискуссионным. Связано это, в первую очередь, с тем, что ст. 274 УК РФ применяет в судебно-следственной практике крайне редко.

Соискателем выделяется несколько моментов, связанных с применением анализируемой нормы. Во-первых, как показала практика, к правилам относятся не только нормы, предусмотренные федеральным законодательством, в том числе ГОСТы и СанПиНы, но и внутренние нормы и правила отдельных предприятий, особенно связанных с обеспечением различных видов тайн. Во-вторых, лицо, совершающее преступление, нередко нарушает соответствующие правила из корыстных или иных личных побуждений, что не нашло отражения в законе.

Четвертый параграф третьей главы посвящен содержанию состава и вопросам квалификации деяния, криминализованного в ст. 274^1 УК РФ, а также соответствующим теоретическим изысканиям, касающимся данного преступления.

Автор справедливо замечает, что конструирование в ч. 2 статьи материального состава исключает ответственность за неправомерный доступ к компьютерной информации объекта КИИ, не повлекший указанных в законе последствий. Например, в ситуации, когда лицо, реализуя преступный умысел, направленный на исследование и изучение системы функционирования и структуры объекта КИИ, из корыстной или иной личной заинтересованности осуществляет неправомерный доступ к охраняемой законом компьютерной

информации на объекте КИИ, однако не наносит вред самой системе, а лишь изучает ее, в том числе получая, например, сведения, составляющие государственную тайну, или осуществляет удаленное слежение за ней.

Соискателем предлагается обновленная редакция ст. 274^1 УК РФ, которая заслуживает, на наш взгляд, внимания законодателя.

В пятом параграфе третьей главы диссертант проводит анализ состава и проблем квалификации преступления, предусмотренного ст. 274^2 УК РФ.

Автор обоснованно обращает внимание на сложности в определении содержания состава преступления вследствие бланкетности предусматривающих его норм, отсутствие правоприменительной практики из-за сравнительно небольшого периода времени, прошедшего с момента криминализации данного деяния. В силу этого обстоятельства практически невозможно оценить перспективы «работы» названной статьи, а также выявить проблемы, которые могут возникнуть в процессе правоприменения.

Ставя общую положительную оценку диссертации на соискание ученой степени кандидата юридических наук Н.А. Лихачева, в то же время следует отметить, что некоторые сформулированные диссертантом положения и выводы носят дискуссионный характер, что обусловлено именно самостоятельным творческим исследованием достаточно сложной уголовно правовой и криминологической проблемы.

1. Так, автор многократно использует категории информационного пространства, медиапространства, киберпространства, виртуального пространства, не определяя соотношение данных терминов. Очевидно, что данное направление исследования позволит расширить теоретические знания, касающиеся проблем уголовно-правового обеспечения информационной безопасности. Но оно нуждается в уточнении характера и содержания используемых категорий.

2. Следует отметить, что в своем сравнительно-правовом исследовании диссертант недостаточно внимания уделил изучению опыта азиатских лидеров цифровизации. Автор не обосновывает свой выбор стран и

юрисдикций для анализа. Опыт многих стран из числа тех, на которые полагается автор, зачастую непереносим на российскую культурную, политическую и правовую реальность. Так, опыт ФРГ, который предлагается автором для заимствования, опирается на другие политические и идеологические подходы в регулировании и охране киберпространства. А вот опыт Китая в этой сфере вполне может быть учтен и использован в России.

3. Предлагая уточнить территориальный принцип действия уголовного закона в пространстве путем определения соотношения киберпространства и информационного пространства, установления юрисдикции государства над его национальным сегментом ИТС «Интернет» и распространения суверенитета за пределы материального мира, автор забывает, что Интернет, по сути, пространство международное. Для разграничения власти государств и других субъектов международного права в отношение сети Интернет требуется принятие международных нормативно-правовых актов.

Как уже было отмечено, указанные замечания носят дискуссионный характер и не умаляют в целом высокой положительной оценки диссертации. Диссертационное исследование подготовлено Н.А. Лихачевым самостоятельно, обладает внутренним единством, содержит новые результаты и положения, выдвигаемые для публичной защиты, и свидетельствует о решении научной задачи, имеющей значение для развития уголовно правовых наук. Предложенные Н.А. Лихачевым решения аргументированы и критически оценены по сравнению с другими известными решениями.

Содержание автореферата соответствует тексту диссертации, в нем отражены основные теоретические выводы и практические рекомендации, сформулированные диссертантом в результате проведенного исследования.

ОБЩИЙ ВЫВОД

Диссертация Лихачева Никиты Александровича на тему: «Уголовно-правовое противодействие преступлениям в сфере обеспечения информационной безопасности: законодательный, правоприменительный и

доктринальный аспекты», представляет собой завершенную научно-квалификационную работу, в которой на основании лично выполненных автором исследований решена научная задача, имеющая значение для развития науки уголовного права. Диссертационное исследование соответствует требованиям абзаца второго пункта 9 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства РФ от 24 сентября 2013 г. № 842 (в ред. от 26 января 2023 г.), а ее автор, Лихачев Никита Александрович, заслуживает присуждения искомой степени кандидата юридических наук по специальности 5.1.4. – Уголовно-правовые науки.

Отзыв подготовлен профессором академии цифровой трансформации, кандидатом юридическим наук, доцентом Дремлюгой Романом Игоревичем (690922, г. Владивосток, остров Русский, п. Аякс, 10, кампус ДВФУ, dremliuga.ri@dvfu.ru) и заведующим кафедрой уголовного права и криминологии, доктором юридических наук, профессором Коробеевым Александром Ивановичем (690922, г. Владивосток, остров Русский, п. Аякс, 10, кампус ДВФУ, korobeev.ai@dvfu.ru).

Отзыв обсужден и одобрен на заседании кафедры уголовного права и криминологии ФГАОУ ВО «Дальневосточный федеральный университет» протокол № 11 от «23» мая 2024 г.

Заведующий кафедрой уголовного права и
криминологии Юридической школы
ДВФУ, доктор юридических наук,
профессор,
заслуженный деятель науки
Российской Федерации

Коробеев
Александр Иванович

«23» мая 2024 г.

Федеральное государственное автономное
образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
690922, Россия, Приморский край, о. Русский, п. Аякс, 10, кампус ДВФУ
Контактные телефоны: 8 (423) 265 24 29; 8 (423) 243 34 72, факс 8 (423) 243 23 15
Электронный адрес (e-mail): rectorat@dvfu.ru
Веб-сайт: www.dvfu.ru

Коробеева Александра Александровича удостоверяю. Начальник отдела кадрового делопроизводства ДВФУ Н.А. Богданова
23 05 2024 г.

С отзывом ознакомлен Лихачев Н.А. 06.06.2024