

Частное образовательное учреждение
высшего образования
«Казанский инновационный университет
имени В.Г. Тимирязова (ИЭУП)»



Шәхси югары һөнәри
белем бирү учреждениесе
«В.Г. Тимирязов исемендәге Казан
инновация университеты (ИЭУП)»

Россия, Республика Татарстан, 420111, г. Казань, ул. Московская, 42
телефон: 8 (843) 231-92-90, факс: 8 (843) 292-61-59
ОКПО 34744628, ОГРН 1021602842095, ИНН/КПП 1654020511/165501001
e-mail: rector@ieml.ru, www.ieml.ru

В диссертационный совет 03.2.010.01,
созданный на базе федерального
государственного казённого
образовательного учреждения
высшего образования
«Омская ордена Почёта академия
Министерства внутренних дел
Российской Федерации»

644092, г. Омск,
пр-т Комарова, д. 7

ОТЗЫВ

**официального оппонента Бегишева Ильдара Рустамовича
на диссертацию Карабекова Канатбека Омирзаковича
«Киберпреступность в Российской Федерации и Республике Казахстан:
состояние и меры предупреждения»,
представленной на соискание ученой степени
кандидата юридических наук по научной специальности
5.1.4. Уголовно-правовые науки (юридические науки)**

1. Актуальность темы диссертации

Диссертация К. О. Карабекова посвящена исследованию одной из наиболее острых и динамично развивающихся проблем современной криминологии – киберпреступности в условиях цифровой трансформации общества. Актуальность избранной темы исследования не вызывает сомнений и обусловлена комплексом взаимосвязанных факторов как объективного, так и субъективного характера.

Прежде всего, следует отметить высокую степень практической

значимости исследуемой проблематики. Статистические данные, приводимые автором, красноречиво свидетельствуют о масштабах киберугроз: в Российской Федерации 88,0 % населения пользуется интернетом, в Республике Казахстан этот показатель достигает 89,2 %. Рост числа киберпреступлений напрямую коррелирует с увеличением количества интернет-пользователей, что создает серьезные вызовы для правоохранительных систем обеих стран. Особую тревогу вызывают приведенные соискателем данные о том, что в 2024 году в России было совершено порядка 680 тысяч преступлений с использованием информационных технологий, причинивших ущерб свыше 156 млрд рублей.

Научная актуальность исследования определяется недостаточной теоретической разработанностью концептуальных основ понимания киберпреступности как криминологического феномена в контексте сравнительно-правового анализа российского и казахстанского опыта. Существующие в юридической литературе подходы к определению сущности и содержания киберпреступности не в полной мере отражают специфику ее проявления в условиях интеграционных процессов на постсоветском пространстве и особенности детерминационного комплекса в различных правовых системах.

Особую актуальность диссертационному исследованию придает трансграничный характер киберпреступности и необходимость координации усилий правоохранительных органов сопредельных государств в борьбе с данным видом противоправной деятельности. К. О. Карабеков справедливо указывает на то, что киберпреступность для России и Казахстана является трансграничной угрозой, что обуславливает потребность в постоянном взаимодействии правоохранительных органов, обмене информацией и опытом противодействия киберугрозам.

2. Структура и содержание диссертации

Структура диссертационного исследования представляется логически

обоснованной, внутренне целостной и соответствующей поставленным автором целям и задачам. Работа состоит из введения, двух глав, включающих шесть параграфов, заключения, списка использованных источников и приложений, что в полной мере отвечает требованиям, предъявляемым к кандидатским диссертациям по юридическим наукам.

Первая глава «Криминологическая характеристика киберпреступности в Российской Федерации и Республике Казахстан» диссертации носит преимущественно теоретико-методологический характер и посвящена фундаментальным вопросам понимания природы и содержания киберпреступности как криминологического феномена. Глава состоит из трех логически взаимосвязанных параграфов, каждый из которых решает определенный круг исследовательских задач.

Первый параграф «Понятие и криминологическая природа киберпреступности» представляет собой глубокое теоретическое исследование понятийного аппарата в сфере киберпреступности. Автор демонстрирует серьезную аналитическую работу, проанализировав широкий спектр научных подходов российских и казахстанских ученых к определению сущности киберпреступности. В параграфе последовательно рассматриваются различные концептуальные подходы к пониманию данного феномена, выявляются их сильные и слабые стороны.

Особую ценность представляет проведенный автором сравнительный анализ терминологического аппарата, используемого в российской и казахстанской криминологической науке. Соискатель справедливо отмечает, что отсутствие единого понимания содержания киберпреступности создает серьезные препятствия для разработки эффективного законодательства и координации правоохранительной деятельности.

На основе критического анализа существующих подходов автор выделяет восемь основных признаков киберпреступности, среди которых: преступность в информационном пространстве; многообъектность посягательств (информационная безопасность, собственность, авторское

право, общественная безопасность, нравственность); охват всех преступных деяний, совершаемых с использованием информационно-коммуникационных технологий; повышенная латентность; автоматизированный характер совершения; дистанционность; высокий потенциал общественной опасности; опережение преступной деятельности темпами законодательного регулирования.

Научной новизной отличается предложенное К. О. Карабековым авторское определение киберпреступности как «исторически изменчивого, обладающего повышенной латентностью социального и уголовно-правового негативного явления, представляющего собой систему преступлений, совершенных дистанционно в информационном пространстве с использованием средств информационно-телекоммуникационных технологий». Данное определение отличается комплексностью подхода и учетом динамической природы исследуемого явления.

Второй параграф «Состояние и тенденции киберпреступности» содержит детальный сравнительный криминологический анализ количественных и качественных характеристик киберпреступности в России и Казахстане. Автор демонстрирует владение современными методами статистического анализа, используя обширную эмпирическую базу, включающую статистические данные ГИАЦ МВД России и Комитета по правовой статистике Генеральной прокуратуры Республики Казахстан за период с 2016 по 2024 годы.

Особую ценность представляют выявленные автором закономерности и различия в развитии киберпреступности в двух странах. Установлено, что доля киберпреступлений в общей структуре преступности в России составляет 40,0 %, в то время как в Казахстане этот показатель значительно ниже – 18,9 %. Вместе с тем темпы роста киберпреступности в Казахстане за последние восемь лет превысили аналогичные показатели в России в три раза, что свидетельствует о различной динамике развития данного вида преступности.

Автор проводит углубленный анализ структуры киберпреступности, выявляя, что в обеих странах преобладают преступления против собственности, совершаемые с использованием информационно-телекоммуникационных технологий. В России такие преступления составляют 63,53 % от общего числа киберпреступлений, в Казахстане – 94,46 %. При этом наиболее распространенным видом в обеих странах является мошенничество (около 50 % в России и 90 % в Казахстане).

Значительный интерес представляет анализ мнений сотрудников правоохранительных органов обеих стран о состоянии киберпреступности. Результаты анкетирования 268 российских и 243 казахстанских сотрудников показывают, что 50,0 % российских и 49,79 % казахстанских респондентов оценивают уровень киберпреступности как высокий, а до 20 % в каждой стране – как сверхвысокий.

Особую научную ценность имеет прогностический анализ развития киберпреступности с использованием технологий искусственного интеллекта, который, по мнению автора, будет способствовать облегчению доступа к совершению кибератак для лиц с ограниченными техническими знаниями.

Третий параграф «Особенности лиц, совершающих киберпреступления» представляет собой комплексное криминологическое исследование личности киберпреступника. Автор анализирует социально-демографические, нравственно-психологические и уголовно-правовые характеристики лиц, совершающих различные виды киберпреступлений.

Особую научную ценность представляет проведенный автором сравнительный анализ особенностей личности киберпреступников в России и Казахстане. Установлено, что российские кибермошенники характеризуются более старшим возрастом (30-49 лет) по сравнению с казахстанскими (21-29 лет), что составляет разницу в среднем в 15 лет. Это различие автор объясняет особенностями социально-экономического развития и цифровизации в двух странах.

Научной новизной отличается предложенная автором классификация

киберпреступников по степени их вовлеченности в преступную деятельность: начинающие киберпреступники (51,7 %), устойчивые киберпреступники (37,4 %) и профессиональные киберпреступники (10,9 %). Каждая категория характеризуется специфическими признаками по возрасту, образованию, уровню доходов и техническим навыкам.

Начинающие киберпреступники характеризуются средним уровнем дохода, возрастом от 18 до 30 лет, преимущественно базовым образованием и способностью использовать одно или несколько компьютерных устройств. Устойчивые киберпреступники отличаются более высоким уровнем доходов, возрастом от 20 до 25 лет, высшим техническим образованием и углубленными знаниями в области информационных технологий. Профессиональные киберпреступники характеризуются высоким материальным благосостоянием, возрастом от 25 до 49 лет, высшим техническим образованием и постоянным совершенствованием навыков, включая собственные разработки.

Вторая глава «Детерминация и предупреждение киберпреступности в Российской Федерации и Республике Казахстан» диссертации имеет ярко выраженную прикладную направленность и посвящена исследованию причинного комплекса киберпреступности и разработке мер ее предупреждения. Структурно глава состоит из трех параграфов, каждый из которых решает конкретные практически ориентированные задачи.

Первый параграф «Детерминанты киберпреступности» представляет собой системный анализ причин и условий, способствующих существованию и развитию киберпреступности в современных условиях. Автор разрабатывает оригинальную классификацию детерминант, разделяя их на внутренние и внешние факторы, что позволяет более точно определить направления профилактического воздействия.

Среди внутренних детерминант автор выделяет четыре основные группы: социально-экономические, организационно-технические, организационно-правовые и организационно-управленческие. К социально-экономическим детерминантам отнесены широкое использование

информационно-коммуникационных технологий в обществе, использование некачественного программного обеспечения, несоответствие между потребностями населения в информационных услугах и их недоступностью из-за низкого уровня жизни, монопольное положение разработчиков программного обеспечения.

Организационно-технические детерминанты включают нарушения мер информационной безопасности, низкий уровень осведомленности о правилах использования интернет-ресурсов, неэффективную защиту информационных систем, уязвимость программного обеспечения, отсутствие эффективных механизмов контроля и обнаружения кибератак.

К организационно-правовым детерминантам автор относит недостаточное правовое урегулирование вопросов кибербезопасности на национальном уровне, отсутствие единства в понимании основных терминов, связанных с кибербезопасностью, отсутствие эффективной правовой защиты интересов пострадавших от кибермошенников.

Организационно-управленческие детерминанты связаны с отсутствием стратегического подхода к противодействию киберугрозам, недостаточным вниманием руководства к проблемам информационной безопасности, отсутствием типовых программ профилактики, низкой квалификацией специалистов правоохранительных органов в области кибербезопасности.

Внешние детерминанты включают организационно-технические факторы (деятельность международных киберпреступных группировок, распространение вредоносного программного обеспечения) и организационно-правовые факторы (недостатки международно-правового регулирования, сложности в международном сотрудничестве).

Особую ценность представляет выделение автором специфических особенностей детерминант киберпреступности в каждой из стран. Для России характерно существенное влияние внешних факторов, связанных с применением зарубежных санкций, для Казахстана – преобладание внутренних социально-экономических факторов, связанных с безработицей

среди молодого населения.

Второй параграф «Правовое обеспечение предупреждения киберпреступности» содержит комплексный анализ нормативно-правовой базы противодействия киберпреступности на различных уровнях правового регулирования. Автор предлагает трехуровневую систему правового обеспечения: международный (акты ООН), межгосударственный (региональные соглашения) и национальный уровни.

Автор обосновывает необходимость подписания Россией и Казахстаном единой международной Конвенции ООН против киберпреступности, принятия единых нормативных актов дружественных стран на межгосударственном уровне, совершенствования национального законодательства. Для Казахстана предлагается принятие постановления Верховного Суда, разъясняющего применение законодательства об ответственности за киберпреступления.

Значительное внимание уделяется анализу позитивного опыта правового регулирования в сфере кибербезопасности. Отмечается необходимость разработки концепции кибербезопасности России с использованием соответствующего опыта Казахстана, закрепления на международном уровне единых определений терминов в сфере кибербезопасности.

Третий параграф «Меры предупреждения киберпреступлений» представляет собой систематизированное изложение конкретных мер профилактического воздействия, структурированных по уровням применения и сферам воздействия. Автор предлагает двухуровневую систему мер: государственный и межгосударственный уровни.

На государственном уровне выделяются меры, направленные на нейтрализацию внутренних факторов: социально-экономические (включение общества в процессы выявления киберпреступлений, совершенствование информационной культуры, обеспечение доступности лицензионного программного обеспечения, создание специализированных баз данных); организационно-технические (внедрение образовательных курсов, совершенствование системы защиты информации, усиление

кибербезопасности критической инфраструктуры, постоянный мониторинг телекоммуникационных сетей); организационно-управленческие (внедрение принципов стратегического противодействия киберугрозам, создание специализированных подразделений, разработка специальных программ профилактики, организация профильного обучения сотрудников).

На межгосударственном уровне предлагаются меры, направленные на сокращение внешних факторов: пресечение влияния недружественных государств, установление эффективного международного сотрудничества, обмен информацией об эффективных мерах борьбы с киберпреступностью, участие в международных форумах по координации действий против киберугроз.

Особую практическую ценность представляют предложения автора по использованию положительного опыта Казахстана в области блокировки зарубежных звонков с подменных номеров, что позволило пресечь свыше 43 млн попыток мошеннических соединений и сократить количество пострадавших более чем в 2,5 раза.

Структура диссертации отражает логическую последовательность научного познания: от общего к частному, от теоретических основ к практическим рекомендациям. Первая глава создает необходимую теоретико-методологическую базу для последующего анализа практических аспектов противодействия киберпреступности, представленных во второй главе.

Внутри каждой главы параграфы логически связаны между собой и образуют целостную систему знаний. В первой главе движение от понятийного аппарата к анализу состояния и характеристике субъектов позволяет сформировать комплексное представление о киберпреступности как криминологическом феномене. Во второй главе последовательность «детерминанты – правовое обеспечение – конкретные меры» обеспечивает системность подхода к разработке мер предупреждения.

Объем каждого структурного элемента соответствует его значимости в общей концепции исследования. Наиболее объемными являются параграфы,

посвященные анализу состояния киберпреступности и мерам ее предупреждения, что отражает прикладную направленность работы.

3. Новизна научных положений, выводов и рекомендаций, сформулированных в диссертации

Научная новизна представленного диссертационного исследования проявляется в нескольких ключевых аспектах, которые вносят существенный вклад в развитие криминологической науки и практики противодействия киберпреступности.

Во-первых, автором разработан оригинальный концептуальный подход к определению киберпреступности, учитывающий специфику правовых систем России и Казахстана. Предложенное определение киберпреступности как «исторически изменчивого, обладающего повышенной латентностью социального и уголовно-правового негативного явления, представляющего собой систему преступлений, совершенных дистанционно в информационном пространстве с использованием средств информационно-телекоммуникационных технологий» отличается комплексностью и учетом динамической природы исследуемого феномена.

Во-вторых, несомненной новизной характеризуется проведенный соискателем сравнительный криминологический анализ состояния киберпреступности в двух государствах. Выявленные различия в уровне, структуре и динамике киберпреступности (доля киберпреступлений в России составляет 40,0 % от общей структуры преступности, в Казахстане – 18,9 %) представляют значительный интерес для понимания особенностей детерминации данного вида преступности в различных социально-экономических условиях.

В-третьих, оригинальной является предложенная автором классификация киберпреступников по степени их вовлеченности в преступную деятельность: начинающие киберпреступники (51,7 %), устойчивые киберпреступники (37,4 %) и профессиональные

киберпреступники (10,9 %). Данная типология имеет не только теоретическое, но и существенное практическое значение для дифференциации мер предупредительного воздействия.

В-четвертых, новизной отличается комплексная система детерминант киберпреступности, структурированная автором на внутренние (социально-экономические, организационно-технические, организационно-правовые, организационно-управленческие) и внешние (организационно-технического и организационно-правового характера) факторы. Такой подход позволяет более точно определить направления профилактического воздействия.

В-пятых, научной новизной обладает разработанная автором система мер предупреждения киберпреступности, дифференцированная по уровням воздействия (государственный и межгосударственный) и сферам применения, что создает методологическую основу для формирования эффективной политики противодействия киберугрозам.

4. Степень обоснованности и достоверности научных положений, выводов и рекомендаций, сформулированных в диссертации

Степень обоснованности и достоверности научных положений, изложенных в диссертации, представляется высокой и соответствующей современным требованиям к научным исследованиям в области юридических наук.

Методологическая обоснованность работы подтверждается использованием комплекса общенаучных и частнонаучных методов познания, включая диалектический метод, формально-юридический, сравнительно-правовой, статистические методы, системно-структурный анализ и метод социологического опроса. Такой методологический плюрализм обеспечивает всесторонность и объективность исследования.

Эмпирическая база исследования характеризуется репрезентативностью и достоверностью. Автор проанализировал обширный массив статистических данных ГИАЦ МВД России и Комитета по правовой статистике Генеральной

прокуратуры Республики Казахстан за период с 2016 по 2024 годы, изучил 153 приговора российских судов и 163 приговора судов Казахстана, провел анкетирование 268 сотрудников российских правоохранительных органов и 243 сотрудников правоохранительных органов Казахстана, а также опросил 320 российских и 434 казахстанских граждан.

Теоретическая обоснованность диссертации подкрепляется анализом широкого круга научных источников, включающих работы ведущих российских и казахстанских криминологов. Автор демонстрирует глубокое знание современного состояния научной разработки проблемы и умение критически оценивать существующие теоретические подходы.

Достоверность выводов подтверждается их логической последовательностью, соответствием эмпирическим данным и возможностью практической реализации предложенных рекомендаций. Особо следует отметить, что результаты исследования уже находят практическое применение, о чем свидетельствуют акты внедрения в учебный процесс ведущих юридических вузов и практическую деятельность правоохранительных органов.

5. Дискуссионные положения и замечания по диссертации

При общей высокой оценке представленного диссертационного исследования необходимо отметить ряд дискуссионных положений и высказать некоторые замечания, которые могут способствовать дальнейшему совершенствованию научных воззрений автора.

Во-первых, представляется дискуссионным вопрос о включении в структуру киберпреступности всех преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Автор справедливо выделяет два основных блока: собственно киберпреступления в сфере компьютерной информации и преступления, совершаемые с использованием ИТ-технологий. Однако представляется, что такой широкий подход может привести к размыванию специфики

киберпреступности как относительно самостоятельного криминологического явления. Возможно, следовало бы более четко разграничить указанные категории и сосредоточиться на анализе собственно киберпреступлений.

Во-вторых, при анализе детерминант киберпреступности автор уделяет недостаточное внимание психологическим факторам, определяющим особенности мотивации киберпреступников. Представляется, что более глубокое исследование психологических механизмов вовлечения в киберпреступную деятельность могло бы обогатить предложенную систему детерминант и повысить эффективность предупредительных мер.

В-третьих, предложенная автором классификация киберпреступников, безусловно, имеет научную и практическую ценность, однако представляется, что критерий «степени вовлеченности в преступную деятельность» не является единственно возможным. Альтернативные подходы, основанные на мотивации, способах совершения преступлений или объектах посягательства, могли бы дополнить предложенную типологию.

В-четвертых, исследование недостаточно учитывает стремительное развитие цифровых технологий (искусственный интеллект, блокчейн, квантовые вычисления), которые кардинально меняют характер киберугроз. Предложенные меры предупреждения могут быстро устареть в условиях технологической революции.

В-пятых, при рассмотрении международно-правовых аспектов противодействия киберпреступности автор недостаточно подробно анализирует возможности использования механизмов Шанхайской организации сотрудничества и Евразийского экономического союза для координации усилий в данной сфере.

Высказанные замечания носят дискуссионный характер и не снижают общей положительной оценки диссертационного исследования. Они могут служить основой для дальнейшего развития научных воззрений автора и продолжения исследований в данной области.

6. Заключение о соответствии диссертации критериям, установленным Положением о присуждении ученых степеней

На основании проведенного анализа диссертации Карабекова Канатбека Омирзаковича можно констатировать, что представленная работа в полной мере соответствует критериям, установленным Положением о присуждении ученых степеней, и требованиям, предъявляемым к кандидатским диссертациям по юридическим наукам.

Диссертация представляет собой самостоятельное, завершенное научное исследование, в котором решена задача, имеющая существенное значение для развития криминологической науки и практики противодействия киберпреступности. Автором получены новые научно обоснованные результаты, которые в совокупности можно квалифицировать как решение научной задачи, имеющей значение для развития уголовно-правовой науки.

Научная новизна и теоретическая значимость работы подтверждаются разработкой оригинальной концепции киберпреступности, созданием комплексной системы ее детерминант, формулированием авторской типологии киберпреступников и предложением системы мер предупреждения. Практическая значимость исследования демонстрируется возможностью использования его результатов в правоохранительной деятельности, законотворческом процессе и образовательной практике.

Достоверность и обоснованность научных положений подкрепляются использованием современной методологии, анализом репрезентативной эмпирической базы и апробацией результатов в научном сообществе. Автор демонстрирует высокий уровень научной квалификации, глубокое знание предмета исследования и способность к самостоятельной научно-исследовательской деятельности.

Представленные в диссертации выводы и рекомендации имеют четкую практическую направленность и могут быть использованы для совершенствования деятельности правоохранительных органов России и Казахстана по противодействию киберпреступности, что подтверждается

актами внедрения результатов исследования в практическую деятельность и учебный процесс.

Таким образом, диссертация Карабекова Канатбека Омирзаковича «Киберпреступность в Российской Федерации и Республике Казахстан: состояние и меры предупреждения» представляет собой квалифицированное научное исследование, соответствующее требованиям п. 9-14 Положения о присуждении ученых степеней, утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842 «О порядке присуждения ученых степеней» (ред. от 16 октября 2024 г.), а диссертант заслуживает присуждения ученой степени кандидата юридических наук по специальности 5.1.4. Уголовно-правовые науки (юридические науки).

Официальный оппонент:

Профессор кафедры уголовного права и процесса
Казанского инновационного университета имени В. Г. Тимирязова,
заслуженный юрист Республики Татарстан,
доктор юридических наук, доцент

«5» ноября 2025 г.

Ильдар Рустамович Бегишев

Контактные данные:

Бегишев Ильдар Рустамович – доктор юридических наук (специальность 12.00.08 – «Уголовное право и криминология; уголовно-исполнительное право»), доцент (специальность 5.1.4. Уголовно-правовые науки)

Полное наименование образовательной организации:

Частное образовательное учреждение высшего образования «Казанский инновационный университет имени В. Г. Тимирязова»

Сокращенное наименование образовательной организации:

Казанский инновационный университет, КИУ имени В. Г. Тимирязова, КИУ

Почтовый адрес: 420111, г. Казань, ул. Московская, д. 42

Телефон: +7 (843) 231-92-90

Факс: +7 (843) 292-61-59

E-mail: begishev@ieml.ru

Сайт: <https://ieml.ru>

