

## **АННОТАЦИЯ**

**на диссертацию на соискание ученой степени доктора философии (PhD)  
докторанта Костанайская академия Министерства внутренних дел  
Республики Казахстан имени Ш. Кабылбаева по образовательной  
программе 8D12301 – «Правоохранительная деятельность»  
Джилкишиева Руслана Булатовича на тему: «Расследование  
преступлений в сфере информационных технологий»**

**Общая характеристика исследования.** Диссертационное исследование посвящено комплексному криминалистическому анализу расследования преступлений в сфере информационных технологий, с акцентом на совершенствование методических и организационных подходов к выявлению и раскрытию киберпреступлений. Целью работы является разработка и модернизация практических рекомендаций, направленных на повышение эффективности расследования противоправных деяний в указанной области. Объектом исследования выступают преступления, совершаемые с использованием информационно-коммуникационных технологий, предметом — закономерности их совершения, а также методы и средства их раскрытия и расследования. Методологическую основу составили системный, сравнительно-правовой, дидактический и статистический методы, позволившие обеспечить целостность подхода к изучаемой проблематике. Теоретическую базу составили научные труды казахстанских и зарубежных авторов, а также действующее законодательство Республики Казахстан и международно-правовые акты. Научная новизна исследования заключается в разработке авторской криминалистической характеристики киберпреступлений, алгоритмов следственных действий и предложении институциональных решений, включая создание Национального центра управления кибербезопасностью и цифровой криминалистики.

**Актуальность темы исследования.** Основоположниками становления информационных технологий (середина XX в.) принято считать Клода Шеннона и Роберта Винера, работы которых заложили основы для понимания процессов передачи и обработки информации и оказали значительное влияние на развитие автоматизированных систем. Достижения в области компьютеров, современных телекоммуникаций и средств связи стали, своего рода, «спусковым механизмом» для развития абсолютного нового сектора экономики, демонстрирующего самые быстрые темпы развития на сегодняшний день.

Процесс усовершенствования и развития технологий характеризуется значительными изменениями в существующих системах коммуникации. Доминирующие две формы общения вплоть до середины XX века — почта и печатные издания (газеты, журналы, книги) были интегрированы и объединены в единое информационно-коммуникационное пространство — кибернетическое пространство.

Появление персональных компьютеров и интернета в 1970-х годах, а позже создание глобальной сети Интернет привело к кардинальным изменениям в различных сферах жизни человека, включая экономику, образование, медицинское обслуживание и социальные взаимодействия. Что, в свою очередь, привело к развитию новых форм преступности, связанных с использованием информационных технологий. В настоящей диссертационной работе предполагается исследовать вопрос совершения противоправных деяний через глобальную сеть интернет или международных систем связи.

Сеть Интернет предоставляет ряд неоспоримых преимуществ для совершения противоправной деятельности. В первую очередь, это неограниченный объем различной информации (текстовая, графическая, аудио-, видео-), передаваемой по сети. Во-вторых, возможность использования психологических приемов для манипулирования пользователями в глобальных масштабах.

Согласно статистическим сведениям с 2019 – 2023 года в Казахстане зарегистрировано 407 деяний: 2019 – 108, 2020 – 62, 2021 – 74, 2022 – 85, 2023 – 78, 2024 - 101 – в сфере информационных технологий и киберпреступности.

Совершаемые киберпреступления имеют высокий уровень латентности, наносят значительный ущерб как индивидуальным пользователям, так и коммерческим компаниям и государственным учреждениями. Учитывая вышеперечисленные моменты, становится очевидным, что традиционные методы расследования противоправных деяний являются недостаточными и малоэффективными. Это делает задачу усовершенствования методов борьбы с киберпреступностью одной из приоритетных в сфере правопорядка и безопасности, что, в свою очередь, создает потребность в разработке специальных методик, учитывающих специфику компьютерных правонарушений.

Актуальность киберпреступности с одной стороны, недостаточная ее разработанности, с другой стороны (детально будет рассмотрено в рамках данной диссертационной работы), вызывает острую необходимость дальнейшего развития криминалистики как научной дисциплины, использование знаний из различных областей науки (информационные технологии, психология, юридические науки и пр.), а также улучшение существующих методов расследования и разработки новых подходов.

Несмотря на наличие значимых исследований в отдельных областях расследования киберпреступлений, в настоящее время наблюдается нехватка целостности и системности работ, охватывающих все аспекты криминалистической методики расследования, отсутствует достаточная интеграция методов и знаний, что снижает (затрудняет) эффективное расследование данной категории дел.

Таким образом, с нынешним состоянием знаний и рекомендаций в области расследования киберпреступлений, необходимо глубокое, системное

исследование, способное оказать реальное влияние на практическую деятельность и повышение эффективности расследования в данной сфере поскольку отдельные частные рекомендации могут быть полезны в отдельных случаях, но не носят системный характер. Практические работники нуждаются в четких, системных и интегрированных методах работы, получение же несистематизированной, частичной информации не может решить основные проблемы, с которыми сталкиваются следователи. Стремление разработки более системной методики, желание предложить новые подходы, основанные как на теории, так и на практике подтолкнуло нас к выбору данной темы диссертационной работы.

#### **Степень научной разработанности темы исследования.**

Проблематика расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий, в последние годы последовательно входит в круг приоритетных направлений научного поиска в уголовно-правовой и криминалистической доктрине. Вопросы квалификации, профилактики и раскрытия киберпреступлений освещены в работах таких авторитетных исследователей, как Ж.К. Аманов, Е.О. Алауханов, А.Н. Агыбаев, К.А. Бегалиев, Б.А. Бекназаров, В.Б. Вехов, Р.Е. Джансараева, А.А. Исаев, В.В. Крылов, Е.И. Каиржанов, И.Ю. Лоскутов, В.А. Мещеряков, В.Ю. Рогозин, И.И. Рогов, С.М. Рахметов, Л.Н. Соловьев, Т.Б. Сеитов, Б.Х. Толеубекова и других, в трудах которых раскрыты теоретико-правовые основы борьбы с преступностью в цифровой среде, а также обозначены отдельные направления по усовершенствованию следственной практики.

В зарубежной криминалистике вопросам противодействия киберугрозам посвящены исследования, преимущественно ориентированные на технические аспекты и международное сотрудничество. Однако в научных источниках, как отечественных, так и международных, сохраняется потребность в систематизации знаний о специфике расследования преступлений в сфере информационных технологий, а также в разработке целостной криминалистической методики, учитывающей национальные особенности правоприменительной практики.

Таким образом, данное диссертационное исследование логически опирается на имеющуюся научную базу и в то же время направлено на её развитие и расширение в условиях современных цифровых вызовов. Работа представляет собой шаг к формированию интегративного подхода, сочетающего правовую, криминалистическую и технологическую составляющие процесса расследования, что подтверждает её научную обоснованность и актуальность.

**Целью настоящей диссертационной работы** является разработка модернизация практических рекомендаций, которые повысят эффективность процесса расследования противоправных деяний в сфере информационных технологий. Нами поставлены следующие **задачи**:

- проанализировать текущую ситуацию в сфере противодействия киберпреступности;
- разработать классификационные признаки преступлений в сфере информационных технологий;
- раскрыть содержание элементного состава криминалистической характеристики киберпреступлений;
- выявить механизмы начала досудебного производства расследования преступлений в сфере информационных технологий;
- сформулировать алгоритмы первоначального этапа расследования преступлений в сфере информационных технологий;
- разработать алгоритмы последующего этапа расследования преступлений в сфере информационных технологий.

**Объектом** данного диссертационного исследования являются противоправные деяния, совершаемые в сфере информационных технологий, а также изучение практических аспектов их раскрытия и расследования.

**Предметом** диссертационного исследования является выявление закономерностей и уникальных черт, характерных для противоправных деяний рассматриваемой сферы, методов и подходов, используемых для расследования, определение следственных действий, которые следователю следует предпринимать в ходе первоначальных и последующих следственных действий.

**Методологическая основа** диссертационного исследования включает в себя различные методы и подходы. В методологической основе — использование дидактических принципов и системного подхода, позволяющие рассматривать предмет исследования в контексте более широкой системы. Применение сравнительно-правового и статистического методов способствует проведению более глубокого анализа, а также позволяет сопоставить различные аспекты расследования противоправного деяния в рассматриваемой сфере.

**Нормативная основа** диссертационного исследования включает Конституцию Республики Казахстан, а также международно-правовые акты, относящиеся к теме диссертации. Проанализированы в части, соответствующей объекту исследования действующее уголовное, уголовно-процессуальное законодательство, а также имеющаяся по теме литература, позволившая построить работу как логическое продолжение и развитие ранее проводившихся исследований в сфере информационных технологий, с учетом новых реалий, сопоставив с ними полученные результаты.

**Эмпирической основой** диссертационного исследования послужили данные проведенного автором анализа статистических отчетов за 2019-2024 годы в предоставленных Комитетом правовой статистики и специальных учетов ГП РК по правонарушениям, в сфере информационных технологий, законы «О национальной безопасности», «Об информатизации», «О государственных секретах», «О персональных данных и их защите», «Об электронном документе и электронной цифровой подписи», «О связи»,

Уголовный кодекс РК, Кодекс РК «Об административных правонарушениях», Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности (постановление Правительства РК от 20.12.2016 г. №832), Концепция кибербезопасности («Киберщит Казахстана»).

В диссертации автор использовал личный опыт работы на различных должностях в правоохранительных органах.

**Научная новизна исследования.** Используемый системный подход впервые позволил не просто изучить отдельные вопросы расследования преступлений в сфере информационных технологий, но и провести их комплексный анализ в контексте более широкой системы во взаимосвязи и взаимодействии исследуемой проблемы с другими элементами.

Настоящий диссертационный труд затронул ряд ключевых проблем организационного, тактического, методического характера, а также правовые и этические аспекты, работу правоохранительных органов.

Предложены новые идеи, способствующие лучшему пониманию и систематизации знаний о противоправных деяниях в рассматриваемой сфере, представляющие теоретический интерес.

Выводы и рекомендации, выработанные в ходе исследования, могут быть применимы в практической деятельности органов правопорядка и других организаций, имеющих непосредственное отношение к расследованию правонарушений в сфере информационных технологий.

На рассмотрение вынесены отдельные вопросы, касающиеся превентивных мер совершения преступлений в сфере информационных технологий.

Новизна работы обусловлена также существенным изменением нормативной правовой базы, сложившейся в последние годы обширной судебной практикой применения нового законодательства по правонарушениям в сфере информационных технологий.

#### **Положения, выносимые на защиту:**

1. Проведенным исследованием осуществлена авторская категоризация совокупности мер и усилий правоохранительных органов и служб, участвующих в раскрытии и расследовании киберпреступлений, которая включает в себя правовое регулирование; специализацию правоохранительных органов; технические инструменты и методы расследования; международное сотрудничество, которые, при условии взаимных реализаций, могут оказать эффективное воздействие на текущую ситуацию в сфере совершения рассматриваемой разновидности преступлений.

2. Предложена классификационная характеристика уголовно-правовых правонарушений, составы которых подпадают под собирательную дефиницию «Правонарушения в сфере информационных технологий», среди которых: неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций (ст. 205 УК); неправомерное уничтожение или

модификация информации (ст. 206 УК); нарушение работы информационной системы или сетей телекоммуникаций (ст. 207 УК); неправомерное завладение информацией (ст. 208 УК); принуждение к передаче информации (ст. 209 УК); создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210 УК); неправомерное распространение электронных информационных ресурсов ограниченного доступа (ст. 211 УК); предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели (ст. 212 УК); неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст. 213 УК).

**3.** Создан авторский вариант криминалистической характеристики преступлений в сфере информационных технологий, включающий в себя следующие элементы: предмет преступного посягательства; время, место, орудие и обстановка совершения; способы подготовки, совершения и сокрытия правонарушений, в сфере информационных технологий; следовая картина; типологические особенности личности правонарушителя, в сфере информационных технологий; причины и условия, способствующие совершению правонарушения в сфере информационных технологий.

**4.** Аргументирован прикладной инструментарий автора, применительно к началу досудебного производства: какие конкретно данные или системы подверглись воздействию злоумышленников, каков характер преступления, какова структура объекта, где возможно было совершено противоправное деяние. Следовательно необходимо проанализировать условия, в которых функционирует объект: способ обработки и хранения данных; система документооборота (товарооборота); параметры оборудования и программного обеспечения, позволяющие определить способ взаимодействия между компьютерами и пользователями; уровень организация мер безопасности для защиты конфиденциальной информации; должностные инструкции сотрудников, в чьи обязанности входит обработки и хранение компьютеров и информации ставшей объектов преступного посягательства.

**5.** Разработанная автором классификация однотипных и неоднотипных следственных ситуаций первоначального этапа расследования правонарушений в сфере информационных технологий, которые обуславливают основные направления раскрытия и расследования рассматриваемых правонарушений, выбор оптимального алгоритма действий по организации и производству необходимого комплекса неотложных следственных действий, включающие в себя: а) наличие лишь частичной информации о факте самого правонарушения, личности пострадавшего, отсутствие сведений о лице, совершившем правонарушение, мотивы которого неясны; б) имеется полная информация о личности пострадавшего, мотивах совершения правонарушения и лицах его совершивших, однако

подозреваемое лицо заявляет о своей непричастности и отказывается от дачи признательных показаний; в) имеется полная картина следствия, однако подозреваемое лицо не желает сотрудничать со следствием, заявляя о своей непричастности к совершенному противоправному деянию, отказываясь признавать свою вину; г) подозреваемое лицо сотрудничает со следствием, полностью признав свою вину в совершении противоправного деяния, давая признательные показания.

6. Обоснован алгоритм производства проверочных следственных действий на последующем этапе расследования преступлений в сфере информационных технологий, с целью преодоления противоречий, устранения нестыковок и несоответствий по следующей формуле: следственный эксперимент – последующие допросы – дополнительные экспертизы.

7. С учётом современных вызовов в сфере цифровой безопасности, предлагается инициировать создание в Казахстане Национального центра управления кибербезопасностью и цифровой криминалистики (далее – НЦУКЦК) как межведомственного координационного органа. Центр будет объединять усилия правоохранительных и специальных государственных органов (МВД, КНБ, Агентство по финансовому мониторингу и других заинтересованных государственных органов), частного сектора и международных партнёров, обеспечивая обмен информацией о киберинцидентах через единую цифровую платформу на основе блокчейн-технологий. Среди ключевых функций – формирование базы киберпреступлений, оперативный обмен данными, развитие цифровой криминалистики с использованием «ИИ» и «Big Data», создание института киберследователей, а также установление механизмов международного сотрудничества. Законодательное обеспечение предлагается реализовать через принятие специального закона «О противодействии киберпреступности».

8. С целью повышения эффективности расследования преступлений в сфере информационных технологий предлагается внедрение специализированного программно-аналитического комплекса (далее – СПАК), обеспечивающего автоматизированный сбор, анализ и хранение цифровых доказательств с применением искусственного интеллекта. СПАК позволит систематизировать данные, ускорить формирование экспертных заключений и улучшить межведомственное взаимодействие. Его внедрение на базе Центра судебных экспертиз и перспективно — в рамках Национального центра кибербезопасности, обеспечит сокращение сроков расследований, повышение квалификации специалистов и повышение качества цифровой криминалистики в Казахстане. Также имеется альтернатива в бедующем СПАК можно будет применять, ранее нами предложенном в новом Национальном центре управления кибербезопасностью и цифровой криминалистики.

9. В условиях стремительного роста бесконтактного сбыта наркотиков через интернет, мессенджеры и даркнет, предлагается сформировать в Казахстане стратегию противодействия цифровым формам наркопреступности, акцентируя внимание на закладчиках. Ключевые меры включают: совершенствование законодательства с введением специальных квалифицирующих признаков, создание цифровых платформ для мониторинга и обмена данными, а также внедрение интеллектуальных систем анализа цифровых следов и метаданных. Предусматривается активное вовлечение общества, разработка мобильных приложений для сообщений о закладках, расширение оперативной деятельности в даркнете и использование ИИ для выявления преступных схем. Комплексный подход обеспечит снижение наркоугроз и повышение эффективности правоохранительной деятельности.

**Основные результаты диссертации отражены в 8 научных публикациях.**

**Опубликованные в международном рецензируемом журнале (имеющем ненулевой импакт-фактор или входящих в базу данных Scopus (Скопус), JSTORE (ДЖЕЙСТОП): Problems of Investigation of Crimes in the Field of Information Technology. Pakistan Journal of Criminology Vol. 16, No. 03, July—September 2024 (97-114).**

**Опубликованные в научных изданиях, включенных в Перечень научных изданий, рекомендуемых для публикации основных результатов научной деятельности, утверждаемый Комитетом по контролю в сфере образования и науки МОН РК.**

1. Современное состояние и перспективы противодействия преступлениям в сфере киберпреступности. «Хабаршы-Вестник», №4(86) 2021 г.

2. Содержание и сущность элементов криминалистической характеристики правонарушений в сфере информационных технологий и киберпреступности. Ученые труды Алматинской Академии МВД Республики Казахстан имени М.Есбулатова, № 4(81) 2024 г.

3. Обстоятельства, подлежащие доказыванию и задачи расследования по уголовным делам об информационных технологиях и киберпреступности. Ученые труды Алматинской Академии МВД Республики Казахстан имени М.Есбулатова, № 4(81) 2024 г.

**Опубликованные в материалах международных конференций.**

1. Проблемы расследования преступлений в сфере информационных технологий. «Аубакировские чтения» Материалы международной научно-практической конференции 19.02.2018 г.

2. Киберпреступность в сфере социальных сетей. Правовой научно-практический журнал «Заң және заман» №12 (216), декабрь 2018 стр. 28-31.

3. On the Forensic Characterization of the Identity of the Subjects of Crimes in the Field of High Technologies - «Journal of Advanced Research in Law and economics», Fall 2018 Volume IX issue 6 (36), pp.2011-2015.

4. Классификация правонарушений в сфере киберпреступности. «Аубакировские чтения». Материалы международной научно-практической конференции, ст.68-72. 19.02.2025 г.