УДК 343

Мауленов Д.

студент

Высшая школа юриспруденции и судебно-технической экспертизы

Санкт-Петербургский политехнический университет Петра Великого

(г. Санкт-Петербург, Россия)

ЦИФРОВИЗАЦИЯ РОЗЫСКА И ОБМЕНА ДОКАЗАТЕЛЬСТВАМИ: НЕОБХОДИМОСТЬ ПРИНЯТИЯ УГОЛОВНО-ПРОЦЕССУАЛЬНОГО КОДЕКСА СНГ В ЭПОХУ ТРАНСНАЦИОНАЛЬНОЙ КИБЕРПРЕСТУПНОСТИ

***Аннотация**: целью настоящей работы является обоснование необходимости разработки и принятия единого Уголовно-процессуального кодекса Содружества Независимых Государств как ответа на вызовы транснациональной киберпреступности. В условиях стремительной цифровизации всех сфер жизнедеятельности преступность приобретает выраженный трансграничный характер, а электронные доказательства становятся ключевым средством доказывания. Однако разрозненность национальных уголовно-процессуальных законодательств государств — участников СНГ, отсутствие унифицированных процедур сбора, хранения и трансграничной передачи цифровых доказательств, а также медлительность существующих механизмов правовой помощи делают борьбу с киберпреступностью на пространстве Содружества малоэффективной. Методология исследования опирается на сравнительно-правовой анализ модельного законодательства СНГ, национальных уголовно-процессуальных кодексов государств — участников, а также международных актов, в частности Будапештской конвенции о киберпреступности и нового проекта Конвенции ООН. Кроме того, использованы формально-юридический метод и метод системного анализа. Результаты работы показывают, что создание единого процессуального кодекса СНГ, интегрирующего цифровые доказательства в качестве самостоятельного источника, закрепляющего ускоренные процедуры трансграничного обмена электронными данными и учреждающего наднациональный координационный механизм, позволит существенно повысить оперативность розыска и доказательственного обеспечения по уголовным делам о киберпреступлениях.*

Практическая значимость исследования заключается в возможности использования его выводов в работе Межпарламентской Ассамблеи СНГ, национальных законодательных органов и правоохранительных структур при разработке и имплементации унифицированных процессуальных норм.

***Ключевые слова**: киберпреступность, СНГ, цифровизация, уголовно-процессуальный кодекс, цифровое доказательство, трансграничный розыск, обмен электронными данными, модельный закон, международная правовая помощь, гармонизация права.*

ВВЕДЕНИЕ.

Стремительное развитие информационно-коммуникационных технологий кардинально изменило облик современной преступности. Если ещё два десятилетия назад киберпреступления воспринимались точнее как экзотика, то сегодня они превратились в одну из наиболее опасных и динамично растущих форм противоправной деятельности. По оценкам экспертов, ущерб мировой экономике от киберпреступности исчисляется триллионами долларов, а количество регистрируемых инцидентов увеличивается год от года. Особую тревогу вызывает то обстоятельство, что значительная часть таких деяний носит транснациональный характер: преступник может физически находиться на территории одного государства, использовать серверы, расположенные во втором, а жертвами становиться граждане третьего. В этих условиях национальные правоохранительные системы, замкнутые в рамках собственных юрисдикций, оказываются заведомо неэффективными.

Для государств – участников Содружества Независимых Государств проблема осложняется ещё и тем, что, несмотря на общее историческое прошлое и во многом схожие подходы к построению уголовного процесса, их национальные законодательства за прошедшие десятилетия существенно разошлись. Модельный Уголовно-процессуальный кодекс, принятый Межпарламентской Ассамблеей СНГ ещё в 1996 году, безнадёжно устарел и не учитывает реалий цифровой эпохи [1].

Он не содержит понятия электронных доказательств как самостоятельного источника, не регулирует порядок их собирания, проверки и оценки, не говоря уже о трансграничном обмене цифровыми данными. В результате правоохранительные органы стран Содружества, сталкиваясь с необходимостью получить электронные доказательства от коллег из соседнего государства, вынуждены действовать в условиях правовой неопределённости, полагаясь на архаичные процедуры международной правовой помощи, которые могут занимать месяцы, тогда как цифровые следы исчезают за считанные дни, а иногда и часы.

Масштаб проблемы становится очевидным при обращении к статистике. В 2022 году общее число киберпреступлений, совершённых на территории государств – участников СНГ, по сравнению с 2019 годом увеличилось почти в 2,7 раза, достигнув 538 438 зарегистрированных деяний [2]. При этом, по оценкам аналитиков, количество атак на страны Содружества продолжает расти: во втором квартале 2024 года зафиксировано в 2,6 раза больше атак по сравнению с аналогичным периодом 2023 года, причём почти три четверти из них пришлись на долю России, тогда как Казахстан и Беларусь подверглись 8% и 7% атак соответственно [3]. Наибольшему числу атак подверглись государственные учреждения, промышленность и телекоммуникационный сектор, что свидетельствует о целенаправленном характере киберугроз и их прямой связи с вопросами национальной безопасности [3].

Определённые шаги в направлении сотрудничества предпринимались и ранее. В частности, Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации, подписанное в Минске в 2001 году, заложило основы для взаимодействия, однако на практике оно не заработало в полной мере [4]. Во многом это объясняется тем, что документ носит рамочный характер и не содержит конкретных процессуальных механизмов, обязательных для исполнения. Кроме того, он не учитывает последующих изменений в технологической и правовой среде.

На глобальном уровне аналогичные проблемы пытались решить в рамках Будапештской конвенции о киберпреступности 2001 года, которая стала первым международным договором, направленным на борьбу с компьютерными преступлениями и обеспечение трансграничного доступа к электронным доказательствам [5]. Однако не все государства участники СНГ присоединились к этому документу, а те, кто это сделал, не всегда могут в полной мере реализовать его положения из-за несоответствия национального законодательства. Второй дополнительный протокол к Будапештской конвенции, принятый в 2022 году, расширил возможности для сотрудничества и ускорил процедуры обмена электронными доказательствами, но его потенциал на пространстве Содружества до сих пор остаётся нереализованным [6].

Настоящая статья исходит из гипотезы о том, что сложившееся положение может быть исправлено только путём принятия качественно нового, единого для всех государств участников СНГ Уголовно-процессуального кодекса, который интегрировал бы цифровые доказательства в качестве полноправного источника, закрепил ускоренные и упрощённые процедуры трансграничного розыска и обмена электронной информацией, а также создал институциональный механизм координации усилий правоохранительных органов на пространстве Содружества.

Материалы и методы.

Исследование опирается на широкий круг источников. Прежде всего, это модельные акты Содружества Независимых Государств, в первую очередь Модельный Уголовно-процессуальный кодекс 1996 года с последующими изменениями, а также Модельный Уголовный кодекс, в котором содержится раздел о преступлениях против информационной безопасности. Анализируются национальные уголовно-процессуальные кодексы государств – участников СНГ, в частности Российской Федерации, Республики Беларусь, Республики Казахстан, Республики Узбекистан, Республики Таджикистан, Кыргызской Республики, Республики Армения и Республики Молдова.

Кроме того, привлекаются международно-правовые документы: Будапештская конвенция о киберпреступности 2001 года и её Второй дополнительный протокол, Соглашение о сотрудничестве государств участников СНГ в борьбе с преступлениями в сфере компьютерной информации 2001 года, Концепция сотрудничества государств участников СНГ в сфере противодействия киберпреступности, а также проект новой Конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Методологическую основу работы составляет сравнительно-правовой метод, позволивший выявить как общие черты, так и принципиальные расхождения в подходах к регулированию электронных доказательств в странах Содружества. Формально-юридический метод использован для анализа нормативных текстов и уяснения содержания правовых норм. Метод системного анализа дал возможность рассмотреть проблему в комплексе, увязывая процессуальные, организационные и технические аспекты. Наконец, историко-правовой метод помог проследить эволюцию модельного законодательства СНГ и оценить, насколько оно соответствует современным вызовам.

Результаты.

Проведённый анализ показал, что ни один из национальных уголовно-процессуальных кодексов государств – участников СНГ не содержит развёрнутого и системного регулирования электронных доказательств. В Российской Федерации Уголовно-процессуальный кодекс относит к доказательствам любые сведения, на основе которых устанавливаются обстоятельства дела, однако специальные нормы, посвящённые электронным данным, в нём отсутствуют [7]. Электронные документы чаще всего рассматриваются через призму иных документов или вещественных доказательств, что порождает споры о допустимости и достоверности.

Как отмечается в научной литературе, в российском законодательстве определение электронного доказательства отсутствует, а сама информация, представленная в цифровой форме, может рассматриваться в статусе вещественных доказательств или иных документов в зависимости от её оформления и хранения [8]. Более того, как показывают исследования, цифровое доказательство наиболее уязвимо для нарушения прав именно в тех свойствах, которые слабее всего охвачены досудебным судебным контролем: его процессуальный статус нормативно не определён, а господствующая доктрина относит вопрос допустимости к стадии судебного разбирательства, выводя законность формирования цифрового доказательства за пределы досудебной проверки [9].

В Республике Беларусь Уголовно-процессуальный кодекс признаёт электронный документ доказательством, равным по юридической силе документу на бумажном носителе, однако процедура его собирания и проверки должным образом не детализирована [10]. В Республике Казахстан Уголовно-процессуальный кодекс содержит более современные подходы, включая упоминание электронных носителей информации [11]. В частности, в пункте 15 статьи 7 УПК Республики Казахстан дано понятие электронного документа как документа, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи, а в части 3 статьи 120 к документам, помимо общепринятого понимания, отнесены и электронные документы [12]. Тем не менее целостная система работы с цифровыми доказательствами, особенно в трансграничном контексте, в казахстанском законодательстве также отсутствует. Как справедливо отмечают исследователи, отсутствие конкретных положений в УПК Республики Казахстан затрудняет правовую классификацию цифровых материалов и создаёт риск судебных ошибок [13].

В Республике Узбекистан Уголовно-процессуальный кодекс выделяет материалы звукозаписи, видеозаписи и кинофотосъёмки в отдельный вид доказательств, однако их трансграничная передача никак не регламентирована [14]. При этом, как отмечается в специальных исследованиях, УПК Узбекистана содержит отдельные статьи об электронных данных и цифровых доказательствах, что выгодно отличает его от законодательства ряда других стран Содружества [15]. В Республике Таджикистан Уголовно-процессуальный кодекс включает в перечень источников доказательств скрытые записи, прослушанные и зафиксированные телефонные разговоры, электронные, видео- и аудиозаписи наблюдения, но процессуальный порядок работы с ними остаётся недостаточно детализированным [16]. Согласно части 2 статьи 72 УПК Республики Таджикистан, помимо традиционных видов, доказательствами могут считаться и иные документы, что создаёт правовую основу для признания электронных материалов, однако не решает проблему их процессуального оформления [17]. Таким образом, даже в тех странах, где законодатель сделал шаг вперёд, отсутствует единый понятийный аппарат и унифицированные процедуры, что создаёт препятствия для сотрудничества.

Модельный Уголовно-процессуальный кодекс СНГ также не содержит понятия электронных доказательств. В его перечне источников доказательств значатся показания, заключения эксперта, вещественные доказательства, протоколы следственных и судебных действий и другие документы. Электронная информация упоминается лишь косвенно, в контексте вещественных доказательств, если она содержится на электронных носителях. Как указывается в доктринальных источниках, Модельный УПК не содержит определений понятий «электронный носитель информации» и «электронная информация», хотя данная терминология в нём и применяется [18]. Очевидно, что такой подход не соответствует ни современному уровню развития технологий, ни потребностям правоприменительной практики. Более того, отсутствие единого понятийного аппарата приводит к тому, что электронное доказательство, полученное на территории одного государства, может быть признано

недопустимым в другом из-за формальных различий в процедуре его собирания. В научной литературе обоснованно подчёркивается, что практика обращения с электронными документами на территории стран СНГ показывает их востребованность и необходимость дальнейшего законодательного регулирования правил их использования в уголовном судопроизводстве [19].

Ситуация усугубляется отсутствием эффективного механизма трансграничного обмена цифровыми доказательствами. Действующее Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации во многом повторяет подходы Будапештской конвенции, однако на практике оно не работает в полной мере. В отличие от Будапештской конвенции, которая обязала каждую сторону назначить круглосуточный коммуникационный пункт для незамедлительного содействия в расследованиях, связанных с компьютерными системами и данными, аналогичный механизм в рамках СНГ так и не был создан. Запросы о правовой помощи направляются по дипломатическим каналам, что приводит к значительным задержкам. Между тем электронные следы преступлений носят временный характер: логи серверов могут быть удалены, аккаунты заблокированы, платёжные следы исчезнуть. Как отмечает ректор Московской академии Следственного комитета РФ имени А.Я. Сухарева Алексей Бессонов, необходимо выработать единые международные подходы к срокам хранения цифровых доказательств, поскольку такие данные могут быть утрачены до получения правоохранителями доступа к ним, а законодательством большинства стран для определённой информации предусмотрены ограниченные сроки хранения [20]. Промедление с направлением запроса зачастую означает безвозвратную утрату доказательств. По словам Бессонова, ежегодно раскрывается лишь около 30% киберпреступлений, совершаемых в отношении граждан и объектов критической инфраструктуры, а сложности с получением данных из-за рубежа связаны в том числе с ограниченными сроками хранения информации [20].

Следует отметить, что на политическом уровне необходимость реформ уже осознана. В мае 2025 года заместитель Генерального секретаря СНГ Нурлан Сейтимов объявил о начале работы по определению основ создания межгосударственной информационной системы обмена цифровыми следами преступлений. Эта инициатива, безусловно, заслуживает поддержки, однако она носит преимущественно организационно-технический характер и не решает главной проблемы – отсутствия единой процессуальной основы. Создание базы данных или информационной системы само по себе не устранит правовую неопределённость, связанную с признанием, допустимостью и процессуальным оформлением электронных доказательств. Необходим именно процессуальный кодекс, который установил бы общие для всех участников правила игры. Кроме того, нельзя не учитывать, что в Центральной Азии уже предпринимаются практические шаги в этом направлении: при поддержке ОБСЕ реализуется проект «E-VIDENCE», направленный на улучшение трансграничного доступа к электронным доказательствам для расследования онлайн-преступлений, в рамках которого представители Казахстана, Кыргызстана, Таджикистана, Туркменистана и Узбекистана участвуют в региональных семинарах и учебных курсах [21]. Эти усилия свидетельствуют о том, что потребность в единых механизмах назрела, однако они носят фрагментарный характер и не охватывают всё пространство Содружества.

Обсуждение.

Полученные результаты позволяют утверждать, что принятие единого Уголовно-процессуального кодекса СНГ является не просто желательным, а насущно необходимым шагом. Такой кодекс должен решить несколько взаимосвязанных задач. Прежде всего, необходимо ввести в понятийный аппарат категорию «электронное доказательство» и определить его место в системе источников доказательств. Электронное доказательство не должно растворяться в традиционных видах – вещественных доказательствах или документах.

Это самостоятельный источник, обладающий специфическими свойствами: нематериальной формой, возможностью лёгкого копирования и изменения, зависимостью от технических средств и программного обеспечения. В научной литературе справедливо указывается, что в условиях цифровизации особое внимание должно уделяться процессуальным требованиям, обеспечению подлинности, допустимости и целостности электронных доказательств, а также стандартизации подходов к цифровым данным [22]. Соответственно, должны быть выработаны особые процессуальные требования к собиранию, фиксации, хранению и исследованию электронных доказательств. В частности, необходимо закрепить обязательность указания в протоколе идентифицирующих признаков электронного носителя – серийного номера, объёма памяти, технических характеристик, а также обеспечить неизменность цифровой информации с момента её изъятия до момента исследования в суде. Как обоснованно отмечается в доктрине, основной процессуальный риск концентрируется на стадии изъятия и фиксации цифровых данных, что требует дополнительных гарантий судебного контроля уже на досудебной стадии [9].

Далее, единый кодекс должен установить ускоренные и упрощённые процедуры трансграничного обмена электронными доказательствами. Речь идёт о создании механизма, аналогичного коммуникационным пунктам Будапештской конвенции, но адаптированного к условиям СНГ [5]. Каждое государство – участник должно назначить компетентный орган, доступный круглосуточно и без выходных, уполномоченный принимать и исполнять запросы о предоставлении электронных данных напрямую, минуя длительные дипломатические процедуры. При этом должны быть предусмотрены гарантии защиты прав человека, включая судебный контроль и соблюдение требований о неприкосновенности частной жизни. Опыт Центральной Азии, где при поддержке ОБСЕ реализуется проект по улучшению трансграничного доступа к электронным доказательствам, показывает, что такие механизмы вполне реализуемы при наличии политической воли и соответствующей правовой базы [21].

Второй дополнительный протокол к Будапештской конвенции также подтверждает, что международное сообщество движется в этом направлении, и игнорировать этот тренд было бы ошибкой. Показателен в этом отношении опыт Казахстана: в 2023 году республике было предложено присоединиться к Будапештской конвенции, после чего началась работа по приведению национального законодательства в соответствие с её стандартами, а в октябре 2025 года Казахстан присоединился к Конвенции ООН против киберпреступности, принятой Генеральной Ассамблеей ООН в декабре 2024 года [23]. Как отмечают исследователи, указанные две конвенции дополняют друг друга и предоставляют уникальную возможность создать оперативную и эффективную систему международного сотрудничества в борьбе с киберпреступностью, содействуя трансграничному доступу к электронным доказательствам [23]. Этот пример наглядно демонстрирует, что государства региона готовы к реформам, и единый процессуальный кодекс СНГ мог бы стать логичным продолжением этой работы.

Наконец, единый кодекс должен учредить институциональный механизм координации. Целесообразно создать на базе одного из существующих органов СНГ, например Совета министров внутренних дел или Координационного совета генеральных прокуроров, постоянно действующий координационный центр по вопросам электронных доказательств. Его задачи могли бы включать не только оперативное содействие в исполнении запросов, но и разработку методических рекомендаций, обучение сотрудников, обобщение практики, а также ведение единой базы данных о типовых схемах киберпреступлений и цифровых следах. Подобный центр позволил бы преодолеть ведомственную разобщённость и обеспечить единый подход к борьбе с транснациональной киберпреступностью на всём пространстве Содружества. Как справедливо отмечает Т.В. Прокофьева, совершенствование противодействия киберпреступности на пространстве СНГ невозможно без гармонизации законодательства и создания общих институтов [24].

При этом важно подчеркнуть, что работа должна вестись не только на уровне правоохранительных органов, но и с привлечением экспертного сообщества: в ноябре 2025 года в Ташкенте состоялся региональный семинар для стран Центральной Азии, посвящённый вопросам запроса электронных доказательств из других стран, что свидетельствует о востребованности таких площадок для обмена опытом.

Возможны возражения, связанные с опасениями по поводу утраты национального суверенитета в уголовно-процессуальной сфере. Однако эти опасения представляются необоснованными. Речь не идёт о создании наднационального органа, который подменял бы национальные правоохранительные системы. Единый кодекс – это рамочный документ, устанавливающий минимальные стандарты и общие процедуры, которые государства добровольно принимают на себя, как они уже сделали это в отношении Модельного УПК и множества других модельных актов. Более того, гармонизация процессуального законодательства не только не ущемляет суверенитет, но и укрепляет его, поскольку позволяет государствам более эффективно защищать своих граждан и свою экономику от транснациональных киберугроз. Опыт Европейского союза, где наднациональные механизмы в сфере электронных доказательств успешно сочетаются с национальными процессуальными системами, подтверждает это.

Выводы.

Проведённое исследование позволяет сформулировать следующие выводы. Транснациональная киберпреступность представляет собой вызов, который не может быть эффективно нейтрализован усилиями отдельных государств. Разрозненность уголовно-процессуальных законодательств стран СНГ, отсутствие единого понятия электронных доказательств и неэффективность механизмов трансграничного обмена цифровой информацией создают благоприятную среду для киберпреступников и ставят правоохранительные органы в заведомо проигрышное положение.

Действующий Модельный УПК СНГ 1996 года морально устарел и не соответствует реалиям цифровой эпохи. Принятие нового, единого Уголовно-процессуального кодекса СНГ, интегрирующего электронные доказательства, устанавливающего ускоренные процедуры трансграничного обмена и учреждающего координационный механизм, является необходимым и своевременным шагом. Такой кодекс не подрывает суверенитет государств, а напротив, укрепляет их способность противостоять общим угрозам. Реализация этой инициативы потребует политической воли, согласованных усилий законодателей и правоохранителей, а также учёта лучших международных практик, однако промедление в этом вопросе обходится неизмеримо дороже, чем его возможные издержки.

СПИСОК ЛИТЕРАТУРЫ:

1. Модельный уголовно-процессуальный кодекс для государств — участников СНГ (принят постановлением Межпарламентской Ассамблеи государств — участников СНГ от 17.02.1996) // Информационный бюллетень МПА СНГ. 1996. № 10
2. Надейкина О.А. Проблемные аспекты борьбы с киберпреступностью в государствах — участниках СНГ // Вестник Всероссийского научно-исследовательского института МВД России. 2023. С. 278–288
3. Актуальные киберугрозы в странах СНГ 2023–2024. М.: Positive Technologies, 2024
4. Соглашение о сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации (заключено в г. Минске 01.06.2001)
5. Конвенция о преступности в сфере компьютерной информации (ETS № 185) (заключена в г. Будапеште 23.11.2001)
6. Второй дополнительный протокол к Конвенции о преступности в сфере компьютерной информации, касающийся усиления сотрудничества и раскрытия электронных доказательств (CETS № 224) (заключен в г. Страсбурге 12.05.2022)
7. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (с изм. и доп.)
8. Философия права. 2021. № 4 (99). С. 112–120

9. Абдурахмонов Д.А. Судебный контроль за цифровыми доказательствами на досудебной стадии: опыт уголовного процесса России и Таджикистана для административного производства ЕАЭС // Бизнес, менеджмент и право. 2026. № 2 (70). С. 113–117

10. Уголовно-процессуальный кодекс Республики Беларусь от 16.07.1999 № 295-З

11. Уголовно-процессуальный кодекс Республики Казахстан от 04.07.2014 № 231-V

12. Вестник Института законодательства и правовой информации Республики Казахстан. 2023. № 3. С. 45–52

13. Уголовно-процессуальный кодекс Республики Узбекистан от 22.09.1994 № 2013-XII

14. Уголовно-процессуальный кодекс Республики Таджикистан от 03.12.2009

15. Диссертационное исследование по уголовно-процессуальному праву. С. 137–142

16. Обращение с электронными унифицированными носителями в рамках взаимодействия на пространстве СНГ // Azərbaycan Prokurorluğu Elmi-praktiki jurnalı. 2025. № 1

17. Бессонов предложил выработать механизм быстрого получения данных из-за границы // РАПСИ. 10 июля 2026

18. OSCE supports Central Asian participating States in improving cross-border access to electronic evidence // OSCE. 2025

19. Собиров Ш. Сравнительно-правовой анализ регулирования электронных доказательств в уголовном судопроизводстве: опыт США, ЕС и стран СНГ // Общество и инновации. 2023. Т. 4, № 5. С. 96–117. DOI 10.47689/2181-1415-vol4-iss5-pp96-117

20. В 2023 году Республике Казахстан было предложено присоединиться к Будапештской Конвенции о компьютерных преступлениях // Vestnik of the Institute of Legislation and Legal Information of the Republic of Kazakhstan. 2025. № 1. С. 27–34

21. Прокофьева Т.В. Совершенствование противодействия киберпреступности на пространстве Содружества Независимых Государств // Вестник Московского государственного лингвистического университета. Образование и педагогические науки. 2023. Вып. 4 (849). С. 108–114

Maulenov J.
student
Higher School of Jurisprudence and Forensic Technical Expertise
Peter the Great St. Petersburg Polytechnic University
(St. Petersburg, Russia)

DIGITALIZATION OF TRACING AND EVIDENCE EXCHANGE: NECESSITY OF ADOPTING CIS CRIMINAL PROCEDURE CODE IN ERA OF TRANSNATIONAL CYBERCRIME

Abstract: *the purpose of this study is to substantiate necessity of developing and adopting a unified Criminal Procedure Code of Commonwealth of Independent States as a response to challenges of transnational cybercrime. In conditions of rapid digitalization across all spheres of life, crime is acquiring a pronounced cross-border nature, while electronic evidence is becoming a key means of proof. However, fragmentation of national criminal procedure legislation in CIS member states, absence of unified procedures for collection, storage, and cross-border transfer of digital evidence, as well as slow operation of existing legal assistance mechanisms, make countering cybercrime in CIS area insufficiently effective. Research methodology is based on comparative legal analysis of CIS model legislation, national criminal procedure codes of member states, and international instruments, in particular Budapest Convention on Cybercrime and new draft UN Convention. In addition, formal legal method and system analysis method were applied. Findings show that creation of a unified CIS procedural code, integrating digital evidence as an independent source, establishing expedited procedures for cross-border exchange of electronic data, and instituting a supranational coordination mechanism, will significantly improve efficiency of tracing and evidentiary support in criminal cybercrime cases.*

Practical significance of study lies in possibility of using its conclusions in work of CIS Interparliamentary Assembly, national legislative bodies, and law enforcement agencies when developing and implementing unified procedural norms.

Keywords: *cybercrime, CIS, digitalization, Criminal Procedure Code, digital evidence, cross-border tracing, electronic data exchange, model law, international legal assistance, legal harmonization.*