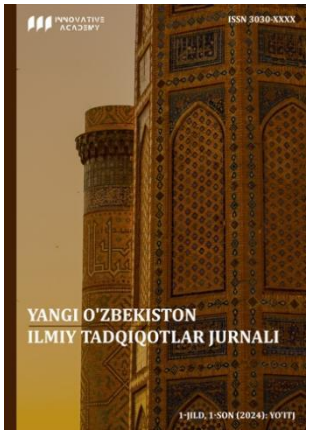

СОВРЕМЕННЫЕ КИБЕРПРЕСТУПЛЕНИЯ В РЕСПУБЛИКЕ УЗБЕКИСТАН: ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ И ПУТИ ИХ РЕШЕНИЯ

Анваров Демирали Тахир угли

Студент 3 курса факультета

«Международное право и сравнительное правоведение»

Ташкентского государственного юридического университета

e-mail: anvarovdemirali@gmail.com

https://doi.org/10.5281/zenodo.21599894

ARTICLE INFO

Qabul qilindi: 12-iyul 2026 yil
Ma'qullandi: 15-iyul 2026 yil
Nashr qilindi: 26-iyul 2026 yil

KEY WORDS

киберпреступность, преступления в сфере информационных технологий, кибербезопасность, мошенничество с использованием информационно-коммуникационных технологий, персональные данные, цифровые доказательства, международное сотрудничество, Республика Узбекистан.

ABSTRACT

Настоящая статья посвящена комплексному анализу национального законодательства Республики Узбекистан в сфере противодействия киберпреступности. Автор последовательно раскрывает уголовно-правовую квалификацию преступлений в сфере информационных технологий, институциональную систему их предупреждения, процессуальный алгоритм расследования подобных деяний — от регистрации обращения до международного сотрудничества по уголовным делам с иностранным элементом, — а также специфические составы мошенничества, совершаемого с использованием информационно-коммуникационных технологий, и вопросы защиты персональных данных как превентивного элемента системы противодействия киберпреступности. На каждом из указанных направлений выявляются практические проблемы правоприменения, приводятся реальные примеры из отечественной практики и официальной статистики, а также формулируются авторские предложения по совершенствованию законодательства. Отдельное внимание уделено присоединению Узбекистана к Конвенции Организации Объединённых Наций против киберпреступности 2024 года и сравнительно-правовому анализу опыта Российской Федерации.

Введение

Стремительная цифровизация общественных отношений — от повсеместного распространения мобильного банкинга до перевода значительной части государственных услуг в электронный формат — закономерно сопровождается ростом

преступности, совершаемой с использованием информационно-коммуникационных технологий. Данная тенденция носит не сугубо технический, а глубоко правовой характер, поскольку требует от законодателя постоянного переосмысления традиционных уголовно-правовых конструкций применительно к общественно опасным деяниям, чья специфика заключается в виртуальной, зачастую трансграничной природе преступного посягательства.

Актуальность настоящего исследования подтверждается официальной статистикой: по данным Центра кибербезопасности при Министерстве цифровых технологий Республики Узбекистан, в 2024 году было зафиксировано свыше 12 миллionов попыток кибератак, тогда как годом ранее данный показатель составлял 11 миллионов, а количество обращений граждан по фактам мошенничества выросло на 34 процента по сравнению с предыдущим годом, при этом около 35 процентов всех подобных обращений связано с мошенничеством с использованием платёжных карт [23]. Данная динамика была прямо отмечена и на высшем государственном уровне: в марте 2026 года Президент Республики Узбекистан Шавкат Мирзиёев, ознакомившись с презентацией по мерам предотвращения преступлений и обеспечению верховенства закона, указал на киберпреступность как на одну из наиболее актуальных проблем современности [15].

Дополнительную актуальность теме придаёт и международно-правовой контекст: 27 октября 2025 года в Ханое Республика Узбекистан в числе более чем семидесяти государств подписала Конвенцию Организации Объединённых Наций против киберпреступности, принятую резолюцией Генеральной Ассамблеи ООН от 24 декабря 2024 года и ставшую первым в истории универсальным международным договором в данной сфере [16, 31], что ставит перед отечественной юридической наукой задачу осмысления перспектив её последующей ратификации и имплементации в национальное законодательство.

Целью настоящей статьи является последовательный анализ национальной системы правового противодействия киберпреступности в Узбекистане — от уголовно-правовой квалификации соответствующих деяний до процессуального алгоритма их расследования и международного сотрудничества, — с выявлением практических проблем на каждом из данных направлений и формулированием предложений по их устранению. Как и в наших предыдущих исследованиях, мы придерживаемся методологического принципа, согласно которому проблемы и предложения не выносятся в отдельные главы, а последовательно раскрываются в рамках той тематической главы, к которой они относятся.

Понятие и виды киберпреступлений: доктринальные подходы и уголовно-правовая квалификация

Прежде чем переходить к анализу отдельных механизмов противодействия, необходимо остановиться на понятийном аппарате темы, поскольку в отечественной и зарубежной доктрине уголовного права термины «компьютерное преступление» и «киберпреступление» нередко используются как синонимы, хотя, на наш взгляд, между ними существует содержательное различие. Понятие «компьютерное преступление» исторически формировалось применительно к посягательствам на сам компьютер и содержащуюся в нём информацию как на непосредственный объект посягательства, тогда как понятие «киберпреступление» — более широкое и охватывает также деяния, при совершении которых информационно-коммуникационные технологии выступают не объектом, а лишь орудием или средством совершения иного преступления (например, хищения, вымогательства или

распространения экстремистских материалов) [39, 38]. Мы полагаем, что данное разграничение имеет не только доктринальное, но и практическое значение, поскольку оно напрямую влияет на структуру уголовного законодательства: должны ли подобные деяния составлять единую, самостоятельную главу Уголовного кодекса, либо же квалифицирующий признак «с использованием информационно-коммуникационных технологий» должен быть интегрирован в традиционные составы преступлений против собственности, чести и достоинства личности, общественной безопасности.

Законодатель Узбекистана в данном вопросе избрал путь выделения самостоятельной главы: Глава XX-1 Уголовного кодекса «Преступления в сфере информационных технологий» объединяет составы, ориентированные преимущественно на защиту компьютерной информации и информационных систем как таковых, — статью 278-1 (нарушение правил информатизации), статью 278-2 (незаконный, несанкционированный доступ к компьютерной информации), статью 278-3 (изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного доступа к компьютерной системе, а также к сетям телекоммуникаций), статью 278-4 (модификация компьютерной информации) и статью 278-5 (компьютерный саботаж) [2]. Одновременно Уголовный кодекс Узбекистана предусматривает и самостоятельную меру наказания — запрет на использование средств связи, в том числе сети Интернет, в качестве составного элемента ограничения свободы [26], что, на наш взгляд, отражает осознание законодателем специфической, «инструментальной» роли информационно-коммуникационных технологий в современной преступности в целом, выходящей за рамки собственно Главы XX-1.

Вместе с тем, на наш взгляд, избранная законодателем модель порождает практическую проблему пограничной квалификации: значительная часть наиболее массовых, статистически преобладающих киберпреступлений — прежде всего мошенничество, совершаемое с использованием методов социальной инженерии, — формально не подпадает под составы Главы XX-1, поскольку не образует непосредственного посягательства на компьютерную информацию как таковую, а квалифицируется по общей норме о мошенничестве (статья 168 Уголовного кодекса), что создаёт риск недооценки специфической общественной опасности подобных деяний и затрудняет ведение сопоставимой, единообразной статистики киберпреступности в узком и широком смысле данного понятия. К данной проблеме — квалификации мошенничества, совершаемого с использованием информационно-коммуникационных технологий, — мы обратимся отдельно после рассмотрения институциональной системы противодействия киберпреступности в целом.

Институциональной и организационно-правовой основой государственной системы противодействия киберугрозам выступает Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года № ЗРУ-764, принятый Законодательной палатой 25 февраля и одобренный Сенатом 17 марта 2022 года и состоящий из 8 глав и 40 статей [5, 28]. Закон определяет кибербезопасность как состояние защищённости интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве [5] и закрепляет полномочия уполномоченного государственного органа — Центра кибербезопасности, — который обязан принимать меры по предупреждению, выявлению и предотвращению киберпреступлений, вести регистрацию обращений и сведений о киберпреступлениях и правонарушениях, представляющих угрозу кибербезопасности, а также своевременно принимать по ним меры в установленном законодательством порядке [5].

Показательной с точки зрения обеспечения дополнительных процессуальных и надзорных гарантий является закреплённая Законом обязанность уполномоченного органа уведомлять в письменной форме прокурора в течение двадцати четырёх часов обо всех случаях осуществления его сотрудниками определённых, затрагивающих права граждан действий [5]. Мы оцениваем данную норму как обоснованный компромисс между необходимостью оперативного реагирования специализированного органа на киберугрозы и конституционным требованием прокурорского надзора за деятельностью, потенциально затрагивающей права и свободы личности, — модель, которая, на наш взгляд, заслуживает изучения и в контексте иных направлений оперативно-розыскной деятельности.

Вместе с тем, на наш взгляд, само по себе создание специализированного органа не устраняет структурной проблемы, присущей противодействию киберпреступности практически во всех государствах, — проблемы эффективной координации между органом технического реагирования на киберинциденты (Центром кибербезопасности) и органами предварительного следствия и дознания, обладающими собственно уголовно-процессуальными полномочиями по возбуждению уголовного дела и производству следственных действий. Технический характер деятельности Центра — фиксация факта кибератаки, определение её источника и масштаба — объективно требует специальных познаний, которыми следователь общей юрисдикции, как правило, не обладает в достаточной мере, тогда как процессуальное оформление добытых Центром сведений в качестве допустимых доказательств по уголовному делу требует специальных процессуальных познаний, которыми, в свою очередь, не всегда в достаточной мере обладают технические специалисты Центра.

Мы полагаем, что решение данной проблемы лежит в плоскости институционализации постоянно действующих совместных следственно-технических групп, а также разработки детализированного межведомственного регламента взаимодействия Центра кибербезопасности с органами внутренних дел и прокуратуры, закрепляющего не только общие обязанности по уведомлению и регистрации обращений, но и конкретные процессуальные стандарты фиксации технических следов кибератаки, обеспечивающие их последующую допустимость в качестве доказательств. Данный тезис приобретает особое значение применительно к процессуальным аспектам расследования, к детальному анализу которых мы обратимся ниже, однако прежде необходимо остановиться на квалификации наиболее массового, статистически преобладающего вида киберпреступлений — мошенничества с использованием информационно-коммуникационных технологий.

Мошенничество с использованием информационно-коммуникационных технологий: проблемы квалификации и предупреждения

Как отмечалось во введении, около 35 процентов всех обращений граждан по фактам мошенничества, зарегистрированных Центром кибербезопасности, связаны именно с мошенничеством с использованием платёжных карт [23], что делает данную категорию деяний наиболее массовой и социально резонансной формой киберпреступности в Узбекистане. Не раскрывая, разумеется, каких-либо технических деталей конкретных мошеннических схем — поскольку подобное раскрытие противоречило бы самим целям настоящего исследования, — на общем, доктринальном уровне необходимо отметить, что подавляющее большинство подобных посягательств строится не на техническом взломе защищённых систем в смысле статьи 278-2 Уголовного кодекса, а на методах социальной инженерии — психологическом манипулировании потерпевшим с целью добровольной передачи им

конфиденциальных данных или совершения им самим распорядительных действий в отношении собственных денежных средств.

На наш взгляд, именно данная особенность способа совершения — отсутствие несанкционированного технического доступа к охраняемой компьютерной информации в узком смысле — образует ключевую доктринальную и практическую сложность квалификации: с точки зрения буквального содержания составов Главы XX-1 подобные деяния зачастую не образуют самостоятельного «компьютерного» преступления, а квалифицируются по общей норме о мошенничестве (статья 168 Уголовного кодекса), информационно-коммуникационные технологии же учитываются судом лишь в рамках назначения наказания либо, при наличии соответствующей квалифицирующей конструкции, как способ совершения преступления. Мы полагаем, что подобная модель влечёт как минимум два практических следствия. Во-первых, она затрудняет формирование единой, сопоставимой статистики киберпреступности, поскольку значительная часть фактически «цифровых» посягательств учитывается в общей статистике имущественных преступлений, а не в специализированной статистике преступлений в сфере информационных технологий. Во-вторых, она потенциально недооценивает специфическую общественную опасность подобных деяний, связанную с их масштабируемостью — способностью злоумышленника посредством единого организационного механизма посягать одновременно на неопределённо широкий круг потерпевших, что структурно отличает подобные посягательства от традиционного, «единичного» мошенничества.

Учитывая изложенное, мы считаем целесообразным дополнение статьи 168 Уголовного кодекса самостоятельным квалифицирующим признаком — совершение мошенничества с использованием информационно-коммуникационных технологий, — предусматривающим повышенную санкцию по сравнению с базовым составом, по аналогии с уже применяемым в Уголовном кодексе Узбекистана подходом к дифференциации ответственности в зависимости от способа совершения имущественных преступлений. Одновременно мы полагаем необходимым закрепление на уровне подзаконного, ведомственного акта единой методики статистического учёта преступлений, совершённых с использованием информационно-коммуникационных технологий, независимо от того, по какой именно статье Уголовного кодекса они формально квалифицированы, — поскольку без подобной единой методики содержательный анализ реальной динамики киберпреступности в широком смысле объективно затруднён.

Значительная часть мошеннических схем, использующих методы социальной инженерии, строится на предварительно полученных злоумышленниками персональных данных потенциальных потерпевших, что придаёт институту защиты персональных данных самостоятельное профилактическое, а не только собственно правозащитное значение в общей системе противодействия киберпреступности, — к анализу которого мы и переходим.

Защита персональных данных как превентивный элемент системы противодействия киберпреступности

Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года № ЗРУ-547 определяет персональные данные как зафиксированную на электронном, бумажном или ином материальном носителе информацию, относящуюся к определённому физическому лицу или дающую возможность его идентификации [6], и закрепляет за государством функцию гарантирования защиты подобных данных [6].

Одной из наиболее дискуссионных особенностей узбекистанской модели правового регулирования выступает требование локализации — обязательного хранения баз персональных данных граждан Республики Узбекистан на серверах, физически расположенных на территории страны.

Практическим примером применения данного требования, получившим широкий общественный резонанс, стало временное ограничение доступа к платформе TikTok на территории Узбекистана в 2021 году в связи с непредоставлением оператором платформы подтверждения соблюдения требований законодательства о локализации персональных данных. На наш взгляд, данный случай наглядно демонстрирует фундаментальное структурное напряжение, присущее институту локализации персональных данных в целом, — между легитимной целью обеспечения национального суверенного контроля за оборотом персональных данных граждан (что объективно облегчает как надзор со стороны уполномоченных органов, так и последующее процессуальное получение подобных данных для целей расследования киберпреступлений) и рисками для развития цифровой экономики и доступности глобальных цифровых сервисов для населения.

Сопоставление узбекистанской модели с европейским Общим регламентом по защите данных (GDPR), который, обеспечивая высокий уровень защиты персональных данных граждан Европейского союза, тем не менее не устанавливает императивного требования территориальной локализации данных, а опирается на систему адекватности защиты в стране назначения передачи данных и договорных механизмов подобной передачи, показывает, что существуют и менее ограничительные с точки зрения трансграничного цифрового оборота модели достижения сопоставимого уровня защиты персональных данных. Вместе с тем мы полагаем, что для государства, находящегося на сравнительно ранней стадии выстраивания собственной институциональной системы противодействия киберпреступности, — в отличие от государств Европейского союза с их развитой системой взаимного признания и трансграничного правоприменения, — требование локализации выполняет важную дополнительную функцию: оно существенно упрощает процессуальное получение national правоохранительными органами доступа к данным в рамках расследования киберпреступлений, избавляя от необходимости обращения за международной правовой помощью применительно к данным, физически хранящимся за рубежом.

На наш взгляд, оптимальным направлением дальнейшего развития данного института является не отказ от требования локализации как такового, а его дифференциация в зависимости от категории и чувствительности персональных данных — с сохранением императивного требования локализации применительно к наиболее чувствительным категориям данных (биометрическим, финансовым, данным о здоровье) и одновременным смягчением данного требования применительно к иным категориям данных при условии предоставления оператором данных достаточных гарантий их защиты, — подход, позволяющий сбалансировать интересы кибербезопасности и развития цифровой экономики без полного отказа от национального суверенного контроля.

Собранные и защищённые в соответствии с рассмотренными выше требованиями данные приобретают процессуальное значение доказательств именно на стадии расследования конкретного киберпреступления — стадии, чей процедурный алгоритм и присущие ему специфические проблемы заслуживают отдельного, углублённого анализа.

Процессуальный алгоритм расследования киберпреступлений и проблема цифровых доказательств

Расследование киберпреступления, в отличие от расследования традиционного, «физического» преступления, обладает рядом принципиальных процедурных особенностей на каждой из последовательных стадий. Первая стадия — регистрация обращения потерпевшего или получение Центром кибербезопасности сведений о киберинциденте в порядке, установленном Законом о кибербезопасности [5], — сталкивается с проблемой позднего обращения потерпевших, вызванного, как правило, недостаточной цифровой грамотностью населения и — применительно к мошенничеству — субъективным ощущением стыда за собственную доверчивость, что объективно снижает шансы на своевременное процессуальное закрепление технических следов преступления, обладающих, как будет показано ниже, повышенной волатильностью.

Вторая стадия — собственно процессуальная фиксация цифровых доказательств — образует, на наш взгляд, наиболее методологически сложное звено всего алгоритма. Цифровые доказательства (логи серверов, метаданные электронных сообщений, записи транзакций) принципиально отличаются от традиционных вещественных доказательств повышенной волатильностью — способностью быть безвозвратно утраченными или изменёнными в результате самого обычного функционирования информационной системы в течение относительно короткого промежутка времени, — что предъявляет повышенные требования к оперативности процессуального реагирования следователя и, соответственно, к его специальной технической подготовке. Мы полагаем, что именно на данной стадии наиболее остро проявляется отмеченная нами выше проблема недостаточной институциональной координации между техническими специалистами Центра кибербезопасности и следственными органами: промедление, вызванное необходимостью получения судебного решения или направления запроса оператору связи в отсутствие налаженного оперативного механизма взаимодействия, способно привести к безвозвратной утрате ключевых цифровых следов преступления.

Третья, завершающая стадия алгоритма — направление, при необходимости, запроса о правовой помощи иностранному государству — приобретает особое значение ввиду принципиально трансграничной природы значительной части киберпреступлений: серверы, использованные злоумышленником, могут физически находиться на территории иностранного государства, равно как и сам злоумышленник может действовать из-за рубежа. Традиционный механизм международной правовой помощи по уголовным делам, построенный на двусторонних договорах и относительно медленной, формализованной процедуре дипломатических или центральных органов, объективно не отвечает требованиям оперативности, продиктованным упомянутой выше волатильностью цифровых доказательств: пока формализованный международный запрос дойдёт до исполнения, ключевые цифровые следы преступления с высокой вероятностью окажутся утраченными.

Именно данная проблема образует главный содержательный контекст значимости подписанной Узбекистаном в Ханое 27 октября 2025 года Конвенции Организации Объединённых Наций против киберпреступности, разработка которой заняла у государств — членов ООН порядка пяти лет и которая была принята резолюцией Генеральной Ассамблеи от 24 декабря 2024 года [16]. Согласно официальному наименованию, Конвенция направлена на укрепление международного сотрудничества в борьбе с определёнными преступлениями, совершаемыми с

использованием информационно-коммуникационных систем, и на обмен доказательствами в электронной форме, относящимися к серьёзным преступлениям [17] — то есть, по существу, на решение именно той проблемы оперативности трансграничного получения цифровых доказательств, которая была выявлена нами выше. Примечательно, что инициатива разработки данной Конвенции принадлежала Российской Федерации, выступившей с соответствующим предложением ещё в 2019 году [48], тогда как ряд государств, включая США и часть государств Европейского союза, проголосовали против её принятия на Генеральной Ассамблее в декабре 2024 года [32], что, на наш взгляд, отражает существующие в мировом сообществе объективные разногласия относительно баланса между эффективностью международного сотрудничества по киберпреступлениям и опасениями за возможное расширительное использование механизмов Конвенции для целей, выходящих за рамки собственно борьбы с киберпреступностью.

Мы полагаем, что подписание Конвенции образует лишь первый шаг, и последующая ратификация должна сопровождаться содержательной имплементационной работой — приведением норм Уголовно-процессуального кодекса Узбекистана, регулирующих порядок направления и исполнения международных следственных поручений, в соответствие с предусмотренными Конвенцией упрощёнными, ускоренными механизмами трансграничного получения электронных доказательств, включая институт оперативного сохранения (предварительной консервации) хранящихся за рубежом компьютерных данных до поступления формального запроса о правовой помощи, — механизм, который, на наш взгляд, представляет собой наиболее практически ценное нововведение современного международного регулирования в данной сфере, поскольку он позволяет разрешить фундаментальное противоречие между волатильностью цифровых доказательств и неизбежной длительностью формализованной процедуры международной правовой помощи.

Наряду с имущественными и связанными с данными киберпреступлениями, самостоятельную группу общественно опасных деяний, совершаемых посредством информационно-коммуникационных технологий, образуют преступления экстремистской направленности, правовое регулирование которых заслуживает отдельного рассмотрения.

Киберэкстремизм и вопросы информационной безопасности несовершеннолетних

Кабулов и Анорбоев, посвятившие специальное исследование уголовно-правовым аспектам совершения экстремистских преступлений посредством информационно-коммуникационных технологий, обоснованно указывают, что стремительное распространение социальных сетей и мессенджеров качественно изменило механизм вовлечения лиц, прежде всего несовершеннолетних, в экстремистскую деятельность — от традиционного личного контакта к анонимному, массовому и трансграничному распространению экстремистского контента [33]. Мы полностью разделяем данную оценку и полагаем, что специфика киберэкстремизма как разновидности киберпреступности заключается именно в том, что информационно-коммуникационные технологии здесь выступают не орудием непосредственного причинения имущественного вреда (как при мошенничестве), а инструментом идеологического воздействия, что предъявляет качественно иные требования к методам его предупреждения — прежде всего к развитию медиаграмотности и критического мышления как самостоятельного элемента государственной образовательной политики, а не только к традиционным уголовно-правовым и техническим мерам блокировки соответствующего контента.

На наш взгляд, применительно к несовершеннолетним данная проблематика приобретает особую остроту, поскольку именно данная возрастная категория объективно наиболее подвержена как манипулятивному воздействию экстремистского контента, так и рискам мошенничества и иных форм киберпреступности ввиду объективно меньшего жизненного опыта и критического восприятия информации. Мы считаем целесообразным системное включение курса цифровой гигиены и основ информационной безопасности в образовательные программы общеобразовательных учреждений Узбекистана — не в качестве факультативного, а в качестве обязательного компонента, — поскольку долгосрочная профилактическая эффективность подобной образовательной меры, на наш взгляд, существенно превышает эффективность исключительно репрессивных, постфактум применяемых уголовно-правовых мер.

Сопоставление узбекистанской модели уголовно-правового регулирования киберпреступности с законодательством Российской Федерации обнаруживает значительное структурное сходство, объясняемое общими историческими корнями национальных уголовно-правовых систем: Глава 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации» так же, как и Глава XX-1 Уголовного кодекса Узбекистана, построена на модели самостоятельных составов, ориентированных на защиту компьютерной информации как таковой (неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ, нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации), тогда как мошенничество, совершаемое с использованием информационно-коммуникационных технологий, квалифицируется по специальной норме о мошенничестве в сфере компьютерной информации, отдельно выделенной законодателем в общей главе о преступлениях против собственности.

Мы полагаем, что именно данное российское решение — выделение самостоятельного, специализированного состава мошенничества в сфере компьютерной информации, а не квалификация подобных деяний по общей норме о мошенничестве, — заслуживает внимания узбекистанского законодателя в контексте сформулированного нами выше предложения о введении соответствующего квалифицирующего признака в статью 168 Уголовного кодекса Узбекистана, поскольку российский опыт демонстрирует практическую состоятельность подобной модели дифференциации ответственности применительно именно к мошенничеству, совершаемому посредством информационно-коммуникационных технологий.

Что касается международно-правового измерения, необходимо отметить, что ни Узбекистан, ни Россия не являются участниками принятой в 2001 году Конвенции Совета Европы о преступности в сфере компьютерной информации (Будапештской конвенции) — старейшего и наиболее детально проработанного на сегодняшний день регионального договора в данной сфере, — что во многом и предопределило описанную выше инициативу разработки альтернативного, подлинно универсального договора в рамках Организации Объединённых Наций. На наш взгляд, факт подписания Узбекистаном именно универсальной Конвенции ООН, а не присоединения к региональной Будапештской конвенции, geopolitически и институционально более последователен для Узбекистана как участника евразийского и центральноазиатского пространства международного сотрудничества, что, впрочем, не исключает целесообразности последующего изучения отдельных детально проработанных процессуальных механизмов Будапештской конвенции — в частности, механизма оперативного трансграничного сохранения компьютерных данных — в целях их

адаптации к национальному законодательству Узбекистана в процессе имплементации Конвенции ООН.

Заключение

Проведённое исследование позволяет сформулировать следующие основные выводы.

Во-первых, система уголовно-правового регулирования киберпреступности в Республике Узбекистан построена на модели самостоятельной, специализированной главы Уголовного кодекса, ориентированной преимущественно на защиту компьютерной информации и информационных систем как таковых, что, однако, порождает проблему пограничной квалификации наиболее массовой категории киберпреступлений — мошенничества, совершаемого методами социальной инженерии, — формально не подпадающего под данную главу.

Во-вторых, институциональная система противодействия киберпреступности, организационно-правовой основой которой выступает Закон «О кибербезопасности» 2022 года и созданный на его основании Центр кибербезопасности, нуждается в дальнейшем развитии механизмов оперативной координации с органами предварительного расследования, что приобретает особую значимость ввиду повышенной волатильности цифровых доказательств.

В-третьих, институт защиты персональных данных, включая дискуссионное требование их территориальной локализации — практическое применение которого было наглядно продемонстрировано случаем временного ограничения доступа к платформе TikTok в 2021 году, — выполняет самостоятельную превентивную функцию в общей системе противодействия киберпреступности, требуя, однако, более дифференцированного, соразмерного подхода в зависимости от категории защищаемых данных.

В-четвёртых, подписание Узбекистаном в октябре 2025 года Конвенции Организации Объединённых Наций против киберпреступности открывает значимые перспективы совершенствования механизмов трансграничного получения электронных доказательств, реализация которых, однако, требует последовательной имплементационной работы на уровне национального уголовно-процессуального законодательства.

В-пятых, на наш взгляд, сформулированные в настоящей статье предложения — введение квалифицирующего признака совершения мошенничества с использованием информационно-коммуникационных технологий, институционализация совместных следственно-технических групп, дифференциация требования локализации персональных данных в зависимости от их чувствительности, скорейшая ратификация и содержательная имплементация Конвенции ООН против киберпреступности, включая институт оперативного сохранения компьютерных данных, а также включение курса цифровой гигиены в обязательные образовательные программы — заслуживают дальнейшей научной разработки и практической апробации.

В заключение отметим, что эффективное противодействие киберпреступности в современных условиях объективно невозможно исключительно репрессивными уголовно-правовыми средствами и требует сбалансированного сочетания уголовно-правовой, процессуальной, институциональной, образовательной и международно-правовой составляющих. Дальнейшее совершенствование рассмотренной нами системы — при последовательном учёте как национальной правовой традиции, так и

новейших международных стандартов — представляет собой значимую и практически востребованную задачу современной узбекистанской юридической науки.

Список использованной литературы:

1. Конституция Республики Узбекистан (в редакции 2023 г.).

2. Уголовный кодекс Республики Узбекистан, утверждён Законом Республики Узбекистан от 22 сентября 1994 г. № 2012-XII (глава XX-1 «Преступления в сфере информационных технологий», статьи 278-1 – 278-5).

3. Уголовно-процессуальный кодекс Республики Узбекистан.

4. Кодекс Республики Узбекистан об административной ответственности.

5. Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 г. № ЗРУ-764.

6. Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 г. № ЗРУ-547.

7. Закон Республики Узбекистан «Об информатизации» от 11 декабря 2003 г. № 560-II.

8. Закон Республики Узбекистан «Об электронной коммерции» от 22 мая 2015 г. № ЗРУ-385.

9. Закон Республики Узбекистан «Об электронном документообороте» от 29 апреля 2004 г. № 611-II.

10. Закон Республики Узбекистан «Об электронной цифровой подписи» от 11 декабря 2003 г. № 562-II.

11. Закон Республики Узбекистан «О противодействии легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения».

12. Закон Республики Узбекистан «О защите детей от информации, наносящей вред их здоровью и развитию» (проектные и действующие нормы в составе законодательства об информатизации).

13. Постановление Кабинета Министров Республики Узбекистан «Об утверждении Положения о Государственном реестре баз персональных данных» от 8 февраля 2020 г. № 71.

14. Постановление Кабинета Министров Республики Узбекистан «Об утверждении некоторых нормативно-правовых актов в области обработки персональных данных» от 5 октября 2022 г.

15. Официальные материалы пресс-службы Президента Республики Узбекистан о мерах противодействия преступности, март 2026 г.

16. Конвенция Организации Объединённых Наций против киберпреступности. Принята резолюцией Генеральной Ассамблеи ООН 79/243 от 24 декабря 2024 г.

17. Организация Объединённых Наций. Конвенция Организации Объединённых Наций против киберпреступности: официальный текст. URL: un.org/ru/documents/treaty/A-RES-79-243

18. Конвенция Совета Европы о преступности в сфере компьютерной информации (Будапештская конвенция). – Будапешт, 23 ноября 2001 г.

19. Уголовный кодекс Российской Федерации, глава 28 «Преступления в сфере компьютерной информации».

20. Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных (GDPR).

21. Конвенция ООН о правах ребёнка. – Нью-Йорк, 1989 г.

22. Центр кибербезопасности при Министерстве цифровых технологий Республики Узбекистан. Официальный сайт. URL: csec.uz

23. Kun.uz. В Узбекистане за год совершено свыше 12 млн кибератак, 3 февраля 2025 г.

24. Институт законодательства и правовой политики при Президенте Республики Узбекистан. Правовая политика в условиях цифровых вызовов: стратегия противодействия киберпреступности. URL: illp.uz

25. Институт законодательства и правовой политики при Президенте Республики Узбекистан. Перспективы правовой политики в области противодействия киберпреступности в Узбекистане. URL: illp.uz

26. UzA.uz. Уголовно-правовая ответственность за преступления против информационной безопасности.

27. Anhor.uz. Безопасность персональных данных в Узбекистане: текущее состояние и перспективы.

28. NORMA.UZ. Принят Закон «О кибербезопасности».

29. NRM.uz. Закон Республики Узбекистан от 15.04.2022 г. № ЗРУ-764 «О кибербезопасности».

30. Lex.uz. Национальная база данных законодательства Республики Узбекистан.

31. Oxu.az. Принята Конвенция ООН против киберпреступности.

32. РБК. В ООН началось подписание Конвенции против киберпреступности, октябрь 2025 г.

33. Кабулов Р., Анорбоев А. Уголовно-правовые аспекты совершения преступления в виде экстремизма через информационно-коммуникационные технологии // Противодействие правонарушениям в сфере цифровых технологий и вопросы организационно-правового обеспечения информационной безопасности. – 2022. – № 01.

34. Русскевич Е.А. Уголовно-правовое воздействие на преступность в сфере компьютерной информации: теоретико-прикладное исследование. – М.: Проспект.

35. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: Юрлитинформ.

36. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт. – М.: Норма.

37. Ефремова М.А. Уголовно-правовая охрана информационной безопасности. – М.: Юрлитинформ.

38. Айсанов Р.М. Компьютерная информация как предмет и средство совершения преступления. – М.: Юрлитинформ.

39. Дремлюга Р.И. Интернет-преступность: монография. – Владивосток: Издательство Дальневосточного университета.

40. Саидов А.Х. Права человека. – Ташкент: Konsauditinform, 2011.

41. Богуславский М.М. Международное частное право: учебник. – М.: Норма.

42. Ryskiyeva.com. Защита персональных данных в Узбекистане: обзор законодательства.

43. Gov.uz. Информация о защите персональных данных.

44. Regulation.gov.uz. О внесении изменения и дополнений в некоторые законодательные акты Республики Узбекистан (в части противодействия киберпреступности).

45. InfoCOM.UZ. Борьба с киберпреступностью – актуальная задача.

46. Cyclowiki.org. Конвенция ООН против киберпреступности.

47. CGITC.ru. В ООН принята Конвенция по борьбе с киберпреступностью.

48. NP.kz. Более 70 государств подписали Конвенцию ООН против киберпреступности.

49. CyberLeninka.ru. Формирование международно-правовой системы противодействия киберпреступности: от терминологии до проекта универсальной конвенции.

50. Толеубекова Б.Х. Компьютерная преступность: криминологические и уголовно-правовые проблемы. – Алматы: Жеті жарғы.

51. Комментарий к Уголовному кодексу Республики Узбекистан (главы о преступлениях в сфере информационных технологий) / отв. ред. коллектив авторов. – Ташкент: Adolat.

52. Батурин Ю.М. Проблемы компьютерного права. – М.: Юридическая литература.