# ЮРИДИЧЕСКИЕ ВОПРОСЫ ИНТЕГРАЦИИ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОЕ ПРОЦЕССУАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО КЫРГЫЗСКОЙ РЕСПУБЛИКИ

Талант Султанов
Джанарбек Мураканов
Айпери Бозоева
Жамиля Акматбаева
Нурбек Арзымбаев

Бишкек – 2023

Выражаем огромную благодарность Фонду «Сорос-Кыргызстан» (ФСК) за поддержку в проведении данного исследования.

Отчет создан в рамках проекта Tech4Society, реализуемого ОФ «Кыргызское отделение интернет-общества ISOC Kyrgyzstan Chapter» при поддержке Фонда «СоросКыргызстан». Данный материал доступен для свободного копирования, переработки и распространения на любом носителе и в любом формате с обязательным указанием имени автора, для любых целей.

Мнения, выраженные в материале, необязательно отражают точку зрения Фонда «Сорос-Кыргызстан».

**ОГЛАВЛЕНИЕ**


1. ВВЕДЕНИЕ ..... 4
2. ПОНЯТИЕ И ПРАВОВАЯ ПРИРОДА ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ ..... 8
   - 2.1. Понятие цифрового доказательства ..... 8
   - 2.2. Юридически значимые особенности цифровых доказательств ..... 11
   - 2.3. Общепризнанные стандарты использования цифровых доказательств ..... 12
3. АНАЛИЗ ДЕЙСТВУЮЩЕГО ЗАКОНОДАТЕЛЬСТВА И ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ ПО ВОПРОСАМ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ ..... 15
   - 3.1. Общая характеристика законодательства Кыргызской Республики по вопросам использования цифровых доказательств в системе правосудия ..... 15
   - 3.2. Обзор уголовно-процессуального законодательства Кыргызской Республики в контексте сбора и использования цифровых доказательств ..... 18
   - 3.3. Особенности использования цифровой информации в качестве доказательства по уголовным делам ..... 21
4. ПРИМЕНЕНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ К РАБОТЕ С ЦИФРОВЫМИ ДОКАЗАТЕЛЬСТВАМИ 40
   - 4.1. Участие специалиста в работе с цифровыми доказательствами ..... 40
   - 4.2. Участие эксперта в работе с цифровыми доказательствами ..... 42
5. ЮРИДИЧЕСКИЕ ВОПРОСЫ ИНТЕГРАЦИИ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОЕ ПРОЦЕССУАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО КЫРГЫЗСКОЙ РЕСПУБЛИКИ ..... 52
   - 5.1. Принципиальные вопросы интеграции цифровых доказательств в уголовное процессуальное законодательство Кыргызской Республики ..... 52
   - 5.2. Механизм интеграции цифровых доказательств в уголовное процессуальное законодательство Кыргызской Республики ..... 57
6. ПРИЛОЖЕНИЯ ..... 60
   - 6.1. Проект Закона Кыргызской Республики «О внесении изменения в Уголовно-процессуальный кодекс Кыргызской Республики» ..... 60
   - 6.2. Проект Правил идентификации, сбора, получения, хранения и исследования цифровой информации в уголовном судопроизводстве ..... 60

# 1. ВВЕДЕНИЕ

Киберпреступность как криминальное применение возможностей компьютерной и сетевой инфраструктуры против интересов личности, общества и государства, а также использование результатов цифрового следообразования для целей привлечения злоумышленников к ответственности и отправления правосудия представляют собой относительно новое социальное явление, зародившееся в результате глобальной интернетизации, стремительного развития современных технологий и критического накопления ценных данных в киберпространстве.

Согласно данным Global Digital 2022,[1] по состоянию на начало 2022 г. количество интернет-пользователей в мире составило 4,95 млрд. человек (62,5% населения планеты), а количество уникальных пользователей мобильных телефонов – 5,31 млрд. человек (67,1% людей в мире). При этом удвоение количества интернет-пользователей – с 2,18 млрд. человека до 4,95 млрд.человек – заняло только последние 10 лет, составляя в среднем 8,6% ежегодного роста. За все время ведения статистики, впервые количество людей, оставшихся «оффлайн» (без подключения к Интернету), составило менее 3 млрд. А количество времени, которое среднестатистический пользователь Интернет в возрасте от 16 до 64 лет проводит онлайн, составляет в среднем по миру почти 7 часов (или более 40% бодрствования) и продолжает ежегодно расти. Эти же тенденции, в целом, характерны и для Кыргызской Республики, где количество пользователей Интернета за последний год выросло на 3,4%, составляя на начало 2022 года суммарно 3,41 миллиона человек (или 51,1% населения страны на момент оценки), а количество мобильных телефонов составило 10,61 миллионов единиц, что на 158% больше, чем все население Кыргызской Республики на момент оценки.[2]

Это свидетельствует о том, что пользование Интернетом, действительно, стало базовой потребностью, а поиск, получение и распространение информации и идей посредством Интернета – базовым правом человека.[3]

Повсеместная интернетизация мирового населения сопровождается бурным развитием современных информационных технологий. Инфраструктура информационных технологий, продуктов и решений, образуя полноценную экосистему, все больше становится глобальной и доступной для каждого пользователя из любой точки планеты. Грань между промышленным, профессиональным и бытовым использованием современных технологий все больше становится неразличимой, а программные обеспечения и технические решения, несмотря на всю сложность своей природы, обеспечивают комфортное интерактивное взаимодействие с пользователями, становясь более дружелюбными для них и равнодоступными на различных платформах и устройствах.

---

[1] Более подробно см.: Digital 2022: Global Overview Report (https://datareportal.com/reports/digital-2022-global-overview-report).

[2] См.: Digital 2022: Kyrgyzstan (https://datareportal.com/reports/digital-2022-kyrgyzstan)

[3] Report of the special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf)

Развитие современных технологий не только преобразило экономику, политику и все другие сферы деятельности, но и кардинально изменило образ повседневной жизни каждого человека. Отныне, отсутствие профиля человека в социальных сетях является, скорее, исключением, чем правилом. Количество пользователей социальных сетей на начало 2022 года составило более 4,62 миллиардов, и оно растет очень динамично, составляя около 10% прироста (или около 424 миллионов новых пользователей) за предыдущие 12 месяцев.[4] При этом, социальные сети, традиционно воспринимаемые как средство досуга, меняются и все больше и больше превращаются не только в поле для рекламы, а полноценные площадки для прямых продаж товаров и услуг, оборот которых по различным оценкам растет в 3 раза быстрее, чем электронная коммерция.

С появлением и практической реализацией концепции «Интернет вещей» (Internet of things, IoT) каждый отдельный пользователь оказался в окружении самых разнообразных вещей, подключенных к сети и управляемых автономно и с минимальным участием или без участия человека. Количество подключенных к сетей устройств давно превысило количество жителей планеты и ожидается, что к 2025 году оно достигнет 55,7 млрд. единиц.[5]

Пандемия COVID-19, повсеместно сопровождаемая жесткими ограничительными мерами по социальному дистанцированию, не только усилила процессы внедрения цифровых решений во всех сферах деятельности, но и увеличила активность пользователей в Интернете на 76% (посредством мобильного телефона), 45% (посредством ноутбуков) и 32% (посредством стационарного компьютера).[6]

Как результат вышеуказанных глобальных процессов, киберпространство стремительно расширяется, и, поглощая и объединяя в себе все больше и больше сферы общественной и личной жизни пользователей. Киберпространство стало точкой соединения всех со всеми.

Отдельно следует отметить, что помимо расширения киберпространства за счет новых пользователей и средств соединения, идет глобальный процесс сбора, хранения и обработки различных данных. И по мере увеличения объемов данных, накапливаемых ежесекундно в хранилищах по всему миру, растет их экономическая и политическая ценность, а персональные, биометрические, финансовые и иные данные человека все чаще становятся предметом преступных посягательств. В то же время добросовестные правообладатели этих данных – государственные органы, представители бизнеса, неправительственные организации, политические активисты, журналисты и рядовые пользователи Интернета, с разным уровнем цифровой грамотности и защиты – становятся все более уязвимыми против неправомерных действий злоумышленников. Такая

[4] Более подробно см.: Digital 2022: Global Overview Report (https://datareportal.com/reports/digital-2022-global-overview-report).

[5] Что такое интернет вещей? (https://trends.rbc.ru/trends/industry/5db96f769a7947561444f118)

[6] см.: Digital 2020: April Global Statshot(https://datareportal.com/reports/digital-2020-april-global-statshot)

картина обоснованно вызывает тревогу. Согласно данным Global Risk Report 2022,[7] провал мер по обеспечению кибербезопасности, когда все более изощренные и частые киберпреступления, опережающие меры кибербезопасности бизнеса, государства и частных лиц, приводят к экономическим потрясениям, финансовым потерям, геополитической напряженности или социальной нестабильности, включен в состав глобальных рисков, имеющих значительный негативный эффект для стран и индустрий.

С полномасштабным перенесением жизни человека в киберпространство, появились новые задачи также и перед системой уголовного правосудия. В частности, все больше и больше становятся актуальными проблемы юридической квалификации преступности в форме криминального применения достижений современных технологий. Кроме этого, расширяются технические возможности сбора, изъятия, исследования так называемых «цифровых следов» человека в киберпространстве и использования их в качестве юридически допустимых доказательства по уголовным делам. Широкий спектр применения цифровых доказательств, а также их трансграничная природа создают необходимость разработки и утверждения правовых стандартов и нормативных актов, которые урегулируют и унифицируют процессы работы с цифровыми доказательствами.

Эти проблемы не обошли также и Кыргызской Республику. В Стратегии кибербезопасности Кыргызской Республики на 2019-2023 годы[8] одной из задач противодействия компьютерной преступности указано *закрепление в Уголовно-процессуальном кодексе Кыргызской Республики методов и средств компьютерной криминалистики, введение в Уголовно-процессуальный кодекс Кыргызской Республики и сопутствующие нормативные правовые акты понятия цифрового доказательства, описание и изложение его критериев, характеристик и способов фиксации, а также обеспечение признания юридической силы цифровых доказательств наравне с другими доказательствами* (пп. “б” п.5.4.). В продолжение этой задачи, Кыргызская Республика также намерена *рассмотреть возможности привлечения частных компаний к сбору цифровых доказательств и проведению судебных экспертиз по цифровым доказательствам для правоохранительных органов Кыргызской Республики* (пп. “г” п.5.4.). Таким образом, и для Кыргызской Республики исследование юридических аспектов сбора, исследования и оценки цифровой информации в качестве доказательств по уголовным делам и последующая интеграция достижений современных технологий в систему правосудия представляют из себя крайне актуальную и необходимую государственную задачу.

В связи с чем становятся своевременными и актуальными задачами.

Целью данного исследования является всестороннее изучение правовой природы цифровых доказательств, их юридически значимых особенностей, а также формирование рекомендаций по вопросам их внедрении в систему уголовного правосудия Кыргызской Республики в соответствии со Стратегией кибербезопасности.

---

[7] The Global Risks Report 2022, 17th Edition, Insight Report (https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf)

[8] Стратегия кибербезопасности Кыргызской Республики на 2019-2023 годы (утв. постановлением Правительства от 24 июля 2019 года №369).

Для достижения данной цели, в рамках данного исследования мы поставили следующие задачи:

(i) изучение теоретических основ понятия и правовой природы цифровых доказательств, определение юридически значимые особенностей цифровых доказательств и общепризнанных стандартов их использования;

(ii) анализ действующего уголовного процессуального законодательства и правоприменительной практики по уголовным делам по вопросам использования цифровых доказательств;

(iii) изучение особенностей применения специальных знаний специалиста и эксперта к работе с цифровыми доказательствами;

(iv) рассмотрение юридических вопросов интеграции цифровых доказательств в уголовное процессуальное законодательство Кыргызской Республики.

В рамках каждой из вышеуказанных задач мы приводим резюме ключевых находок и выводов, а также рекомендации для дальнейшего рассмотрения и реализации. В качестве практического результата проведенного исследования, мы разработали проекты нормативных правовых документов, предлагаемых к рассмотрению профильными государственными органами Кыргызской Республики.

## 2. ПОНЯТИЕ И ПРАВОВАЯ ПРИРОДА ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ

### 2.1. Понятие цифрового доказательства

В основе понятия цифрового доказательства находится механизм образования *цифрового следа*. Под цифровым следом, который используется как синоним понятий «цифровая отпечатка», «кибер-тень», «интернет-след» и других, понимается уникальный состав данных, оставляемых пользователем при совершении действий в Интернете, на цифровых или внешних запоминающих устройствах. Широко используемый в криминалистике принцип обмена Локара, согласно которому «каждый контакт оставляет след» и «при соприкосновении двух предметов произойдет обмен»[9], является актуальным и для киберпространства. Следовательно, все многообразие действий пользователя в киберпространстве оставляет бессчетное количество цифровых следов.

По своему содержанию цифровые следы могут различаться. Так, одни следы могут содержать в себе информацию об определенном *контенте* (текстовые сообщения, комментарии, аудио-, видео- и фотоматериалы, имена пользователей, голосования, лайки и др.), *метаданные* («данные о данных»: формат и размер файла, дата и время отправки, заголовок письма, адрес отправителя и получателя, автор, геолокация, версия браузера, операционная система и пр.). Цифровые следы могут быть «оставлены» на оптических, полупроводниковых или магнитных носителях, а доступ к ним может быть получен локальным или удаленным способом. Цифровые следы также классифицируются уровнем доступа (доступные, скрытые или зашифрованные) и зависимостью от энергии (энергозависимые и энергонезависимые).

Механизм цифрового следообразования может быть как активным, так и пассивным. *Активными* цифровыми следами принято считать совокупность информации, предоставленной пользователем осознанно, совершая ряд активных действий (к примеру, заполнение анкеты с собственными персональными данными, загрузка изображения, набор текста с определенным содержанием, «лайкать» и др.). Пользователь может оставить цифровые следы также непреднамеренно, не совершая каких-либо осознанных действий (к примеру, история поиска, IP-адрес, файлы cookie и др.). В этом случае речь идет о *пассивных* цифровых следах, формируемых из данных, которые различные сервисы получают и сохраняют автоматически и часто без ведома самого пользователя. При этом, следует особо подчеркнуть, что криминалистический интерес представляют оба вида цифровых следов, и их юридический вес не зависит от роли пользователя в следообразовании, поскольку факт, имеющий значение для правильного рассмотрения и разрешения дела, может быть подтвержден или опровергнут как активными, так и пассивными цифровыми следами.

[9] Edmond Locard (http://aboutforensics.co.uk/edmond-locard).

Цифровой след воплощается в форму *цифровой информации*.[10] Другими словами, цифровой след не может существовать сам по себе, он всегда обличен в форму цифровой информации, т.е. такой информации, которая преобразована в цифровой код посредством двоичного кодирования путем комбинации двух чисел – 0 и 1 (биты). Цифровая информация генерируется, фиксируется, хранится и передается в виде различных сигналов посредством различных технических устройств (компьютеры, телефоны, маршрутизаторы, другие устройства, подключенные к Интернету) и сетевой среды (кабели, коннекторы, сетевые карточки и пр.). При этом, сами сигналы могут иметь различную техническую природу (электрические, световые импульсы, радиоволны, механические).[11] Цифровая информация, будучи изначально закодированной посредством двоичной системы, не может в таком виде восприниматься человеком.[12] Следовательно, восприятие цифровой информации органами чувств человека возможно только в результате раскодирования с помощью специальных компьютерных программ, призванных преобразовать цифровую информацию в аналоговую.

Понятие «цифровое доказательство» используется для обозначения и подчеркивания особой природы цифровой информации, используемой в системе правосудия в качестве источника доказательства по делу (так же, как и в случае с «вещественными» или «письменными» доказательствами). Это понятие является *видовым* по отношению к понятию «доказательство». Другими словами, «доказательство», как *родовое* понятие, содержит в себе (или должно содержать в себе), помимо прочего, также и доказательства, относимые к цифровым. Поэтому, следует согласиться с мнением, что в доктринальном аспекте понятие «цифровое доказательство» не содержит какой-либо новый смысл, поскольку цифровое доказательство остается доказательством[13] и оно должно быть интегрировано в систему доказывания с учетом всех требований, предъявляемых к так называемым традиционным источникам доказательств. В практическом плане сказанное означает, что цифровые доказательства должны быть включены в систему источников доказательств в рамках действующей системы доказывания по Уголовно-процессуальному кодексу Кыргызской Республики (далее – УПК КР), а не создавать параллельную систему исключительно цифровых доказательств.

С учетом этого, основываясь на существующем в уголовно-процессуальном законодательстве Кыргызской Республики определении понятия

[10] В данном исследовании мы рассматриваем понятие «цифровая информация» в качестве родового понятия по отношению к «компьютерной информации», следовательно, цифровая информация, являясь более широкой по своему содержанию, включает в себя все среды обращения информации, не ограничиваясь только компьютерной средой.

[11] Русман Г.С., Родионов В.С. Цифровая информация как содержательный элемент компонентов цифровой индустрии с позиции права (на примере кибербезопасности). Проблемы права №5(79), 2020, с.100-104.

[12] Воронин И.М. О правовой природе электронных (цифровых) доказательств. Вестник Университета имени О.Е.Кутафина (МГЮА) №10, 2020, с.75.

[13] Пастухов П.С. «Электронные доказательства» в нормативной системе уголовно-процессуальных доказательств. Пермский юридический альманах, №2, 2019, с. 695-707.

«доказательства», можно дать следующее *теоретическое* определение понятия «цифровое доказательство»:

***Цифровое доказательство*** *– это цифровая информация, полученная в установленном законом порядке и на основе которой устанавливается наличие или отсутствие обстоятельств, имеющих значение для дела.*

Следует подчеркнуть, что термин «*цифровое доказательство*» является юридическим, а не техническим, и он характеризует процессуально-правовой статус цифровой информации, которая по своему содержанию способна подтвердить наличие или отсутствие определенных обстоятельств, имеющих значение для разрешения конкретного дела. Юридический статус доказательства присваивается цифровой информации исключительно при соблюдении ряда процессуальных требований к сбору, хранению и использованию доказательств.

Отдельно хотелось бы отметить, что прилагательное «цифровое» не должно вводить в заблуждение, будто такой вид доказательства допустим только при рассмотрении дел по так называемым компьютерным преступлениям или преступлениям против кибербезопасности. К последним, согласно законодательству Кыргызской Республики относятся несанкционированный доступ к компьютерной информации и электронным документам, в информационную систему или сеть электросвязи (ст.319 УК КР), создание вредоносных программных продуктов (ст.320 УК КР), кибер-саботаж (ст.321 УК КР), массовое распространение электронных сообщений (ст.322 УК КР). Напротив, сфера применения цифровых доказательств давно уже вышла за рамки таких узконаправленных высокотехнологичных преступлений и в настоящее время является общепризнанным, что цифровые доказательства должны быть эффективным инструментом правосудия не только против киберпреступности, а преступности в целом.[14] Правильное применение цифровых доказательств открывает безграничные возможности для органов правосудия, и теперь любое обстоятельство, входящее предмет доказывания и имеющее значение по тому или иному делу, может быть прямо или косвенно подтверждено цифровыми доказательствами. В практике иностранных государств есть кейсы, когда применение современных способов сбора, использования и оценки цифровых доказательств стали ключевыми в доказывании как вины, так и невиновности по различным видам преступлений. К примеру, цифровая экспертиза метаданных файла Microsoft Word на дискете привела к раскрытию личности убийцы, разыскиваемого в течение 30 лет,[15] данные из кардиостимулятора были использованы в качестве доказательств страхового мошенничества,[16] а извлечение

[14] Управление ООН по наркотикам и преступности. Всесторонее исследование проблемы киберпреступности, 2013 (https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf).
[15] Подробнее: Dennis Rader (https://en.wikipedia.org/wiki/Dennis_Rader).
[16] Подробнее: Is using pacemaker data ‘stealing personal information’? Judge in Middletown arson case says no (https://www.journal-news.com/news/crime--law/using-pacemaker-data-stealing-personal-information-judge-middletown-arson-case-says/BAGH5WM0iCxOTwTPfM3P7J/).

и исследование фотографий из мобильного телефона доказали невиновность обвиняемого и привели к прекращению обвинения в убийстве.[17]

Дополнительно, понятие «цифровое доказательство» не является исключительно уголовно-правовым, напротив, оно характеризируется кросс-дисциплинарностью, т.е. применимостью во всех видах судопроизводств (уголовного, гражданского, административного). Из этого вытекает, что, хотя и субъект, предмет и пределы доказывания в каждом из судопроизводств могут отличаться, концептуальное и содержательное наполнение цифрового доказательства остается неизменным: это всегда цифровая информация, которая собирается и используется в порядке, установленном законом, и оценка которой позволяет делать вывод о том, насколько эта цифровая информация подтверждает наличие или отсутствие предмета доказывания. Практическое значение этой теоретической конструкции заключается в том, что законодатель при интеграции цифровых доказательств в систему правосудия должен обеспечить, чтобы правила сбора, использования и оценки цифровых доказательств во всех отраслях процессуального законодательства были единообразными.

## 2.2. Юридически значимые особенности цифровых доказательств

По сравнению с так называемыми традиционными источниками доказательств, цифровые доказательства обладают следующими техническими особенностями:

- **Цифровая сущность:** в основе цифрового доказательства находится цифровая информация, которая представляет собой результат цифрового следообразования в виде двоичного кодирования посредством комбинации двух чисел – 0 и 1 (бит).
- **Абстрактность и опосредованность:** из цифровой сущности доказательства следует, что оно не может быть воспринято человеком невооруженным взглядом, и сбор, использование и оценка цифрового доказательства требуют определенного материального носителя;
- **Интерпретируемость:** ценность цифрового доказательства для системы правосудия зависима от интерпретации специалистов, вовлеченных в процесс сбора цифровых доказательств, и от того, в какую форму, воспринимаемую органами чувств человека, в результате будет облечено цифровое доказательство;
- **Хрупкость:** цифровые доказательства по своей природе является хрупкими, незащищенными против изменения, повреждения или уничтожения, в том числе, непредумышленного, и, следовательно, юридическая ценность

[17] Подробнее: Finding Innocence with Digital Evidence (https://www.digitalinnocence.com/2019/07/09/finding-innocence-with-digital-evidence/).

цифровых доказательств для правосудия может быть утрачена в результате неправильного обращения с ними;

- **Неограниченность в копировании:** цифровые данные, служащие в качестве цифровых доказательств, могут быть размножены, что позволяет нескольким субъектам одновременно и в разных местах работать над доказательствами;
- **Многообразие форм:** цифровые доказательства могут иметь многочисленные формы, одни из которых могут быть относительно простыми, представлены и продемонстрированы сравнительно простым способом, тогда как другие формы могут быть сложной природы и их доказательственная сила может быть обеспечена за счет применения сложных техник;
- **Трансграничность:** цифровые доказательства и/или их лица, владеющие ими, могут находиться за пределами юрисдикции страны компетентного следственного органа;
- **Специальные знания и навыки:** обращение с цифровыми доказательствами требует повышенной юридической и технической квалификации, специальных знаний и навыков от всех участников процесса сбора, использования и оценки цифровых доказательств.

Вышеуказанные особенности цифровых доказательств являются юридически значимыми, т.е. такими, которые при совершении правильных или неправильных действий с ними могут иметь совершенно различные юридические последствия для участников дела. Следовательно, технические особенности цифровых доказательств должны быть не только исследованы и продекларированы, их следует учесть при интеграции цифровых доказательств в систему правосудия и регламентации правил работы с ними.

### 2.3. Общепризнанные стандарты использования цифровых доказательств

Вышеуказанные особенности цифровых доказательств, их существенное отличие от традиционных источников доказательств, а также все более значимая роль, которую играют цифровые доказательства в современных системах правосудия, сформировали базовые правила, требуемых соблюдения органами правосудия при работе с цифровыми доказательствами. Несмотря на различия формулировок, использованных в изученных нами источниках, обобщенно можно говорить об определенном уровня международного консенсуса относительно следующих стандартов использования цифровых доказательств:[18]

1) **Обеспечение целостности и аутентичности цифровых доказательств:** целостность и аутентичность цифровых данных, имеющих значение для дела, напрямую влияют на их «доказательственный вес» с точки зрения их надежности. Следовательно, сторона, заинтересованная сторона судебного

[18] Electronic Evidence Guide. A Basic Guide for Police Officers, Prosecutors and Judges (https://rm.coe.int/0900001680a22757).

процесса, представляя цифровые доказательства по делу, обязана также продемонстрировать непрерывность и сохранность доказательств путем обеспечения так называемой «цепочку хранения» («chain of custody») – механизм, применяемый для сохранения и документирования хронологической истории цифровых доказательств по мере их перемещения из одного места в другое. Этот механизм позволяет подтвердить, что цифровые доказательства не были подделаны или иным образом изменены.[19] При этом, целостность и аутентичность цифрового доказательства должны быть обеспечены как на уровне физического устройства, содержащего цифровые данные, так и на уровне самих хранящихся данных.

2) **Документирование процесса работы с цифровыми доказательствами**: все действия, предпринятые в ходе работы с цифровыми доказательствами, должны быть задокументированы (записаны и сохранены) с тем, чтобы их можно было впоследствии проверить. Независимая третья сторона, при необходимости, должна иметь возможность не только получить доступ к такой документации, но и повторить задокументированные действия и выйти на те же результаты.
3) **Поддержка специалистов:** для работы с цифровыми доказательствами, в том числе на стадии сбора и изъятия, желательно своевременно и юридически корректно привлекать профильных специалистов, обладающих соответствующими и подтвержденными знаниями для компетентного обращения с цифровыми доказательствами.
4) **Квалификация органов дознания:** лица, выступающие органами дознания,[20] должны пройти необходимую и соответствующую подготовку, чтобы иметь возможность проводить работу по поиску и изъятию цифровых доказательств, если на месте происшествия нет специалистов. Действия органов дознания по сбору цифровых доказательств должны быть совершены в соответствии с официально утвержденными процедурами.
5) **Правовая состоятельность:** при работе с цифровыми доказательствами все требования и ограничения процессуального законодательства должны быть соблюдены неукоснительно, и несоблюдение правовых требований должно привести к исключению цифровых доказательств из дела, как не прошедших тест допустимости доказательств.

[19] Управление ООН по наркотикам и преступности. Всесторонее исследование проблемы киберпреступности, 2013 (https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf).

[20] Согласно ст.39 УПК КР, к органам дознания отнесены органы внутренних дел, органы и учреждения уголовно-исполнительной системы, командиры воинских частей, соединений и начальники военных учреждений, командиры пограничных частей, командиры воздушных судов, органы национальной безопасности, таможенные органы, органы службы чрезвычайных ситуаций, руководители геологоразведочных партий, экспедиций в отдаленных местностях, главы дипломатических представительств и консульских учреждений Кыргызской Республики, органы налоговой службы. Одной из главных задач органов дознания в уголовно-процессуальном контексте является принятия неотложных мер к сохранению следов происшествия и передача собранных материалов следственным органам.

**КЛЮЧЕВЫЕ ВЫВОДЫ:**

1. Цифровое доказательство является юридическим термином, характеризующим процессуально-правовой статус цифровой информации.
2. Цифровая информация является формой материализации цифрового следа человека в киберпространстве.
3. Цифровые доказательства обладают рядом юридически значимыми особенностями (цифровая сущность, абстрактность, опосредованность, интерпретируемость, хрупкость, неограниченность в копировании, многообразие форм, трансграничность, квалифицированное обращение).
4. К международно признанным стандартам использования цифровых доказательств в системе правосудия относятся:
    - Обеспечение целостности и аутентичности цифровых доказательств;
    - Документирование процесса работы с цифровыми доказательствами;
    - Поддержка специалистов;
    - Квалификация органов дознания;
    - Правовая состоятельность.

# 3. АНАЛИЗ ДЕЙСТВУЮЩЕГО ЗАКОНОДАТЕЛЬСТВА И ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ ПО ВОПРОСАМ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ

## 3.1. Общая характеристика законодательства Кыргызской Республики по вопросам использования цифровых доказательств в системе правосудия

Доказательство является институтом процессуального законодательства и основной массив норм, определяющих систему доказывания, сконцентрированы в уголовно-процессуальном, гражданско-процессуальном и административно-процессуальном законодательстве Кыргызской Республики. Безусловно, каждая из перечисленных отраслей законодательства, имея собственный предмет регулирования, кодифицирована отдельным законодательным актом, и отличается как составом источников доказательств, так и предметом и пределами доказывания. Кроме этого, в зависимости от вида судопроизводства, вопросы оценки доказательств с точки зрения их относимости, допустимости, достоверности и достаточности могут существенно отличаться.

В данном исследовании мы проводим предметный анализ УПК КР с точки зрения регламентации правил использования цифровых доказательств.

Вместе с тем, системный анализ отраслей процессуального законодательства Кыргызской Республики позволяет сделать следующие выводы *общего характера* в контексте сбора, использования и оценки цифровых доказательств:

### *1) Отсутствует системный подход к регламентации правил использования цифровых доказательств*

Несмотря на то, что правовая природа цифровых доказательств является единой для всех для всех видов судопроизводств, в процессуальном законодательстве не применяется системный подход к определению цифровых доказательств и регламентации правил их использования для рассмотрения и разрешения дела. Напротив, каждый из процессуальный кодексов оперирует собственным уникальным понятийным аппаратом, применимым к доказательствам, и как результат, одно и то же явление – цифровое доказательство – может наполняться различным содержанием и облекаться в форму, характерную только для конкретного вида судопроизводства.

### *2) Отсутствует легальное определение цифровых доказательств*

В действующих процессуальных кодексах Кыргызской Республики нет какой-либо нормы, содержащей определение цифрового доказательства. Кроме этого, кодексы не содержат статьи, косвенно или опосредованно указывающие на отдельные признаки цифрового доказательства. Следовательно, цифровое доказательство в процессуальном законодательстве Кыргызской Республики

воспринимается как *видовое понятие* по отношению к понятию «доказательство» и его содержание можно установить исключительно посредством дефиниции понятия «доказательство». При этом, само понятие «доказательство» и его смысловое наполнение, в том числе контексте цифровых доказательств, может различаться в зависимости от вида судопроизводства.

***3) Цифровое доказательство не выделено в самостоятельный вид источников доказательств***

Во всех процессуальных кодексах Кыргызской Республики цифровая информация, потенциально имеющая доказательственную силу для дела, не выделена в самостоятельный источник доказательства. Любая цифровая информация, способная теоретически подтвердить наличие или отсутствие обстоятельств, имеющих значение для дела, становится предметом исследования суда или уполномоченного органа только в качестве одного из источников доказательств, исчерпывающий перечень которых приведен в соответствующем кодексе. Такой подход приводит к тому, что любая цифровая информация, являющаяся исключительно цифровой по своей природе, изучается и оценивается в качестве вполне стандартного, «традиционного», доказательства. Другими словами, цифровая информация материализуется или «аналогизируется» в ту или иную форму, чаще всего, протокола следственных действий и приложенного к нему физического носителя цифровой информации, распечатки страниц сайтов на бумаге, вещественного и письменного доказательства, и «иного документа».

***4) Нет специальных требований к сбору и представлению цифровых доказательств***

Невыделение цифровых доказательств в самостоятельный источник доказательств приводит к тому, что нормы процессуального законодательства не учитывают многообразие форм цифровых доказательств и их юридически значимые особенности. Законодатель, как правило, не проводя системную дифференциацию между процессами сбора и представления цифровых и традиционных доказательств при рассмотрении дел, игнорирует особую правовую и техническую природу цифровой информации, используемой в системе правосудия. Следовательно, по законодательству одни и те же следственные или судебные действия могут быть одинаково применены по отношению к цифровым и нецифровым источникам доказательств.

***5) Нет специальных правил оценки цифровых доказательств***

Процессуальное законодательство Кыргызской Республики не содержит специальные правила, по которым органам правосудия следует оценивать цифровые доказательства по делу. Напротив, любое цифровое доказательство, рассматриваемое законодательством как вполне стандартное доказательство, должно отвечать общим требованиям относимости, допустимости, достоверности

и достаточности доказательств. Такой подход, в целом, не лишен логики и обоснования, поскольку доказательства, представленные по делу, должны быть оценены по единым стандартам, однако, как будет показано в дальнейшем, некоторые вопросы допустимости цифровых доказательств по уголовным делам требуют уточнения и конкретизации.

Кроме этого, доказательство, рассматриваемое нами как цифровое, в юридическом плане не обладает каким-либо преимуществом над традиционными источниками доказательств, и, как и любое доказательство по делу, цифровое доказательство не имеет заранее установленной силы и подлежит оценке в совокупности с другими доказательствами, собранными и представленными по конкретному делу.

***6) Цифровые доказательства могут быть представлены в качестве заключения и показания эксперта или показания специалиста***

Хотя и вопросы, связанные с цифровыми доказательствами, отдельно не выделяются и не именуются в процессуальных кодексах, в последних предусмотрено общее правило, по которому вопросы, требующие специальных неправовых знаний и навыков применения технических средств (к которым можно отнести и цифровые доказательства), могут быть разрешены с привлечением эксперта или специалиста. При этом, не определен какой-либо круг вопросов, по которым привлечение эксперта или специалиста является обязательным для сбора, использования и оценки цифровых доказательств, и эти вопросы разрешаются судом или уполномоченным органом по своему усмотрению или по ходатайству лиц, участвующих в деле, в общем порядке.

***7) Правила взаимодействия с провайдерами цифровой информации являются поверхностными***

Несмотря на то, что отдельные провайдеры услуг (операторы сотовой связи и интернет-соединения, операторы платежной и процессинговой информации, держатели различных публичных баз данных, операторы специальных аппаратно-программных комплексов по фото- и видеофиксации, коммерческие банки и другие финансовые институты, владельцы отдельных сайтов и информационных агентств), выступая держателями массива персональных и иных данных, в той или иной форме представляют цифровую информацию, имеющую доказательственную силу для конкретного дела, они сами редко становятся участниками процесса, а их процессуально-правовой статус не имеет четких юридических очертаний. Основное взаимодействие следствия и провайдера осуществляется в бумажной форме. Как правило, следственные органы

обращаются с письменным запросом о предоставлении определенных данных, а провайдеры предоставляют данные на основании судебного акта.[21]

При этом, хоть и не закреплено законодательно, есть основание утверждать, что при рассмотрении дел действует *презумпция достоверности* данных провайдеров услуг, согласно которой цифровая информация, оформленная в установленном порядке и представленная суду или уполномоченному органу провайдерами услуг, по умолчанию считается соответствующей действительности и не требует проведения мероприятий по перепроверке и дополнительному подтверждению ее действительности.

### 3.2. Обзор уголовно-процессуального законодательства Кыргызской Республики в контексте сбора и использования цифровых доказательств

Действующий УПК КР содержит специальный раздел III, полностью посвященный доказательствам и доказыванию в уголовно-процессуальном контексте. Согласно ч.1 ст.80 УПК КР, *доказательствами по делу являются полученные в установленном законом порядке сведения, на основе которых следователь, прокурор, суд определяют наличие или отсутствие обстоятельств, имеющих значение для дела*. К источникам доказательств отнесены *показания (подозреваемого, обвиняемого, потерпевшего, свидетеля), заключения и показания эксперта, показания специалиста, вещественные доказательства, протоколы специальных следственных, следственных и судебных действий, и иные документы* (ч.2 ст.80 УПК КР). Предметом любого доказательства, используемого в уголовном процессе по законодательству Кыргызской Республики, являются следующие обстоятельства (ст.81 УПК КР):

1) *событие преступления (время, место, способ и другие обстоятельства совершения преступления и наступившие его вредные последствия);*
2) *совершение или несовершение деяния лицом;*
3) *виновность или невиновность лица в совершении преступления, форма его вины и мотивы;*
4) *обстоятельства, влияющие на степень и характер ответственности подозреваемого, обвиняемого;*
5) *обстоятельства, характеризующие личность подозреваемого, обвиняемого;*
6) *характер и размер материального ущерба и (или) морального вреда, причиненного преступлением;*
7) *обстоятельства, исключающие уголовную противоправность деяния;*
8) *обстоятельства, влекущие освобождение от уголовной ответственности, наказания и его отбывания за преступление;*
9) *обстоятельства, подтверждающие, что имущество, подлежащее конфискации в соответствии с Уголовным кодексом, получено в результате*

[21] Ответ ЗАО «Альфа Телеком» №01-04/3422 от 27 декабря 2022 года, ответ ОсОО «НУР Телеком» №03/3300 от 22 декабря 2022 года на наш запрос.

*совершения преступления или является доходом от этого имущества либо использовалось или предназначалось для использования в качестве орудия преступления.*

Действующему УПК КР неизвестно понятие «цифровое доказательство», а цифровая информация, имеющая потенциальное доказательственное значение, не квалифицируется как самостоятельный источник доказательства по делу. Кроме этого, понятие «цифровая информация», которое, кстати, определено в ст.5 УПК КР крайне неудачно и грамматически некорректно,[22] вообще не используется по всему тексту кодекса, в связи с чем цель легального определения данного понятия для нас осталась не выясненной.

Вместе с тем, по нашему мнению, следующие данные, прямо указанные в УПК КР и собираемые и представляемые суду по уголовному делу, есть смысл относить к категории цифровой информации:

- Электронная переписка, электронные и иные и сообщения (ст.231);
- Телефонные и иные переговоры (ст.230);
- Фотографии, в том числе:
  - как вещественные доказательства (ч.2 ст.86, ч.2, ст.87);
  - как иной документ (ч.2 ст.89);
  - как приложение к протоколу следственного действия (ч.4 ст.170, ч.10 и 11 ст. 172, ч.3 ст.174, ч.6 ст.175, ч.7 и 8 ст.177, ч.3 ст.211, ч.7 ст.212, ч.6 ст.216, ч.7 ст.217, ч.8 ст.219, ч.1 ст.228);
  - как способ фиксации результатов наблюдения за лицом или местом (ч.2 ст.234);
  - как способ фиксации обнаруженных объектов в результате проникновения и обследования нежилого помещения или иного владения лица (ч.3 ст.235);
  - как способ фиксации результатов осмотра в ходе судебно-медицинской экспертизы по заявлениям о применении пыток и жестокого обращения (ч.11 ст.179);
  - как способ проведения опознания определенных объектов (ч.4 ст.209, ч.3 ст.211) и лиц (ч.8 и 9 ст.210, ч.3 ст.211);
  - как способ фиксации хода судебного разбирательства (ч.4 ст.308);
- Аудио- и видеозаписи, в том числе:
  - как иной документ (ч.2 ст.89);
  - как сведения, записанные адвокатом как необходимые для защиты, представления инетересов потерпевшего (ч.4 ст.53);
  - как способ фиксации допроса ребенка потерпевшего (ч.1 ст.78);

[22] Согласно подпункту 48 ст.5 УПК КР: «цифровая информация – цифровые данные, хранящиеся и циркулирующие в информационно-телекоммуникационных системах в ходе уголовного судопроизводства и их последующее использование в доказывании по досудебному производству» (прим.: цитата дословная).

  - как способ фиксации хода личного обыска задержанного (ст.98);
  - как приложение к протоколу по отдельным следственным действиям (ч.2, 4, ст.170, ч.10, 11 ст.172, ч.6 ст. 175, ч.7 ст.177, ч.8 ст.198, ч.7. 204, ч.7. ст.212, ч. 6 ст.216, ч.7 ст.217, ч.8 ст.219, ч.1 ст.228);
  - как способ удостоверения факт отказа от подписания протокола следственного действия (ст.171);
  - как способ фиксации результатов осмотра в ходе судебно-медицинской экспертизы по заявлениям о применении пыток и жестокого обращения (ч.11 ст.179);
  - как способ фиксации хода допроса (ст.200);
  - как способ проведения опознания лиц (ч.8 и 9 ст.210, ч.3 ст.211);
  - как способ скрытой фиксации речевой информации, поведения лица или разговоров и других звуков, событий, происходящих в строго определенном месте (ст.233);
  - как способ фиксации результатов наблюдения за лицом или местом (ч.2 ст.234);
  - как способ фиксации хода судебного разбирательства (ч.4 ст.308, ст.310, 311);
  - для воспроизведения на суде показаний потерпевшего и свидетеля, данных в ходе досудебного производства (ст.330);
- Информация о соединениях между абонентами и (или) абонентскими устройствами (ст.231);
- Информация с компьютеров, серверов, сетей электросвязи и других устройств (ст.232);
- Информация на любых носителях (пп.8 ч.2, ч.3 ст.87);
- Электронные документы (ч.3 ст.89).

Кроме этого, цифровая информация может быть представлена в качестве доказательства в форме или в составе заключения и показания эксперта, а также в качестве показания специалиста (ч.2 ст.80 УПК КР).

Следует отметить, что УПК КР не ограничивает сбор и использование любых других данных, в том числе цифровых, которые могут иметь доказательственное значение для дела. Напротив, стороны обвинения и защиты, действующие самостоятельно друг от друга и на принципах равноправия и состязательности вправе избрать свою позицию по делу, способы и средства ее отстаивания (ст.18 УПК КР), в том числе путем собирания и представления любых сведений, которые могут установить обстоятельств, имеющих значение всестороннего рассмотрения и разрешения дела. Другими словами, любые цифровые доказательства, добытые сторонами в установленном законом порядке, могут быть представлены на оценку суда.

По аналогии с традиционными источниками доказательства по уголовному делу, цифровые доказательства, в какой бы форме ни представлялись перед судом, должны также отвечать требованиям УПК КР и проходить тест на соответствие следующим *общим* критериям:

- **Относимость доказательств:** цифровое доказательство должно прямо или косвенно подтверждать наличие или отсутствие обстоятельств, имеющих значение для дела (ч.1 ст.93 УПК КР). Цифровое доказательство по своему содержанию должно иметь причинно-следственную связь с предметом доказывания. Следовательно, цифровое доказательство, как и любое другое доказательство, должно позволять познать и оценить, насколько данные, полученные посредством доказательства, соотносятся с рассматриваемым делом, какие факты дела они подтверждают или опровергают и т.д.
- **Допустимость доказательств:** цифровое доказательство может быть использовано в осуществлении правосудия только в том случае, если оно получено из источников, указанных в законе и без нарушения требований закона (ч.3 и 4 ст. 80, ч.1 и 4 ст.93 УПК КР).
- **Достоверность доказательств:** содержание цифрового доказательства, данные, полученные посредством цифрового доказательства, должны соответствовать действительности (ч.1 и 5 ст.93 УПК КР). Другими словами, обстоятельства, являющиеся предметом доказывания, должны быть подтверждены цифровыми доказательствами точно и правильно, с исключением искажения, неоднозначностей, сомнения или разного понимания. Кроме этого, цифровое доказательство, устанавливая те или иные факты по делу, должно дополнять другие источники доказательств, находиться с последними в гармонии, не входить в противоречие с ними и не исключать их.
- **Достаточность доказательств:** цифровое доказательство в совокупности с другими доказательствами в деле должно отвечать требованиям достаточности для разрешения дела по существу (ч.2 ст.23, ч.1, 2 и 6 ст.93 УПК КР).

### 3.3. Особенности использования цифровой информации в качестве доказательства по уголовным делам

В результате анализа уголовного процессуального законодательства и правоприменительной практики по уголовным делам мы обнаружили следующие особенности использования цифровой информации в качестве доказательства по уголовным делам:

1) **Приоритетность протокола следственных действий над другими источниками доказательств**

Характерной особенностью уголовного процессуального законодательства Кыргызской Республики является приоритетность протокола следственного действия как форма фиксации доказательств по уголовному делу. Протокол следственного действия, как своего рода «зеркало» содержания данного действия, представляет собой основную процессуальную форму, посредством которой создается единообразный, юридически определенный и достаточно детально регламентированный режим совершения конкретного следственного действия[23] и выступают в качестве самостоятельного источника доказательств (ч.2 ст.80 УРК КР). Следовательно, все другие способы фиксации доказательств, как правило, носят факультативный характер и без протокола следственных действий фактически не имеют самостоятельной доказательственной силы. Это напрямую относится также и к цифровым доказательствам.

Вышеуказанное подтверждается не только постатейным анализом текста УПК КР, но и правоприменительной практикой судов Кыргызской Республики. Мы убеждаемся, что в уголовном процессе абсолютное большинство информации, являющей цифровой своей по природе, оцениваются в основном, как приложение к протоколу какого-нибудь следственного действия. Часто в приговорах судов не приводится отдельный анализ цифровой информации, а обстоятельства, вытекающие из цифровой информации и имеющие значения для дела, объявляются доказанными в результате исследования и оглашения протоколов следственных действий, составленных органами следствия.

К примеру, фонограмма, составленная в результате специального следственного действия (прослушивание переговоров) в порядке ст. 230 УПК КР, осматривается и прослушивается следователем, по результатам чего составляется протокол с дословным изложением информации, которая имеет значение для дела. В последующем, как показывает судебная практика, именно протокол осмотра и прослушивания фонограммы предстает в качестве доказательства по делу. В частности, в деле №УД-36-18-Ч7, как указано в приговоре суда, в качестве доказательства вины подсудимого был приведен протокол осмотра и прослушивания фонограммы, который в ходе судебного заседания «*был оглашен*».[24] Другими словами, в судебном заседании не был прослушан сам аудиофайл с записью разговора, а зачитан и оценен протокол, в котором излагалось содержание аудиофайла. Таким образом, если следовать тексту судебного приговора, цифровая информация, записанная на аудиофайле, не подвергалась судом *непосредственной* оценке, суд не исследовал обстоятельства, в которых создан данный аудиофайл, его неизменность и сохранность, а факты, имеющие

[23] Яковлева Людмила Валериевна, Агибалова Виктория Геннадьевна Процессуально-правовая природа протоколов следственных и судебных действий // Общество и право. 2003. №1. URL: https://cyberleninka.ru/article/n/protsessualno-pravovaya-priroda-protokolov-sledstvennyh-i-sudebnyh-deystviy (дата обращения: 28.10.2022).
[24] Приговор Токмокского городского суда Чуйской области от 25 апреля 2018 года (дело №УД-36-18-Ч7).

значение для дела, суд объявил установленными посредством протокола, в котором письменно изложено содержание такого аудиофайла.

Аналогично, по делу №УД-400/22.Б2 в обвинительном приговоре суд, приводя доводы в пользу доказанности вины обвиняемого, указывает, что «*согласно протокола осмотра предметов от 4 ноября 2021 года, осмотрен DVD-диск, выданный А.Н.С., где имеется запись: 18.10.2021 года, время 18:09 на кадрах видно, как О.у.Б. ходит по коридору учебного корпуса, всматривается в телефон; в 18:09:50 заходит в компьютерную лабораторию, включает свет, подходит к одному из компьютеров, так как в это время в аудиторию заходят два преподавателя, он покидает помещение. В 18:41:22 О.у.Б. вновь заходит в класс, подойдя к компьютеру наклоняется вниз, где расположен системный блок, находясь около 20-30 секунд выходит из помещения. В 18:47:35 О.у.Б. вновь заходит в кабинет и наклоняясь к компьютерам, вытаскивает деталь, и вновь выходит с помещения (том 1, л.д.16)*».[25] Т.е. в данном деле суд не воспроизвел имеющуюся в деле видеозапись в судебном заседании, не исследовал ее непосредственно, а буквально описал содержание видеоматериала, основываясь на протоколе, составленном органами следствия в ходе досудебного производства.

По делу №УД-355/22.Б2 в качестве доказательства приведен протокол осмотра предметов от 24 ноября 2021 года, которым «*был осмотрен DVD диск, на котором запечатлен момент, где А.Р.У. один подходит к автомашине, берет камень с земли и разбивает камнем переднее боковое стекло, после чего срабатывает сигнализация автомашины марки "***" (л.д.51). В последующем данный DVD диск постановлением следователя признан вещественным доказательством и приобщен к материалам дела (л.д.52)*»[26]. Иными словами, в качестве доказательства по делу суд приоритетно рассматривает протокол осмотра предмета, но не сам предмет (в данном случае – видеозапись).

В деле УД-644/22-О6 факт распространения запрещенных экстремистских материалов суд расценил «доказанными» четырьмя скриншотами страниц из личного профиля обвиняемого в «ВКонтакте», представленными на DVD диске и соответствующим протоколом осмотра, без просмотра самого профиля.[27]

В деле №УД-16/18 Б2 в судебном заседании факт просмотра обвиняемым роликов по применению боевых оружий, приемов с ножами, по пользованию взрывных устройств суд первой инстанции посчитал «подтвержденным» посредством “*планшета модели “Самсунг”, в ходе осмотра которого через специальное приложение “YouTube” просмотрены видео ролики*”.[28] Адвокат подсудимого указал в апелляционной жалобе, что «*суд не смог установить, посещал*

[25] Приговор Октябрьского районного суда города Бишкек от 28 марта 2022 года (дело № УД-400/22.Б2).
[26] Приговор Октябрьского районного суда города Бишкек от 15 июля 2022 года (дело УД-355/22.Б2).
[27] Приговор Ошского городского суда Ошской области от 29 августа 2022 года (Дело № УД-644/22-О6).
[28] Приговор Судебной коллегии по уголовным делам и делам об административных правонарушениях Бишкекского городского суда от 13 июля 2018 года (Дело №УД-16/18 Б2).

*ли на самом деле А.Т. (обвиняемый) каналы Ютуб или другие сайты, где можно найти руководство для изготовлены взрывных устройств*», и что «*такой истории посещений интернет сайтов на данном планшете не содержится*», и что «*ДВД-диски, приложенные к материалам уголовного дела, не удалось воспроизвести в судебном заседании, ни один из них не открылся*». Тем не менее, суд апелляционной инстанции повторно сослался на осмотр планшета и слово в слово повторил аргументацию суда первой инстанции, не дав надлежащую оценку доводам адвоката подсудимого. Таким образом, прямое разногласие между сторонами обвинения и защиты по вопросу посещения обвиняемым специализированных сайтов и просмотра роликов (на чем было построено обвинение в подготовке взрывного устройства) было разрешено в пользу обвинения исключительно на основе протоколов следственных действий, без воспроизведения обстоятельств и без сбора и оценки достоверной технической и цифровой информации.

Несмотря на его общераспространенность такого подхода по уголовным делам, в которых фигурируют цифровые доказательства, его следует считать порочным и нарушающим принцип непосредственности исследования доказательств, установленный в ст. 289 УПК КР. В данной статье (которая называется «Непосредственность и устность судебного разбирательства») установлено, что *в судебном разбирательстве дела все доказательства подлежат* ***непосредственному*** *исследованию. Суд заслушивает показания обвиняемого, потерпевшего, свидетелей, заключение эксперта, осматривает вещественные доказательства, оглашает протоколы и иные документы, проводит другие судебные действия по исследованию доказательств. Приговор суда может быть основан лишь на тех доказательствах, которые были исследованы в судебном заседании либо получены в результате депонирования доказательств.*

Соблюдение принципа непосредственности исследования доказательств представляется крайне важным для уголовного судопроизводства и представляет собой важнейшую гарантию всестороннего, полного и объективного исследования обстоятельств дела.[29] Дело в том, что судья, не будучи непосредственным очевидцем события преступления, решает судьбоносные вопросы для участников процесса только путем исследования доказательств, собранных по делу. Поэтому судьи обязаны делать выводы и выносить решение по делу, основываясь на информации о фактических обстоятельствах дела, полученных ими на основе *личного* восприятия всех доказательств в ходе судебного заседания. Их восприятие не может быть опосредованным и зависеть от интерпретации технически сложных вопросов органами следствия, которые прямо заинтересованы в исходе дела. В контексте оценки судом цифровых доказательств, которые, как отмечалось ранее,

[29] Митяева Е. В. Непосредственность исследования доказательств по уголовному делу // Вестник МГУ. 2009. №4. URL: https://cyberleninka.ru/article/n/neposredstvennost-issledovaniya-dokazatelstv-po-ugolovnomu-delu (дата обращения: 31.10.2022).

могут быть легко изменены в ходе их сбора и хранения, данный вопрос становится еще более актуальным и острым.

Ради справедливости, следует отметить, что такая практика не является единообразной. Напротив, в ходе исследования приговоров по уголовным делам мы встречали отдельные случаи, в которых обстоятельства, имеющие значение для дела, были доказаны цифровой информацией, которая не только была протоколирована следственными органами, но воспроизведена в ходе судебного заседания, предметно и непосредственно изучена судом в качестве доказательства по делу. К примеру, в приговоре по делу №УД-403/21Б3 сказано, что «*в ходе судебного разбирательства DVD-диск с видеозаписями с места происшествия, которая предоставлена потерпевшим М.Ж.М. в ходе досудебного производства, была воспроизведена и исследована в судебном заседании. Из указанной видеозаписи видно, что между обвиняемым С.Н.О. и потерпевшим М.Ж.М. происходит драка, в которой обвиняемый С.Н.О. повалив на землю потерпевшего М.Ж.М. наносит последнему удары руками и ногой в разные части тела. Вместе с тем, как видно из видеоматериала, со стороны Ж.И.Ж. предпринимались меры, направленные на предотвращение противоправных действий С.Н.О., сопровождавший рукоприкладство в отношении потерпевшего, то есть разнимал последних*».[30] Другими словами, в данном деле суд, следуя принципу непосредственности исследования доказательств, воспроизвел запись в судебном заседании и сформировал свое мнение по делу, основываясь на собственном личном восприятии информации. К сожалению, такой подход является, скорее, редким исключением, чем распространенным правилом.

**2) Размытость и неопределенность юридически значимых категорий**

Несмотря на то, что цифровая информация *де факто* используется в качестве доказательства по делу, понятийный аппарат юридически значимых категорий, приведенный в уголовном процессуальном законодательстве Кыргызской Республики и применимый к цифровым доказательствам, не отличается полнотой и строгой логической структурой. Это не только препятствует правильной правовой квалификации тех или иных процессуальных действий органов следствия, но и является причиной достаточно противоречивой правоприменительной практики. В результате не только страдает качество следственного и судебного исследования доказательств по делу, но и создается реальная угроза для прав и свобод участников уголовного процесса.

В данном контексте крайне важно обратить внимание на то, что уголовному процессуальному законодательству Кыргызской Республики не знакомо понятие «*мобильный телефон*», и его процессуально-правовой статус остается неопределенным.

[30] Приговор Первомайского районного суда города Бишкек от 16 июля 2021 года (дело № УД-403/21Б3).

Бесспорно, что современные мобильные телефоны[31] давно перестали быть только средством телефонной связи. В настоящее время мобильные телефоны являются хранилищем огромного спектра информации, включая личной и деловой переписки, контактов, электронной почты, фотографий, аудио- и видеоматериалов, текстовых сообщений, заметок, уведомлений, напоминаний, отметок в календаре, истории звонков, подписки на разные сервисы, информации о покупках, банковской и платежной информации и др. Кроме этого, мобильные устройства, как правило, также могут содержать в себе метаданные (данные о геолокации, история просмотра сайтов, история скачивания, удаления или пересылки файлов, данные об IP-адресах и др.). Поэтому, при расследовании уголовных дел сложно переоценить доказательственные возможности современного мобильного телефона и сбор и исследование данных из него становится первичным фокусом интереса для расследователей.[32]

Вместе с тем, действующее уголовное процессуальное законодательство Кыргызской Республики никак не определяет правовой статус мобильного телефона и однозначно не причисляет его к какому-либо «устройств», указанных в УПК КР. Как результат, следственные действия с мобильным телефоном (выемка, обыск, осмотр, изъятие и пр.) не регламентированы отдельно и могут быть проведены в стандартном режиме, без учета особенностей, вытекающих из технологических возможностей мобильного телефона и ценности хранимой в нем информации для его владельца. Неопределенность правового статуса мобильного телефона, а равно свободная интерпретация отдельных норм уголовного законодательства по этому вопросу приводят к ряду проблем в правоприменительной практике.

Прежде всего, следует особо подчеркнуть, что следственные действия в отношении мобильного телефона по делам, скажем, о краже или грабеже находятся вне нашего внимания, поскольку в таких делах отсутствует информационная или цифровая составляющая, и мобильный телефон в этом контексте интересует органы следствия как исключительно как физический объект хищения и вещественное доказательство. Так, в деле №УД-136-22 ч8 мобильный телефон был квалифицирован в качестве вещественного доказательства и осмотрен как объект хищения.[33] Такое применение процессуального законодательства по отношению к мобильному телефону у нас не вызывает вопросов.

Вопросы возникают именно в делах, где мобильный телефон (чаще всего, обвиняемого) осматривается и протоколируется как носитель определенной

[31] В данном контексте мы под «мобильными телефонами» рассматриваем все виды смартфонов, планшетов, iPad и другие средства мобильной связи.
[32] Sean E. Goodison, Robert C.Davis, Brian A.Jackson. Digital Evidence and the U.S. Criminal Justice System.
[33] Приговор Ысык-Атинского районного суда Чуйской области от 29 июля 2022 года (№УД-136-22 ч8).

информации, а данные, извлеченные из мобильного телефона, представляются в суде в качестве доказательства по существу обвинения.

Так, в деле №УД-518/19.Б3, АБ-04-525/19УД, факт переписки, имеющей значение для дела, «доказан» через *«протокол осмотра сотового телефона от 2 апреля 2019 года, в ходе которого была установлена переписка с неустановленным следствием лицом по имени "А", из переписки установлено, что последний отправил контакты С.у.К. который должен был по приезду в Турецкую Республику созвониться и дальше направиться в Сирийскую Арабскую Республику»*.[34]

В данном случае мобильный телефон был осмотрен следствием и судом не только как физический объект, но и как хранилище информации, являющей юридически значимой для дела и имеющей доказательственную силу. Вместе с тем, суд, в отсутствие четких процессуальных правил проведения следственных действий с мобильным телефоном, не отнесся критически к действиям следствия и не исследовал вопрос о том, как получена и представлена суду цифровая информация, хранящаяся в мобильном телефоне, и насколько правомерно рассматривать ее как *допустимое* доказательство по делу. К сожалению, суд, по сложившейся практике, установил содержание переписки обвиняемого через протокол осмотра мобильного телефона, не прибегая к оценке правомерности действий следственных органов при сборе и представления такой информации в качестве доказательства по делу. Критический подход, на наш взгляд, непременно привел бы к ряду сложных юридических вопросов, правильное разрешение которых изменило бы судьбу данного конкретного уголовного дела и обвиняемого.

Аналогично, в деле № УД-1110/19.Б3 фото- и видеоматериалы, обнаруженные в телефоне в ходе его осмотра, были интерпретированы в качестве одного из ключевых доказательств вины подсудимого в хранении экстремистских материалов.[35] На наш взгляд, суд, вопреки своей обязанности, установленной в ч.1 ст.93 УПК КР, не провел оценку доказательства на предмет его допустимости, и не задался вопросом относительно того, стоит ли считать использование файлов из мобильного телефона, изъятого в ходе осмотра, допустимым с точки зрения требований уголовного процессуального законодательства.

Осмотр как следственное действие (ст.172 УПК КР) является одним из наиболее распространенных способов сбора доказательств по делу. Однако, в случаях, когда предметом осмотра выступает не только сам мобильный телефон, но и его информационное содержание, то возникают вопросы о правомерности и допустимости такого осмотра и его соотношении с констиционными гарантиями прав человека на личную тайну. Несомненно, что информация, которая хранится в мобильном телефоне и может оказаться в распоряжении следственных органов в

[34] Приговор Судебной коллегии по уголовным делам и делам об административных правонарушениях Бишкекского городского суда от 26 ноября 2019 года (Дело №УД-518/19.Б3, АБ-04-525/19УД).
[35] Приговор Первомайского районного суда города Бишкек от 23 октября 2019 года (Дело №№ УД-1110/19.Б3).

результате осмотра, относится к категории тайны, охраняемой законом. Следовательно, следственные действия с мобильными телефонами не могут быть «стандартными», и есть необходимость в внедрении специальных требований к таким следственным действиям.

По нашему мнению, законодательство должно однозначно определять процессуальный статус мобильного телефона как сложного технического устройства, в котором хранятся чувствительные и ценные данные персонального характера, и предусмотреть четкие правила работы с ним, как с источником доказательства, в ходе досудебного и судебного производства.

Отрадно, что такой подход также поддерживается позициями отдельных судов. Так, в деле №УД-309/22-Б3, АБ-04-441/22-УД, где суд, справедливо заметив, что «*сотовый телефон является устройством, хранящим информацию, в том числе устройством обмена сообщениями и для переговоров, переписки*», отметил необходимость проведения специального следственного действия, а именно снятие информации из телефона на основании постановления следственного судьи в порядке ст.232 УПК КР (снятие информации с компьютеров, серверов и других устройств).[36] Такой подход суда аргументирован конституционной гарантией тайны граждан на переписку и недопустимостью осмотра телефона «протокольно» (т.е. в стандартном режиме, без получения постановления следственного судьи). Суд посчитал, что, получая информацию из телефона без постановления следственного судьи, органы досудебного производства грубо нарушили требования уголовного процессуального законодательства, в результате чего *«протокол осмотра от 27 ноября 2021 года, а в целом любые сведения, полученные из телефона Б.Н.Б. с нарушением его конституционных прав на тайну переписки и норм уголовно-процессуального закона, не могут иметь юридической силы, относятся к недопустимым доказательствам и не могут быть положены в основу решения по делу».*

Аналогично, в деле №УД-704/22.Б3 суд исключил переписку по приложению WhatsApp, скопированную из мобильного телефона обвиняемого, из состава доказательств по делу, справедливо отмечая отсутствие согласия обвиняемого на сбор информации с его мобильного телефона, а также отсутствие разрешения следственного судьи на проведение специального следственного действия в виде снятие информации с компьютеров, серверов, сетей электросвязи и других устройств. Такая позиция суда мотивирована достаточно подробно, что является редкостью:

*«Так, В Конституции Кыргызской Республики, в главе второй, закреплены основные права и свободы человека. В частности, согласно части 1 статьи 29 Конституции Кыргызской Республики, каждый имеет право на неприкосновенность*

[36] Судебная коллегия по уголовным делам и делам о проступках Бишкекского городского суда от 29 июня 2021 года (дело №УД-309/22-Б3, АБ-04-441/22-УД).

*частной жизни, на защиту чести и достоинства. Право на неприкосновенность частной жизни, как юридическая категория состоит из ряда правомочий, обеспечивающих гражданину возможность находиться в состоянии автономии от государства и общества, а также юридических гарантий невмешательства в реализацию этого права.*

*К числу правомочий, являющихся существенным условием неприкосновенности частной жизни, Конституция относит право на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных, электронных и иных сообщений (часть 2 статьи 29). Право на тайну иных переговоров, от негласной записи разговоров - это право каждого на установление коммуникации с другими людьми без цензуры и вмешательства, при этом любые сведения, передаваемые одним человеком другому или другим, в том числе при помощи средств связи (различных средств межличностного общения) независимо от их содержания, являются конфиденциальной информацией и не должны предаваться огласке без оснований или согласия лица, в отношение которого ведется запись. Неприкосновенность такой информации предполагает ее известность только этим лицам, охраняется и гарантируется Конституцией и национальным законодательством.*

*Незаконный сбор, хранение, использование информации, поступившие вследствие переписки свидетеля с другими лицами, в том числе с обвиняемым, причиняют вред или создают угрозу его причинения правам и законным интересам индивида. В связи с этим, Конституция Кыргызской Республики запрещает сбор, хранение, использование и распространение конфиденциальной информации и информации о частной жизни человека без его согласия, кроме случаев, установленных законом, и тем самым выступает общей гарантией права на неприкосновенность частной жизни (часть 3 статьи 29). В случаях произвольного вмешательства в сферу частной жизни, Конституция гарантирует защиту, в том числе судебную, и право на возмещение материального и морального вреда, причиненного неправомерными действиями (часть 4 статьи 29).*

*Вместе с тем, согласно части 2 статьи 29 Конституции Кыргызской Республики право на тайну переговоров, не является абсолютным правом и может подвергаться ограничениям, допускаемым только в соответствии с законом и исключительно на основании судебного акта. При этом требования части 2 статьи 20 Конституции Кыргызской Республики предопределяют критерии вводимых ограничений, которые должны быть соразмерны целям защиты национальной безопасности, общественного порядка, охраны здоровья и нравственности населения, защиты прав и свобод других лиц.*

*Таким образом, право законодателя на ограничение тайны переговоров, на сбор информации путем применения специальных технических средств обеспечивается в Кыргызской Республике согласно Конституции и в соответствии с общепризнанными принципами и нормами международного права.*

*По смыслу вышеприведенных статей, правоограничения, касающиеся тайны иных переговоров, установлены законом, вмешательство государственных органов в данную сферу допускается исключительно на основании судебного акта.*

*Однако как уже отмечено выше, в материалах дела отсутствует постановление следственного судьи, дающее право на проведения специального следственного действия в виде снятии информации с компьютеров, серверов, сетей электросвязи и других устройств в соответствии с требованиями статьи 232 УПК Кыргызской Республики.*

*Так, согласно части 1 статьи 232 УПК Кыргызской Республики, при наличии достаточных оснований полагать, что информация с компьютеров, серверов, сетей электросвязи и других устройств, предназначенных для сбора, обработки, накопления и хранения информации, может содержать сведения, имеющие значение для уголовного дела, следователь на основании постановления следственного судьи вправе дать поручение уполномоченному подразделению органа дознания о конспиративном снятии необходимой информации.*

*То есть, неизвестно, каким способом и с помощью каких технических средств, был осуществлен перенос данных с сотового телефона А.А., после ее осмотра, на внешний диск, поскольку данная процедура не было соответствующим образом задокументирована, отсутствует судебный акт.*

*Суд по результатам судебного разбирательства по делу проверил все доказательства, как приведенные сторонами, так и добытые в ходе следствия и судебного разбирательства, сопоставил их между собой, и каждому из них дал оценку с точки зрения относимости, допустимости и достоверности.*

*В данном случае, суд отмечает, что результаты вышеуказанных следственных действий не могут быть положены в основу обвинения, в связи с тем, что были получены в нарушении требований норм УПК.*

*Так, уголовно-процессуальное законодательство закрепило основные требования по собиранию доказательств в уголовном судопроизводстве, как их получение путем проведения процессуальных действий, предусмотренных УПК. При этом, этим же Кодексом, законодательно закреплены требования к доказательству в части ее оценки на допустимость.*

*В частности, базисом доказательственного права является законодательно закрепленные принципы в части того, что каждое доказательство подлежит оценке по критериям относимости, допустимости, достоверности, а совокупность всех доказательств характеристике достаточности для разрешения уголовного дела по существу.*

*Законодательством признается исключительная важность требования допустимости доказательств, обеспечения прав и законных интересов участников процесса.*

*В соответствии с требованиями УПК Кыргызской Республики, собранные по делу доказательства подлежат всесторонней и объективной проверке. Проверка состоит в анализе полученного доказательства, его сопоставлении с другими доказательствами, собирании новых доказательств, проверке источников их получения. Суд оценивает доказательства по своему внутреннему убеждению, основанному на всестороннем, полном и объективном рассмотрении всех обстоятельств дела в их совокупности, при этом руководствуясь законом.*

*С учетом вышеуказанных требований законодательства, суд отмечает о недопустимости принятия вышеуказанных доказательств для обоснования вины обвиняемого и постановления в отношении него обвинительного приговора».*[37]

Мы полностью разделяем позицию суда по данному вопросу и считаем, что ее следует поддержать законодательно и сделать системной. Ограничения полномочий следственных органов, имеющиеся в уголовном процессуальном законодательстве и направленные на соблюдение конституционных прав и свобод человека, должны быть в центре внимания суда, а действие и бездействие следственных органов должны получать свою юридическую оценку в ходе рассмотрения и разрешения дела, в том числе в контексте сбора и использования в уголовном деле цифровых доказательств.

**КЛЮЧЕВЫЕ ВЫВОДЫ:**

1. Отсутствие процессуального статуса мобильного телефона служит источником противоречивой правоприменительной практики, приводящей к нарушению конституционных прав и свобод человека.
2. Есть отдельные судебные кейсы, в которых суды правильно разобрались с вопросом о допустимости использования мобильного телефона в качестве доказательства и, основываясь на гарантиях Конституции на частную жизнь, юридически корректно квалифицировали действия следственных органов.
3. Основываясь на позициях отдельных судов, необходимо дополнить УПК КР нормами, определяющим статус мобильного телефона как носителя личной информации.
4. Необходимо дополнить УПК КР специальными требованиями, согласно которым следственные действия с мобильными телефонами могут быть осуществлены на основании постановления следственного судьи.

[37] Приговор Первомайского районного суда города Бишкек от 4 ноября 2022 года (Дело №УД-704/22.БЗ)

### 3) Поверхностность следственного и судебного исследования цифровых доказательств

Как было указано выше, УПК КР не содержит специальных правил о допустимости цифровых доказательств. Другими словами, законодательно не решен вопрос о том, в каких случаях и при наличии каких *конкретных* критериев цифровое доказательство, представленное суду в рамках конкретного уголовного дела, может быть рассмотрено как правомерное и использовано для подтверждения тех или иных обстоятельств, имеющих значение для дела.

Анализ приговоров судов Кыргызской Республики по уголовным делам, в которых в качестве доказательства приводятся отдельные виды цифровой информации, показывает, что следственные органы и суды на практике не задаются вопросами о допустимости цифровых доказательств и не проводят исследование их технических аспектов. Кроме этого, как будет продемонстрировано в последующем, привлечение специалиста или назначение экспертизы также не обеспечивают полноту исследования природы и технических особенностей цифровых доказательств. Как правило, суды выносят свое решение, основываясь на совокупности всех доказательств, представленных по делу, и не предпочитают погружаться в технические детали отдельных цифровых доказательств.

В частности, в открытых источниках, СМИ, интернет-публикациях, приговорах судов, которые мы анализировали в качестве материала по уголовным делам, в которых были использованы отдельные цифровые данные или доказательства, мы не смогли найти правовую позицию следственных органов и судов по следующим вопросам:

- **Установление аутентичности цифрового доказательства**

Следственные органы и суды практически не исследуют вопрос о том, насколько цифровая информация, представленная суду как потенциально имеющая доказательственное значение по делу, была технически правильно изъята и сохранила свою первоначальную характеристику. Как отмечалось выше, сами по себе цифровые доказательства очень редко представляются суду для непосредственного исследования, а прилагаются к протоколу следственных действий. В тех редких случаях, когда цифровые доказательства представляются суду для непосредственного и личного исследования, происходит своеобразная «аналогизация» цифровой информации. К примеру, если предметом исследования является интернет-сайт, то суду этот сайт (или его сохраненная версия) не демонстрируется в режиме реального времени с его открытием посредством браузера, а представляется распечатка скриншотов в бумажной форме,[38] и, в

[38] Приговор Ошской областного суда от 24 октября 2022 года (Дело №УД-597/22-06).

отдельных случаях, с удостоверительной надписью нотариуса.[39] Следовательно, вопрос об обеспечении аутентичности представленного цифрового доказательства выводится за пределы судебного исследования и передается третьей стороне, не специализирующейся в вопросах сбора и исследования цифровых доказательств (в данном примере – передается к нотариусу).

К сожалению, следует констатировать, что общие нормы уголовного процессуального законодательства Кыргызской Республики, применимые к традиционным источникам доказательств, не привели к созданию конструктивной правоприменительной практики по установлению аутентичности цифровых доказательств. В частности, в правоприменительной практике не выработаны практические правила, следуя которым стороны уголовного процесса обеспечивают допустимость цифровых доказательств и исключают сомнения в технической целостности цифровой информации и отсутствии манипуляции в процессе ее сбора, хранения и исследования. В приговорах судов, изученных нами, мы не обнаружили оценку и позицию суда относительно того, насколько цифровая информация, представленная и принятая судом в качестве доказательства по делу, по мнению суда, сохранила свою аутентичность и не была подвергнута изменениям, что делает ее допустимым доказательством.

- **Установление принадлежности аккаунта к определенному лицу или совершения лицом определенных действий в интернете**

Несмотря на то, что термин «аккаунт» (как вариант, «страница в социальной сети», «профиль») все чаще и чаще используется в правоприменительной практике, уголовное процессуальное законодательство Кыргызской Республики никаким образом не определяет его понятие. Анализ приговоров по уголовным делам показывает, что суды вовсе не исследуют принадлежность аккаунта к определенному лицу или в лучшем случае по умолчанию *допускают* принадлежность аккаунта к владельцу мобильного телефона или компьютера, в котором имеется доступ к аккаунту или из которого осуществлен такой доступ. В дальнейшем, все действия, совершенные посредством такого аккаунта, *по умолчанию* приравниваются к действиям владельца мобильного телефона.

В деле №КИ1111-22/Б3 по обвинению в распространении экстремистских материалов, вопрос о принадлежности аккаунта в Facebook обвиняемому не был предметно и отдельно исследован, а установлен посредством изучения протокола об изъятии мобильного телефона обвиняемого, из которого следует, что *«в ходе осмотра названного мобильного телефона определено распространение фотографий*

[39] Согласно Инструкции о порядке совершения нотариальных действий нотариусами Кыргызской Республики, утв. Постановлением Правительства Кыргызской Республики от 20 апреля 2011 года №179, нотариус при освидетельствовании копии интернет-страниц осматривает информацию, размещенную в сети Интернет: интернет-страница полностью распечатывается на бумажный носитель с обязательным указанием даты печати и адреса файла, установленных в автоматическом режиме. После распечатки печатная версия сличается с электронным вариантом. В удостоверительной надписи нотариус указывает адрес страницы в сети Интернет, реквизиты документа, при необходимости указывается заголовок текста или графической информации, ее месторасположение на интернет-странице.

*и различных записей с аккаунта Н.А. в социальной сети «Фейсбук»*[40] (прим.: неофициальный перевод с кыргызского языка). Следовательно, суд, основываясь на протоколе следственного действия, применил *серию допущений* о том, что если телефон принадлежит обвиняемому, то аккаунт, который имеется в данном телефоне и открывается в нем, принадлежит обвиняемому, следовательно, авторство публикаций является *само собой разумеющимся*. Это допущение, хоть и может быть достоверным на практике, также и не исключает вероятности обратного и, как требует ст.17 УПК КР, не разрешает неустранимые сомнения в пользу обвиняемого.

В деле №УД-1050/22.Б3, в котором публикация Twitter была расценена как возбуждение расовой, этнической, национальной, религиозной, межрегиональной вражды (ч.1. ст.330 УК КР), вопрос о принадлежности рассматриваемого аккаунта в Twitter обвиняемой не исследован технически, а разрешен путем констатации того, что обвиняемая *«посредством своего мобильного телефона марки «Редми» опубликовала пост в интернет сервисе микроблогов и социальной сети «Твиттер».*[41] Опять же, прослеживается простое умозаключение о том, что владелец телефона является владельцем аккаунта. В контексте данного дела такое упрощение, в совокупности с признанием самой обвиняемой, может и не ставит под сомнение факт публикации обвиняемой конкретного текста на конкретном сайте, однако, оно не может рассматриваться как приемлемый способ исследования цифровых доказательств.

В правоприменительной практике Кыргызской Республики известны случаи, когда пользователь социальной сети Facebook привлекался к уголовной ответственности за комментарий, оставленный посторонним пользователем в ленте обвиняемого.[42] Другими словами, следственные органы, возлагая на пользователя Facebook обязанности модерирования контента, что является необоснованным с точки зрения законодательства Кыргызской Республики,[43] квалифицируют действия посторонних пользователей как действия самого пользователя. Такой подход, безусловно, недопустим, поскольку он необоснованно расширяет границы вины обвиняемого и создает чрезвычайно высокие риски неправомерного обвинения, которым подвергается практически любой человек.

В настоящее время органы правосудия, к сожалению, крайне далеки от компетентного исследования технических вопросов по надлежащей идентификации личности пользователя интернета и его действий в сети вообще и в социальных сетях в частности. Яркой иллюстрацией того, насколько значимыми

[40] Приговор Первомайского районного суда города Бишкек от 6 октября 2022 года (дело №КИ1111-22/Б3).
[41] Приговор Первомайского районного суда города Бишкек от 13 сентября 2022 года (дело №УД-1050/22.Б3).
[42] Институт Медиа Полиси. Обзор по делам о возбуждении расовой, этнической, национальной, религиозной или межрегиональной вражды (розни).
[43] Юридическое заключение ОФ ГИИП по факту ареста Жоробекова А. (https://internetpolicy.kg/2019/12/02/juridicheskoe-zakljuchenie-of-giip-po-faktu-aresta-zhorobekova-a/)

являются вопросы установления допустимости цифровых доказательств в уголовном деле, и чем грозит игнорирование изучения технических вопросов сбора, исследования и оценки цифровых доказательств, является дело Камрана Шенвари.

*Камран Шенвари, гражданин Афганистана, проживающий в Кыргызстане, был обвинен и признан виновным в возбуждении национальной, расовой, религиозной вражды, ему было назначено наказание в виде лишения свободы на 5 лет.*[44] *Поводом для обвинения послужил негативный комментарий в Facebook, оставленный пользователем с именем Kamran Shinwari. Следствие, а в последующем и суд, посчитали, что этот аккаунт принадлежит обвиняемому, и следовательно, комментарий, признанный разжигающим рознь – оставленным самим обвиняемым. Ключевым доказательством вины обвиняемого, на котором базировался обвинительный приговор, стала фотография Шенвари в профиле Facebook, с которого был написан комментарий. Сам К.Шенвари категорически отрицал свою вину, утверждая, что аккаунт, с которого был оставлен комментарий, никогда не принадлежал ему, не был создан им и не управлялся им. Из писем профильных ведомств (Государственное агентство связи Кыргызской Республики, Государственный комитет информационных технологий и связи Кыргызской Республики, Государственный комитет национальной безопасности Кыргызской Республики) и провайдеров связи, представленных защитой обвиняемого, следовало, что невозможно идентифицировать пользователей Facebook, определить, кем и когда был зарегистрирован аккаунт, а также подвергался ли аккаунт взлому со стороны третьих лиц. Для разрешения таких вопросов, как сообщалось, нужно обращаться в администрацию Facebook.*[45]

Благодаря усилиям защитника и членов семьи обвиняемого, дело Шенвари широко освещалась в СМИ, и на сегодняшний день является одним из немногих уголовных дел в правоприменительной практике Кыргызстана, в которых отдельные вопросы сбора, использования и оценки цифровых доказательств, были правильно сформулированы и поставлены защитой перед органами правосудия публично, но, к сожалению, оставлены без ответа по существу.

В данном деле, в отличие от других подобных дел, связанных с публикацией в Facebook, не фигурировало какое-либо устройство (как телефон или планшет), которое было бы изъято у обвиняемого, осмотрено протокольно и посредством которого можно было «выйти» на искомый аккаунт обвиняемого. Следовательно, обычный для таких дел логический алгоритм «устройство – аккаунт – обвиняемый» в данном случае не применим. По информации провайдеров сотовой

[44] В последующем, Верховный суд Кыргызской Республики изменил наказание на денежный штраф в размере 300 000 сом. См.: Верховный суд изменил наказание Камрану Шенвари. Он получил штраф (https://kaktus.media/doc/439056_verhovnyy_syd_izmenil_nakazanie_kamrany_shenvari._on_polychil_shtraf.html)

[45] Тексты писем цитируются согласно апелляционной жалобе защитника Камрана Шенвари. Текст апелляционной жалобы доступен по следующей ссылке: https://data.kaktus.media/file/file/2020-12-05_20-50-44_774020.pdf?load

связи, установить принадлежность аккаунта Facebook посредством абонентского номера мобильного телефона невозможно. Согласно показаниям специалиста, участвовавшего в деле, аккаунт в Facebook может создать любой человек без какой-либо сложности, а также без ведома того, на чье имя создается аккаунт. Есть также техническая возможность взлома аккаунта.[46] По оценке защиты, «*следствие не доказало его авторство поста, а защита привела достаточно аргументов, что Шенвари не мог этого написать*».[47] Таким образом, объективно какое-либо доказательство, прямо или косвенно указывающее на принадлежность аккаунта обвиняемому, суду представлено не было. Официального обращения к администрации Facebook тоже не было. Тем не менее, суд вынес обвинительный приговор, основываясь на том, что на фотографии, прикрепленной к профилю аккаунта, изображен обвиняемый, а также в деле есть видео следственных органов, на котором запечатлен процесс осмотра аккаунта, который, по мнению следствия, принадлежит обвиняемому.

По нашему мнению, суд, рассматривая данное уголовное дело, не обеспечил соблюдение стандартов рассмотрения и разрешения уголовных дел, установленных в уголовном процессуальном законодательстве Кыргызской Республики. Так, в частности, суд, вопреки пп.1 с.81 УПК КР, не разобрался с тем, в чем заключалось, как минимум, событие преступления (время, место, способ и другие обстоятельства совершения преступления и наступившие его вредные последствия), а также насколько в ходе судебного процесса было доказано совершение или несовершение вменяемого деяния данным обвиняемым лицом. Несмотря на откровенные пробелы в расследовании и соответствующие ходатайства защиты, суд не стал вникать в технические детали, имеющие чрезвычайное значение как для данного дела, так и для всей правоприменительной практики страны.

В ситуации, когда рассматривается достаточно специфичное дело, требующее погружения в технические аспекты присутствия человека в интернете и правовой оценки его действий, следствие и суд, по нашему мнению, должны были задаться, как минимум, следующими вопросами и направить все усилия для их правильного разрешения:

- Как идентифицировать пользователя интернета и его действия для целей правосудия?
- Как определить время, место и способ совершения преступления, совершенного в интернете?
- Достаточно ли наличие фотографии в профиле, чтобы считать, что пользователь однозначно идентифицирован и приравнен к личности,

[46] Все факты по делу цитируются согласно апелляционной жалобе защиты К.Шенвари.
[47] Житель Кыргызстана получил 5 лет колонии за комментарий в фейсбуке. Он утверждает, что не писал его. См.: https://www.currenttime.tv/a/prigovor-za-komment-facebook/31111673.html

чье лицо запечатлено на фотографии? Можно ли в этом случае считать, что установлен субъект преступления?

- Каков состав технических условий, при установлении которых аккаунт расценивается как принадлежащий конкретному человеку?
- Какой состав юридических и технических действий, однозначно доказывающих совершение каким-либо лицом какого-либо действия в интернете?
- Какие дополнительные цифровые данные могут подтвердить или опровергнуть позицию обвинения и защиты?
- Как отличить аккаунт реального человека и его действия от фейкового аккаунта?
- Как провайдеры услуг (в том числе, администрация социальных сетей и мессенджеров) могут помочь в осуществлении справедливого правосудия?

Нам доподлинно неизвестно, почему суд не стал задаваться такими вопросами. Вместе с тем, мы можем с уверенностью сказать, что в отсутствие специальных процессуальных правил регламентации работы следствия и суда с цифровыми доказательствами, такая практика поверхностного изучения юридически значимых технических вопросов будет продолжаться. Следовательно, задачи уголовного процессуального законодательства Кыргызской Республики, установленные в ст.6 УПК КР (а именно, защита личности, общества и государства от преступлений; защита личности от незаконного и необоснованного обвинения, осуждения, ограничения ее прав и свобод; быстрое и полное расследование преступлений; изобличение и привлечение к уголовной ответственности лиц, совершивших преступления; справедливое судебное разбирательство и правильное применение уголовного закона и др.), не будут выполнены в полной мере.

В связи с чем, мы считаем, что усилие законодателя должно быть направлено на формирование и внедрение стандартов сбора, исследования и оценки цифровых доказательств, а также расширение правовых основ для применения специальных знаний к исследованию и оценке цифровых доказательств в ходе осуществления правосудия. Мы разделяем точки зрения о том, что «институт допустимости в свете доказательств, содержащих электронную информацию, должен быть пересмотрен путем отказа от ее следственных гарантий в пользу технических гарантий верифицируемости и полезности доказательства».[48] Такие меры, по нашему мнению, особенно актуальны, когда, законодательство объективно не успевает за технологиями, а создание и использование фейк-

[48] Защита личных прав при использовании электронной информации в расследовании преступлений. Современные направления развития криминалистических методик и технологий в уголовном судопроизводстве. Сибирский Федеральный Университет, 2020.

аккаунтов в неправомерных целях стало самостоятельной масштабной индустрией.[49]

При этом, отдельные законодательные инициативы в Кыргызстане по регулированию правоотношений в Интернет-пространстве мы расцениваем как не отвечающие целям и задачам уголовного судопроизводства.

К примеру, Закон Кыргызской Республики «О защите от недостоверной (ложной) информации» от 23 августа 2021 года №101 устанавливает, что владелец сайта и (или) страницы сайта в интернет-пространстве Кыргызской Республики обязан разместить на своем сайте или странице сайта в сети Интернет свою фамилию и инициалы, электронный адрес для направления ему сообщений. С технической точки зрения такой способ «идентификации» пользователя в Интернете следует считать не состоятельной, поскольку он базируется на ничем не подкрепленном *допущении,* что каждый пользователь самостоятельно и добровольно укажет собственные персональные данные в Интернете. Откладывая в сторону нерешенные в законодательстве вопросы об осуществлении контроля за исполнением такого требования и привлечения к ответственности за его нарушение, мы лишь отметим, что в целом, подход, согласно которому доступ к Интернету будет обусловлен тотальной и обязательной идентификацией пользователей Интернета, напоминает концепцию «В интернет – по паспорту»,[50] не отвечает современным представлениям о ценностях прав человека,[51] справедливо расценивается как попытка ограничения свободы слова,[52] а его конституционность вызывает серьезные сомнения.[53] Кроме этого, с практической точки зрения, такие инициативы не решают какие-либо задачи в вопросах сбора, исследования и оценки цифровых доказательств в уголовно-правовой плоскости. В частности, в рамках конкретного уголовного дела идентификация человека и его действия в сети должна быть доказана технически и юридически допустимыми средствами доказывания, а не полагаться на декларации фамилии и инициалов (которая, кстати, может быть ложной). В целом, следует отметить, что технические средства, используемые в системе правосудия, должны служить принципам индивидуализации и личного характера уголовной ответственности и наказания (ст.7 и 8 УК КР), не ограничивать свободу человека *ex ante,* а оказывать содействие в доказывании обстоятельств, имеющих знание для дела, и осуществлении правосудия в рамках конкретного дела *ex post*.

---

[49] Подробнее: “У каждого было около 200 аккаунтов в соцсетях”. Как устроены “фабрики троллей” в Кыргызстане (https://www.opendemocracy.net/ru/fabriki-trollei-v-kyrgyzstane/).

[50] Регистрацию в соцсетях предложили проводить по паспорту (https://pravo.ru/news/244584/).

[51] Права человека, шифрование и анонимность в цифровой век (https://www.ohchr.org/ru/stories/2015/07/human-rights-encryption-and-anonymity-digital-age).

[52] Закон о фейках несет угрозу для всех СМИ, а тролли остаются безнаказанными (https://24.kg/obschestvo/244866_zakon_ofeykah_neset_ugrozu_dlya_vseh_smi_atrolli_ostayutsya_beznakazannyimi/)

[53] Нам известно о не менее 2 попыток оспорить конституционность положений Закона Кыргызской Республики «О защите от недостоверной (ложной) информации», а также подзаконных актов, принятых в развитие данного Закона. Информация о результатах рассмотрения Конституционном судом Кыргызской Республики таких ходатайств отсутствует в публичной сфере.

**КЛЮЧЕВЫЕ ВЫВОДЫ:**

1. Уголовно-процессуальное законодательство Кыргызской Республики системно не регламентирует правила использования цифровых доказательств. В нем отсутствует определение цифровых доказательств, а их место в системе источников доказательств не установлено. Цифровые доказательства собираются, представляются и оцениваются в общем порядке, без применения специальных правил.
2. Цифровые доказательства используются на те же цели, что и традиционные доказательства, а именно, для установление обстоятельств, указанных в законодательстве и имеющих значение для дела. Относимость, допустимость, достоверность и достаточность цифровых доказательств оцениваются в общем порядке без конкретизации и учета специфики цифровых доказательств.
3. Правоприменительная практика по использованию цифровых доказательств в уголовных делах является противоречивой:
    - Протокол следственных действий является центральным источников доказательств по уголовным делам и, чаще всего, цифровые доказательства оформляются в качестве приложения к нему, не имея самостоятельной доказательственной силы. Вследствие этого, цифровые доказательства почти не подвергаются непосредственному судебному исследованию.
    - Неопределенность процессуально-правового статуса мобильного телефона позволяет применить к нему «стандартные» следственные действия, что является источником противоречивой правоприменительной практики, приводящей к нарушению конституционных прав и свобод участников уголовного процесса.
    - Редкие цифровые доказательства, представленные на практике судам, исследуются крайне поверхностно, в том числе тогда, когда привлекаются эксперты и специалисты.
    - В отсутствие специальных законодательных требований, суды не сформировали свою позицию относительно того, как устанавливать аутентичность цифровых доказательств. Суды, как правило, полагаются на гарантию допустимости, предоставляемой следственными органами.
    - При установлении принадлежности аккаунта к определенному лицу или совершения лицом определенных действий суды применяют ряд технически и юридически необоснованных допущений, основанных на физическом владении устройством.
    - Суды не изучают технические подробности цифровых доказательств, их допустимость в качестве доказательства, и полагаются на позиции обвинения.
4. Отдельные законодательные инициативы по идентификации пользователя в сети не отвечают целям и задам уголовного судопроизводства.

# 4. ПРИМЕНЕНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ К РАБОТЕ С ЦИФРОВЫМИ ДОКАЗАТЕЛЬСТВАМИ

## 4.1. Участие специалиста в работе с цифровыми доказательствами

Безусловно, сбор, исследование и оценка таких технически сложных доказательств, к которым относятся цифровые доказательства, не могут быть полноценно осуществлены усилиями только следователя или судьи, и требуют привлечения других лиц, обладающих специальными знаниями и навыками.

Базовые правила привлечения специалиста для участия в деле регламентированы в УПК КР. Так, согласно ч.1 ст.57 УПК КР в качестве специалиста для участия в производстве по делу может быть привлечено незаинтересованное в деле лицо, обладающее специальными знаниями и навыками, необходимыми для оказания содействия в обнаружении, закреплении, изъятии предметов и документов, применении технических средств, для постановки вопросов экспертиз, а также для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию. Специалист может быть привлечен как по инициативе следствия (ч.1 ст.37, ст.168 УПК КПР), так и адвокатом (ч.4 ст.53 УПК КР).

Показания специалиста, т.е. сведения, сообщенные им на допросе в целях разъяснения или уточнения обстоятельств, требующих специальных познаний, являются одним из источников доказательств (ч.2 ст.80 УПК КР). Сведения, сообщенные специалистом, могут иметь доказательственное значение для дела и оказывать влияние на конечное решение суда, в связи с чем, уголовное процессуальное законодательство Кыргызской Республики устанавливает ряд достаточно строгих требований как к самому специалисту, так и к его показаниям. Так, специалист сам не должен быть заинтересованным в исходе дела (ч.1 ст.57 УПК КР) и его участие в деле может быть отведено в случаях, когда есть обстоятельства, исключающие его незаинтересованность в исходе дела (ст.73 УПК КР). Объективность и беспристрастность специалиста также обеспечиваются принятием государством мер безопасности от посягательства на его жизнь или иного насилия в связи с рассмотрением дел в суде или досудебном производстве (ст.75 УПК КР). Для признания показаний специалиста допустимым доказательством по делу, они должны быть включены в опись материалов уголовного дела (ч.4 ст.80 УПК КР). За отказ или уклонение специалиста от выполнения своих обязанностей без уважительных причин на него может быть наложено дисциплинарное взыскание (ч.4 чт.57 УПК КР), а заведомо ложные показания специалиста влекут уголовную ответственность (ст.364 УК КР).

Анализируя уголовное процессуальное законодательство в контексте участия специалиста в работе с цифровыми доказательствами, мы бы хотели акцентировать внимание на следующих моментах:

1) В подавляющем большинстве случаев следственные органы вправе привлекать специалистов в работу по сбору, изъятию, исследованию и оценке цифровых доказательств по своему усмотрению («*при необходимости*»). [54] Из УПК КР следует, что участие специалиста обязательно только при изъятии электронных носителей информации в ходе обыска и выемки, а также при копировании информации в случае невозможности изъятия электронных носителей (ч.17 ст.212 УПК КР). Кроме этого, в законе установлено, что в случае невозможности возврата электронных носителей информации после производства следственных действий, информация, содержащаяся на этих электронных носителях, копируется на другие носители с участием специалиста (ч.3 ст.87 УПК КР).

Во всех других случаях, когда предметом следственных действий или их отдельных эпизодов потенциально могут быть сбор, изъятие, исследование или оценка цифровых доказательств, вопрос об участия специалистов решается следствием по своему усмотрению. К последним относится достаточно широкий перечень следственных действий, включая осмотр места происшествия (ч.2 ст.172 УПК КР), обыск и выемка (ч.7 ст.212 УПК КР), проверка показаний на месте (ч.4 ст.215 УПК КР), следственный эксперимент (ч.3 и 4 ст.217 УПК КР). Более того, участие специалиста в специальных следственных действиях, которые, как правило, сопровождаются с применением технических средств сбору и хранению цифровой информации, так же определяется по усмотрению следователя. Так, специалист *может быть* привлечен по решению следователя при необходимости к осмотру и (или) выемке почтово-телеграфных отправлений (ч.4 ст.229 УПК КР), осмотру и прослушиванию фонограммы переговоров (ч.6 ст.230 УПК КР), исследованию информации о соединениях между абонентами и абонентскими устройствами и (или) о местоположении абонента (ч.3 ст.231 УПК КР), исследованию результатов снятия информации с компьютеров, серверов и других устройств (ч.3 ст.232 УПК КР), исследованию аудио-, видеозаписи по результатам аудио-, видеоконтроля лица или места (ч.3 ст.233 УПК КР), материалов наблюдения за лицом или местом (ч.3 ст.234 УПК КР) и др.

2) Уголовное процессуальное законодательство не содержит в себе нормы, устанавливающие порядок определения квалификации специалистов. По крайней мере, требование, содержащее к квалификации привлекаемого специалиста – владение специальными знаниями и навыками, необходимыми для оказания содействия в обнаружении, закреплении, изъятии предметов и документов, применении технических средств, для постановки вопросов экспертиз, а также для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию – оценивается, опять же, следственными органами. Хотя и предполагается, что специалист вправе отказаться от участия в производстве по делу, если не обладает соответствующими специальными знаниями и навыками

[54] В УПК КР отсутствует перечень случаев, образующих такую необходимость, и этот вопрос решается по личному усмотрению и согласно суждению следователя.

(ч.2 ст.57 УПК КР), сама по себе некомпетентность специалиста не является основанием для его отвода (ст.73 УПК КР).

К сожалению, в публичной сфере отсутствуют открытые эмпирические данные об участии специалистов в следственных действиях по уголовным делам, где используются цифровые доказательства. Тем не менее, сложно переоценить важность своевременного привлечения специалистов, компетентных по вопросам информационно-компьютерных технологий, на этапе планирования и подготовки следственных действий, связанных с поиском, обнаружением и фиксацией цифровых следов.[55] И напротив, самостоятельное решение технических вопросов самими органами следствия, равно как и привлечение специалистов без необходимой квалификации, могут привести к рискам неквалифицированного обращения с цифровыми доказательствами и потери последними аутентичности. Как отмечалось ранее, обращение с цифровыми доказательствами требует не только юридической, но и технической квалификации, а также специальных знаний и навыков, в связи с чем, стандарты по работе с цифровыми доказательствами требуют своевременно привлекать профильных специалистов, обладающих соответствующими и подтвержденными знаниями для компетентного обращения с цифровыми доказательствами.

## 4.2. Участие эксперта в работе с цифровыми доказательствами

Участие эксперта в работе с цифровыми доказательствами, бесспорно, является наиболее корректным способом исследования цифровой информации, установления ее целостности и аутентичности, а также определения допустимости ее использования в качестве доказательства по делу.

### 3.2.1. Правовые основы участия эксперта в уголовном процессе

В отличие от специалиста, правила привлечения эксперта в уголовное дело регламентированы не только в УПК КР, но и рядом специализированных нормативных актов.

Так, согласно ч.1 ст.56 УПК КР, экспертом является не заинтересованное в уголовном судопроизводстве лицо, назначенное судом, следователем, прокурором или, по их требованию, руководителем экспертной организации для разрешения вопросов, возникших в ходе досудебного производства или судебного разбирательства уголовного дела, с использованием специальных научных знаний и дачи на этой основе заключения. Эксперт должен обладать специальными знаниями в области науки, техники, искусства, ремесел, достаточными для дачи заключения по поставленным вопросам (ч.2 ст.56 УПК КР).

[55] Семикаленова А.И., Рядовский И.А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики. Актуальные проблемы российского права. 2019.№6(103) июнь.

Признав необходимым назначение экспертизы, следователь, прокурор, следственный судья, суд выносят об этом постановление, определение, в которых, помимо прочего, указываются вид экспертизы[56], объекты, направляемые на экспертизу, и информация об их происхождении, а также разрешение на возможное полное или частичное уничтожение указанных объектов, изменение их внешнего вида или основных свойств в ходе исследования, фамилия, имя и отчество эксперта или наименование экспертной организации, в которой должна быть произведена экспертиза, а также вопросы, поставленные перед экспертом (ч.1 ст.179 УПК КР). Проведение экспертизы может быть поручено государственным и (или) негосударственным экспертам, иным лицам, обладающим специальными познаниями, в том числе из числа лиц, предложенных участниками процесса и не являющихся гражданами Кыргызской Республики (ч.3 ст.179 УПК КР).

В зависимости от предмета исследования, в уголовном процессе могут быть назначены следующие экспертизы:

- *комиссионная* (для проведения сложных экспертных исследований с участием 2 или более экспертов одной специальности) (ст.187 УПК КР);
- *комплексная* (для проведения исследований на основе разных отраслей познаний с участием экспертов различных специальностей в пределах компетенции каждого из них) (ст.188 УПК КР);
- *дополнительная* (при недостаточной ясности или полноте выводов заключения проведенной первичной экспертизы, а также при возникновении необходимости решения новых дополнительных вопросов) (ст.189 УПК КР);
- *повторная* (для исследования тех же объектов и решения тех же вопросов в случаях, когда предыдущее заключение эксперта недостаточно обосновано либо его выводы противоречат фактическим обстоятельствам дела и вызывают сомнение в их правильности, либо были существенно нарушены процессуальные нормы о назначении и производстве экспертизы) (ст.189 УПК КР).

Заключение эксперта (оформленный в письменном виде официальный документ, содержащий ход судебно-экспертного исследования и выводы по вопросам, поставленным перед экспертом следователем, прокурором, судом), а также его показания (сведения, сообщенные им на допросе, проведенном после получения его заключения в целях разъяснения или уточнения данного заключения) являются самостоятельными источниками доказательства (ч.2 ст.80, ст.84 УПК КР). Так же, как и специалист, эксперт сам не должен быть заинтересованным в исходе дела (ч.1 ст.56 УПК КР) и его участие в деле может быть

[56] Не допускается назначение экспертизы по правовым вопросам (ч.3 ст.56 УПК КР), что справедливо, поскольку правовые вопросы решаются судом, который и считается наилучшим экспертом в области права.

отведено в случаях, когда есть обстоятельства, исключающие его незаинтересованность в исходе дела или свидетельствующие об его некомпетентности (ст.72 УПК КР). Объективность и беспристрастность эксперта также обеспечиваются принятием государством мер безопасности от посягательства на его жизнь или иного насилия в связи с рассмотрением дел в суде или досудебном производстве (ст.75 УПК КР). Для признания заключения и показания эксперта допустимыми доказательствами по делу, они должны быть включены в опись материалов уголовного дела (ч.4 ст.80 УПК КР). Злоупотребление полномочиями эксперта, а также заведомо ложные показания или заводомо ложные заключения эксперта, а равно отказ от дачи заключения или показания влекут уголовную ответственность (ст.248, 364, 365 УК КР).

Правовой статус эксперта как участника уголовного процесса не ограничивается исключительно процессуальными нормами. Закон Кыргызской «О судебно-экспертной деятельности» от 24 июня 2013 года №100 (далее «Закон») определяет правовую основу, организационные принципы и основные направления судебно-экспертной деятельности в Кыргызской Республике, а также регулирует правоотношения, возникающие при осуществлении судебно-экспертной деятельности. В частности, Закон устанавливает принципы судебно-экспертной деятельности (законность, соблюдение прав и свобод человека и гражданина, независимость судебного эксперта, объективность, всесторонность и полнота исследований, соблюдение профессиональной этики, а также допустимость использования средств и методов проведения судебно-экспертных исследований) (ст.4-10 Закона). В Законе дана классификация судебно-экспертных организаций, а также определены виды экспертиз, проводимых государственной и негосударственной экспертной организациями. В Законе также установлены профессиональные и квалификационные требования, предъявляемые к экспертам, а также порядок их сертификации и учета. Отдельные главы Закона посвящены регламентации вопросов, возникающих в процессе назначения, производства и оформления результатов судебной экспертизы, а также финансовому, организационному, научно-методическому и информационному обеспечению деятельности судебно-экспертных организаций.

Далее, подзаконными актами регламентированы вопросы назначения и проведения отдельных видов судебных экспертиз (судебно-медицинской экспертизы,[57] в том числе трупа,[58] вещественных доказательств и установления

[57] См.: Правила производства судебно-медицинских экспертиз в Кыргызской Республике, утв. постановлением Правительства Кыргызской Республики от 12 января 2012 года №33.

[58] См.: Правила производства судебно-медицинской экспертизы трупа, утв. постановлением Правительства Кыргызской Республики от 12 января 2012 года №33.

родства,[59] судебно-психиатрической экспертизы,[60] медико-криминалистической и медико-автотехнической экспертизы[61] и др.). Совместным приказом Министерства юстиции Кыргызской Республики, Министерства здравоохранения Кыргызской Республики, Министерства внутренних дел Кыргызской Республики, Государственной службы по контролю наркотиков при Правительстве Кыргызской Республики утверждены Классификатор экспертных специальностей, квалификационные требования, предъявляемые к судебным экспертам Кыргызской Республики, а также Положение «Об организации профессиональной подготовки и повышения квалификации судебных экспертов Кыргызской Республики»[62].

В Кыргызской Республике создан и функционирует специальный государственный орган – Судебно-экспертная служба при Министерстве юстиции Кыргызской Республики (далее – СЭС), призванная осуществлять политику в сфере судебно-экспертной деятельности в Кыргызской Республике. К основным задачам СЭС отнесены:

- организация и осуществление судебно-экспертной деятельности;
- оказание методической и методологической помощи судебным и правоохранительным органам в применении специальных знаний и технических средств;
- обеспечение обучения в области судебной экспертизы;
- организация подготовки и повышения квалификации судебных экспертов[63].

### 3.2.1. Проблемы терминологии при экспертизе цифровой информации

При рассмотрении вопросов назначения и проведения экспертизы цифровой информации в уголовном судопроизводстве следует учесть следующее:

Во-первых, появившееся на английском языке и распространенное в академических и практических материалах словосочетание digital forensics не имеет четкого и емкого перевода на русский язык. В исследованных нами источниках можно встретить такие варианты, как «цифровая криминалистика»,

[59] См.: Правила производства судебно-медицинской экспертизы вещественных доказательств и установления родства в судебно-биологических отделениях лабораторий центра судебно-медицинской экспертизы, утв. утв. постановлением Правительства Кыргызской Республики от 12 января 2012 года №33.

[60] См.: Инструкция об организации производства судебно-психиатрических экспертиз в отделе судебно-психиатрической экспертизы государственных психиатрических организаций, утв. Приказом Министерства здравоохранения Кыргызской Республики от 12 сентября 2014 года №521

[61] См.: Правила организации производства комплексных медико-криминалистических и медико-автотехнических экспертиз, постановлением Правительства Кыргызской Республики от 12 января 2012 года №33.

[62] См.: Совместный приказ Министерства юстиции Кыргызской Республики от 13 июля 2015 года №84, Министерства здравоохранения Кыргызской Республики от 1 июля 2015 года №376, Министерства внутренних дел Кыргызской Республики от 9 июля 2015 года №694, Государственной службы по контролю наркотиков при Правительстве Кыргызской Республики от 8 июля 2015 года №100.

[63] См.: Положение о Судебно-экспертной службе при Министерстве юстиции Кыргызской Республики, утв. постановлением Кабинета Министров Кыргызской Республики от 21 июня 2021 года №33.

«цифровая экспертиза», «цифровая криминалистическая экспертиза», «судебная цифровая экспертиза» и др.

Во-вторых, в Классификаторе экспертных специальностей[64] отсутствует какое-либо упоминание об экспертизе цифровой информации в качестве самостоятельного вида экспертизы. Судя по контексту данного документа, а также по ответу СЭС,[65] мы полагаем, что законодательство Кыргызской Республики относит экспертизу цифровой информации к компьютерно-технической экспертизе.

Кроме этого, следует добавить, что в контексте рассматриваемой тематики экспертиза сознательно называется судебной, в том числе в законодательстве и академической литературе, поскольку она часто назначается в рамках судопроизводства, а ее результаты используются для определения истинности фактов или для определения причины и обстоятельств происшествия, исследуемого в рамках конкретного дела.

Таким образом, для обеспечения устойчивости дефиниций, применяемых в законодательстве и правоприменительной практике, в данном исследовании мы будем использовать устоявшийся термин «судебная компьютерно-техническая экспертиза». Кроме этого, как будет показано в дальнейшем, данный термин обладает родовыми признаками и семантически включает в себя все компоненты экспертного исследования, как аппаратные объекты (компьютеры, периферийные устройства, серверы, мобильные телефоны, карты памяти и др.), так и программные обеспечения и информационные данные, а также сетевую инфраструктуру.[66]

### 3.2.2. Судебная компьютерно-техническая экспертиза как источник доказательств по уголовным делам

С процессуальной точки зрения, судебная компьютерно-техническая экспертиза (далее – СКТЭ) назначается и производится в общем порядке, т.е. так же, как и назначается и производится любая другая экспертиза.

СКТЭ не отнесена к числу экспертиз, проводимых исключительно государственными экспертными учреждениями, следовательно, проведение СКТЭ может быть поручено любому эксперту или экспертной организации, в том числе из числа негосударственных. Как и любая экспертиза, СКТЭ может быть первоначальной, повторной, дополнительной, комиссионной или комплексной.

---

[64] См.: Совместный приказ Министерства юстиции Кыргызской Республики от 13 июля 2015 года №84, Министерства здравоохранения Кыргызской Республики от 1 июля 2015 года №376, Министерства внутренних дел Кыргызской Республики от 9 июля 2015 года №694, Государственной службы по контролю наркотиков при Правительстве Кыргызской Республики от 8 июля 2015 года №100.

[65] Ответ Судебно-экспертной службы при Министерстве юстиции Кыргызской Республики (№05-20/100 от 09 ноября 2022 года) на наш запрос.

[66] Сысенко А.Р., Смирнова И.С., Тимошенко С.Е. Проблемы назначения и производства судебной компьютерно-технической экспертизы. Сибирское юридическое обозрение. 2020, №4.

Несмотря на то, что в законодательстве Кыргызской Республики экспертной специальностью СКТЭ названо только исследование информационных компьютерных средств[67], а в теории криминалистики предмет исследования СКТЭ является дискуссионным,[68] на практике есть относительный компромисс о том, СКТЭ состоит из следующих компонентов, каждый из которых охватывает достаточно широкий круг объектов и вопросов для исследования:[69]

| Компонент СКТЭ | Объект исследования | Наиболее типичные вопросы для исследования |
|---|---|---|
| Экспертиза аппаратных средств | Все виды персональных компьютеров, серверы, периферийные устройства, сетевые аппаратные средства, мобильные телефоны, встроенные системы на основе микропроцессорных контроллеров, любые комплектующие изделия всех указанных компонентов (аппаратных блоков, плат расширения, микросхем и др.), микросхемы памяти, магнитные и лазерные диски, магнитооптические диски, магнитные ленты, карты памяти и др. | • Относится ли представленное устройство к аппаратным компьютерным средствам и к какому типу (марке, модели) относится аппаратное средство?<br>• Каково функциональное предназначение представленного аппаратного средства, используются ли данное аппаратное средство для решения конкретной функциональной задачи?<br>• Каково фактическое состояние (исправен, неисправен) представленного аппаратного средства? Имеются ли в нем отклонения от типовых (нормальных) параметров, в т.ч. физические дефекты?<br>• Является ли представленное аппаратное средство носителем информации и какой вид (тип, модель, марку, емкость) имеет представленный носитель информации?<br>• Доступен ли для чтения представленный носитель информации, если не доступен, то каковы причины отсутствия доступа к носителю информации? |
| Экспертиза программных средств | Операционные системы, утилиты, средства разработки и отладки программ, служебная системная информация, приложения общего назначения: тестовые и графические редакторы, редакторы презентаций и т.д. | • Какова общая характеристика представленного программного обеспечения, из каких компонентов (программных средств) оно состоит?<br>• Обладает ли они признаками контрафактности либо нет?<br>• Какое общее функциональное предназначение имеет программное средство?<br>• Имеет ли программное средство защитные возможности (программные, аппаратно-программные) от несанкционированного доступа и копирования?<br>• Какова хронология использования программного средства (начиная с ее инсталляции)?<br>• Соответствует ли разработанное программное обеспечение требования договора и технического задания, нормативно-технической документации? Если не соответствует, то в чем выражаются данные несоответствия?<br>• Имеются ли в программном средстве враждебные функции, которые влекут уничтожение, блокирование, модификацию либо копирование информации, нарушение работы компьютерной сети? |
| Экспертиза информации (экспертиза данных) | Файлы с расширениями текстовых форматов (.txt, .doc), графических форматов (.bmp, .jpg, .tif, .cdr), форматов баз данных (.dbf, .mdb), электронных таблиц (.xls, .cal) и др. | • Какие свойства, характеристики и параметры (объемы, даты создания/изменения, атрибуты и др.) имеют данные на носителе информации?<br>• Какого вида (явный, скрытый, удаленный, архив) имеется информация на носителе? |

[67] См.: Совместный приказ Министерства юстиции Кыргызской Республики от 13 июля 2015 года №84, Министерства здравоохранения Кыргызской Республики от 1 июля 2015 года №376, Министерства внутренних дел Кыргызской Республики от 9 июля 2015 года №694, Государственной службы по контролю наркотиков при Правительстве Кыргызской Республики от 8 июля 2015 года №100.

[68] Сысенко А.Р., Смирнова И.С., Тимошенко С.Е. Проблемы назначения и производства судебной компьютерно-технической экспертизы. Сибирское юридическое обозрение. 2020, №4.

[69] Ответ Судебно-экспертной службы при Министерстве юстиции Кыргызской Республики (№05-20/100 от 09 ноября 2022 года) на наш запрос.

| | | |
|---|---|---|
| | | • Каким образом организован доступ (свободный, ограниченный и пр.) к данным на носителе информации и каковы его характеристики?<br>• Какие несоответствия типовому представлению имеются в выявленных данных (нарушение целостности, несоответствие формата, вредоносные включения и пр.) имеются в данных?<br>• Каким способом и при каких обстоятельствах произведения действия (операции) (блокирование, модификация, копирование, удаление) определенных данных на носителе информации? |
| Экспертиза сети | Сетевое оборудование, модемы, WiFi роутер, сетевые платы, средства связи и коммуникации | • Установить/подтвердить факт отправки/получения электронного письма с электронного ящика «электронный@ящик». Каковы дата/время отправки электронного письма? Возможно ли достоверно установить факт доставки пользователям отправленного письма?<br>• Осуществлялся ли выход в сеть Интернет с представленного на исследование системного блока (ноутбука, смартфона)? Провести фиксацию имеющихся посещений в определенный промежуток времени?<br>• Осуществлялось ли удаленное подключение к представленному на исследование системному блоку (ноутбуку, смартфону)? Какие признаки указывают о наличии установленных подключений?<br>• Была ли опубликована информация «следующего характера» на сайте «сайт»? |

К сожалению, информация об использовании результатов СКТЭ в реальных уголовных делах не является публичной. Из ответа СЭС на наш запрос следует, что в среднем за 1 календарный год Отдел судебной комьпютерно-технической экспертизы СЭС проводит от 100 до 140 СКТЭ. При этом, средняя продолжительность проведения СКТЭ занимает около 30 календарных дней.

В отсутствие утвержденной методологии или стандартов проведения СКТЭ, крайне сложно оценить, насколько СКТЭ оказывает содействие в установлении обстоятельств, имеющих значение для дела и выполняет основную свою доказательственную функцию. Тем не менее, из отдельных приговоров по уголовным делам можно сделать вывод, что результаты СКТЭ, несмотря на то, что принимаются судами в качестве бесспорного доказательства, по нашему мнению, не отличаются глубиной и разнообразием исследования, и по сути, не решают задачи по обеспечению допустимости цифровых доказательств.

Так, в деле №УД-38/22Ба3, приводя в приговоре факт отрицания обвиняемым публикации запрещенных материалов посредством профиля в Odnoklassniki, суд не указал каких-либо доводов, доказывающих обратное и опровергающих позицию обвиняемого, что не помешало ему вынести обвинительный приговор. Предмет судебно-технической экспертизы, назначенной по делу, был ограничен заключением о том, что *«в социальной сети «Одноклассники» создан профиль под наименованием «И*******», который является закрытым»,* и что на этот профиль *«подписаны 78 друзей»,* и через него «оставлены 60 заметок». Кроме этого, в заключении эксперта отмечено, что «*из-за того, что профиль является закрытым,*

*то все посты, заметки, фото, видео доступны только 78 подписчикам»,* и *«недоступны пользователям, не являющимся друзьями»,* и что «*постороннее лицо не может загружать материалы, не зная пароль и логин от профиля в социальной сети «Одноклассники».*[70] Другими словами, обстоятельство, имеющее значение для правильного разрешения дела (а именно, факт распространения обвиняемым запрещенных материалов), было расценено как доказанное не на базе точных и неопровержимых данных, а посредством *допущения*, что раз постороннее лицо не может размещать публикации, то владелец аккаунта их и разместил.

В деле №УД-739/22-О6 техническая экспертиза по другому делу в отношении к профилю обвиняемого в Facebook пришла к таким же выводам.[71]

### 3.2.3. Юридические вопросы регламентации процесса СКТЭ

Из ответа СЭС на наш запрос следует, что эксперты при производстве СКТЭ руководствуются общими нормативными правовыми актами, регламентирующими процесс производства судебной экспертизы *вообще*. К последним СЭС относит Закон Кыргызской Республики «О судебно-экспортной деятельности», Положение о Судебно-экспертной службе при Министерстве юстиции Кыргызской Республики, утв. постановлением Кабинета Министров Кыргызской Республики от 21 июня 2021 года №33, Инструкцию о производстве судебной экспертизы Судебно-экспертной службе при Министерстве юстиции Кыргызской Республики, утв. постановлением Правительства Кыргызской Республики от 25 сентября 2012 года №648, а также отдельные статьи УПК КР, названные в данном исследовании. Следует подчеркнуть, что эти нормативные правовые документы применимы к любым видам судебных экспертиз и в них нет каких-либо положений, посвященных конкретно вопросам назначения и производства СКТЭ. Анализ законодательства Кыргызской Республики, проведенный нами, также подтверждает тезис о том, что в стране отсутствует специальный нормативный акт, определяющий порядок сбора и исследования цифровых доказательств в рамках уголовного процесса, в том числе в порядке производства СКТЭ. Более того, мы убеждаемся (и ответ СЭС это косвенно подтверждает), что в Кыргызстане отсутствуют методические руководства или рекомендации по работе с цифровыми доказательствами, а практика и проблемы СКТЭ вовсе не анализируется и не обобщается в какие-либо прикладные материалы для экспертного сообщества.

Может показаться, что процесс производства судебной экспертизы не требует правовой регламентации, поскольку сфера знаний судебного эксперта является настолько специфичной, что не может быть урегулирована. Вместе с тем, это не так, и как и любая деятельность, процесс проведения судебной экспертизы может быть регламентирован. В пример этому можно привести ряд нормативных

[70] Приговор Кызыл-Кийского районного суда Баткенской области от 10 октября 2022 года (Дело №УД-38/22Ба3).
[71] Приговор Ошского городского суда от 20 октября 2022 года (Дело №УД-739/22-О6).

правовых актов Кыргызской Республики, призванных регулировать вопросы проведения отдельных судебных экспертиз, в том числе специфичные вопросы из сферы специальных отраслей знаний.[72]

Необходимость регулирования процесса производства судебной экспертизы обоснована несколькими соображениями. Формализация процесса судебной экспертизы может помочь обеспечить его последовательное и надежное проведение, что может повысить точность результатов судебной экспертизы. Регламентированный процесс судебной экспертизы может обеспечить его прозрачность, а также установить меры контроля качества (такие как внутренние аудиты и внешняя аккредитация), которые в конечном итоге могут гарантировать высокое качество и достоверность результатов судебной экспертизы. Кроме этого, регулирование процесса проведения экспертизы приводит к его унификации, когда разные эксперты и экспертные организации последовательно применяют одни и те же методы и протоколы, что снижает риск ошибок, предвзятости и несоответствий в результатах. Такой подход может способствовать повышению профессионализма и высокоэтического поведения в соответствующей области, что может помочь предотвратить неправомерные действия и злоупотребления в процессе судебной экспертизы. В конечном итоге, безусловно, следование формальным правилам судебной экспертизы может облегчить принятие результатов органами правосудия как юридически приемлемых и допустимых источников доказательства по делу.

С учетом вышеизложенного, мы поддерживаем идею о разработке и утверждении нормативного правового акта, регламентирующего процесс сбора и исследования цифровых доказательств, в том числе в процессе проведения СКТЭ.

Вместе с тем, при разработке нормативных актов, призванных регламентировать процесс производства СКТЭ, следует исходить из того, чтобы обеспечить оптимальный баланс между так называемым «жестким правом» (нормативным правовым регулированием СКТЭ в форме официально утвержденного документа, обязательного исполнению всеми адресатами) и «мягким правом» (совокупностью правил поведения, принципов, стандартов, практик, которые носят рекомендательный характер). Бесспорно, что допустимость результатов СКТЭ как источников доказательств по делу должна быть оценена с точки зрения соблюдения норм «жесткого права», тогда как «мягкое право» должно оказывать содействие экспертам в применении лучших подходов к СКТЭ.

[72] К примеру: Правила производства судебно-медицинской экспертизы вещественных доказательств и установления родства в судебно-биологических отделениях лабораторий центра судебно-медицинской экспертизы, утв. постановлением Правительства Кыргызской Республики от 12 января 2012 года №33, которым регламентированы вопросы проведения судебно-медицинских экспертиз крови, спермы, слюны, пота, мочи, волос и прочих объектов.

**КЛЮЧЕВЫЕ ВЫВОДЫ:**

1. Правила привлечения специалистов к сбору цифровых доказательств регламентированы в УПК КР. При этом:
    - УПК КР предоставляет широкие полномочия следственным органам в определении необходимости привлечения специалистов к следственным действиям, в том числе, к тем из них, предметом которых является сбор, изъятие, исследование или оценка цифровых доказательств.
    - УПК не определяет квалификационные требования к специалистам.
2. Правила привлечения экспертов к исследованию цифровых доказательств регламентированы УПК КР, специальным законом, а также рядом подзаконных актов Правительства КР и профильных министерств и ведомств. При этом:
    - Есть теоретические разногласия относительно правильного наименования экспертизы, назначаемой для исследования цифровых доказательств, а также предмета ее исследования.
    - СЭС МЮ КР проводит судебную компьютерно-техническую экспертизу (СКТЭ), в состав которой входит экспертиза аппаратных средств, экспертиза программных средств, экспертиза информации (данных), экспертиза сети.
    - СКТЭ проводится на базе общих нормативных правовых актов и в КР отсутствуют какие-либо специальные правила, регламентирующие вопросы проведения СКТЭ.

# 5. ЮРИДИЧЕСКИЕ ВОПРОСЫ ИНТЕГРАЦИИ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОЕ ПРОЦЕССУАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО КЫРГЫЗСКОЙ РЕСПУБЛИКИ

## 5.1. Принципиальные вопросы интеграции цифровых доказательств в уголовное процессуальное законодательство Кыргызской Республики

Мы считаем, что целостность и внутренняя согласованность государственного подхода к вопросам регламентации работы с цифровыми доказательствами могут быть обеспечены за счет правильного разрешения следующих принципиальных вопросов:

### 1) Определение места цифровых доказательств в системе доказательств по уголовным делам

Несмотря на то, что цифровые доказательства обладают юридически значимыми особенностями (см.: раздел 2.2. настоящего исследования), что, безусловно, влияет на то, как работа с ними должна быть регламентирована, цифровые доказательства, все же, должны оставаться одним из элементов действующей системы источников доказательств по уголовным делам. Нам представляется правильной позиция ряда авторов, согласно которой цифровые доказательства выступают как *видовое* понятие к термину «доказательство», и, следовательно, не формируют собой параллельную систему цифровых доказательств по уголовному делу. Практическое значение такого подхода заключается в том, что все сущностные и формальные требования УПК КР к «обычным» доказательствам в равной степени должны распространяться также на и цифровые доказательства. В частности, цифровые доказательства (как и «обычные», традиционные доказательства) используются в целях определения наличия или отсутствия обстоятельств, имеющих значение для дела, а суд основывает свое решение лишь на тех доказательствах, участие в исследовании которых на равных основаниях было обеспечено каждой из сторон. Кроме этого, суд не вправе собирать дополнительные доказательства в целях устранения неполноты следствия. Никакие доказательства, в том числе цифровые, не имеют заранее установленной силы и оцениваются судьей в совокупности. Критерии относимости, допустимости, достоверности и достаточности доказательств (см.: раздел 3.2. настоящего исследования) в равной степени могут применяться и к цифровым доказательствам.

Сказанное совсем не отменяет необходимость того, что отдельные вопросы сбора, исследования и оценки цифровых доказательств могут быть дополнительно уточнены и урегулированы в уголовном процессуальном законодательстве.

Следовательно, разрабатывая проект изменений в УПК КР в целях внедрения цифровых доказательств в уголовное судопроизводство, нормы следует излагать,

с одной стороны, с учетом действующей системы источников доказательств, а с другой стороны – гармонично «встраивать» в текстуру УПК КР необходимые нормы по отдельным вопросам сбора, исследования и оценки цифровых доказательств, избегая создания смысловых коллизий и противоречий с действующими нормами УПК КР.

**2) Сохранность конституционно-правовых гарантий неприкосновенности тайны личности**

Мы убеждены, что при интеграции цифровых доказательств в уголовное процессуальное законодательство должны быть сохранены действующие конституционно-правовые гарантии, установленные, как в самой Конституции Кыргызской Республики, так и в УПК КР, и направленные на обеспечение защиты прав и свобод человека и гражданина при осуществлении правосудия по уголовным делам. В частности, применение следственными органами передовых технологий сбора цифровых доказательств не может оправдывать ослабление гарантий неприкосновенности тайны личности и его частной жизни, охраны прав и свобод человека и гражданина в уголовном судопроизводстве, включая защиты от незаконного и необоснованного использования информации и охраны тайны переписки в самом широком смысле слова. Напротив, в отдельных случаях есть необходимость расширить действие юридических гарантий на случаи сбора цифровых доказательств по уголовным делам.

Необходимость соблюдения конституционно-правовых гарантий при интеграции цифровых доказательств в систему правосудия по уголовным делам неизбежно ставит вопрос о поиске балансе между публичными и частными интересами в уголовном судопроизводстве. Естественный конфликт указанных интересов – публичный интерес в установлении вины обвиняемого и привлечения к ответственности против частного интереса в сохранении тайны частной жизни – не может быть разрешен за счет умаления одного из них.

Ключевой способ достижения баланса между публичными и частными интересами при расследовании преступлений находится в процессуальной плоскости – это соблюдение закона и процедурных требований, которые обеспечивают защиту прав и свобод человека, такие как право на конфиденциальность и недопущение незаконного поиска и сбора доказательств. В этой же логике должен функционировать специальный институт, введенный в уголовное процессуальное законодательство Кыргызстана с недавних пор – следственный судья, призванный осуществлять судебный контроль за законностью действий (бездействия) и решений должностного лица органа дознания, следователя, руководителя следственной группы, прокурора, и обладающий достаточно широкими полномочиями на всех стадиях следствия.

Следовательно, в контексте интеграции цифровых доказательств необходимо расширять контрольные полномочия следственного судьи в вопросах проверки законности действий следственных органов при работе с цифровыми доказательствами.

### 3) Юридические основы сотрудничества следственных органов с провайдерами цифровой информации

При интеграции цифровых доказательств в уголовное процессуальное законодательство неизбежно возникает вопрос о правовом статусе, правах и обязанностях провайдеров цифровой информации, имеющей доказательственное значение для уголовного дела. Поскольку провайдерами являются, как правило, держатели массива персональных и других чувствительных данных, по нашему мнению, данный вопрос также должен быть решен законодателем с учетом вышеуказанных конституционно-правовых гарантий неприкосновенности тайны личности. Другими словами, взаимоотношения между следственными органами и провайдерами информации должны быть основаны на таких юридических нормах, которые гарантируют применение мер по обеспечению гарантий неприкосновенности тайны личной жизни человека и исключают злоупотребление властью и полномочиями.

В этом контексте есть интересный кейс из практики Кыргызстана.

*Постановлением Правительства Кыргызской Республики от 30 июня 2014 года №360 была утверждена Инструкция о порядке взаимодействия операторов электросвязи и операторов мобильной сотовой связи с государственными органами Кыргызской Республики, осуществляющими оперативно-розыскную деятельность, согласно которой была введена СОРМ – система обеспечения оперативно-розыскных мероприятий. Приобрести, установить и ввести технические средства СОРМ в эксплуатацию должны операторы электросвязи и операторы мобильной связи за свой счет, а пользователем объявлен орган национальной безопасности. Операторы связи обязаны обеспечить пользователю СОРМ пассивный доступ в базу данных об абонентах и оказанных им услугах связи, круглосуточно в режиме реального времени по организованным каналам удаленного доступа, для проведения оперативно-розыскных мероприятий в соответствии с законодательством Кыргызской Республики. Вопрос о конституционности отдельных положений данного нормативного правового акта, а также части 1 статьи 21-1 Закона Кыргызской Республики «Об электрической и почтовой связи», нормативных положений части 3, части 5 статьи 7 Закона Кыргызской Республики «Об оперативно-розыскной деятельности» был рассмотрен Конституционным судом Кыргызской Республики, который не посчитал его непротиворечащим положениям Конституции Кыргызской Республики в части гарантии прав личности на прикосновенность частной жизни.*[73]

[73] Решение Конституционной Палаты Верховного Суда Кыргызской Республики от 22 апреля 2015 года N 7-р.

*Доводы Констиционного суда Кыргызской Республики были построены на допустимости негласного собирания данных граждан органами национальной безопасности в целях оперативно-розыскной деятельности (защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств).*[74]

В свете применения цифровых доказательств по уголовным делам мы бы хотели акцентировать внимание на чрезвычайной важности соблюдения конституционных гарантий неприкосновенности личности и допустимость сбора доказательств *ex post*, по фактам состоявшегося события преступления и в процессе следственных действий по конкретному уголовному делу, под судебным контролем и в пределах относимости к расследуемым событиям. Негласный сбор данных, в том числе в формате прослушивания и записи переговоров без привязки к какому-либо событию преступления или безотносительно к предмету доказывания по уголовному делу следует признать опасным прецедентом в нарушении прав человека.[75] Поэтому, проект законодательного акта по внедрению цифровых доказательств в уголовное процессуальное законодательство должен быть усилен дополнительными процессуальными гарантиями соблюдения прав на неприкосновенность личной жизни участников уголовного процесса.

Кроме этого, в силу того, что цифровые данные, используемые в уголовном деле, могут иметь трансграничный характер, сотрудничество следственных органов с провайдерами цифровой информации может иметь различные формы.

Во-первых, цифровые доказательства, находящиеся под юрисдикцией иностранного государства, могут быть запрошены и получены у органов иностранного государства в порядке оказания правовой помощи на основании двусторонних и многосторонних международных соглашений, участницей которых является Кыргызская Республика либо дипломатическим путем (глава 59 УПК КР). Следовательно, применение цифровых доказательств в уголовных делах имеет также международный аспект и ставит перед правоохранительными органами задачи по налаживанию сотрудничества с иностранными государствами по вопросам сотрудничества по обмену цифровыми данными.

Во-вторых, держателями цифровых данных, которые потенциально могут иметь доказательственное значение для уголовного дела, чаще всего, являются

[74] Пока проводилось данное исследование, Кабинет Министров Кыргызской Республики своим постановлением от 16 ноября 2022 года №626 расширил основания для сбора данных посредством СОРМ, к которым теперь относятся не только случаи, установленные в Законе Кыргызской Республики «Об оперативно-розыскной деятельности», но и случаи, предусмотренные Законом Кыргызской Республики «О контрразведывательной деятельности» и УПК КР (в части осуществления специальных следственных действий). Теоретически, в виду расширения сферы применения СОРМ за пределы целей, признанных конституционными, вопрос о конституционности нововведений может быть поставлен перед Конституционным Судом Кыргызской Республики. Кроме этого, постановлением Кабинета Министров Кыргызской Республики от 13 января 2023 года № 6 внесены изменения в Положение о Координационном центре по обеспечению кибербезопасности Государственного комитета национальной безопасности Кыргызской Республики, согласно которым к функциям последнего отнесены, помимо прочего, проведение контрразведывательных мероприятий.

[75] МВД признало факт «прослушки» десятков граждан. Насколько это было законно? (https://rus.azattyk.org/a/mvd-priznalo-fakt-proslushki-desyatkov-grazhdan-naskolko-eto-bylo-zakonno/31439035.html)

частные организации, созданные и функционирующие в различных юрисдикциях и относящиеся к т.н. ИТ-гигантам. К примеру, отношения между Google (зарегистрирована в соответствии с законами штата Делавэр (США) и осуществляет деятельность согласно праву США) и его пользователем из Кыргызстана регламентируются Политикой конфиденциальности и Условиями пользования, и носят гражданско-правовой характер, а все споры между ними, связанные с использованием сервисов Google, независимо от норм коллизионного права, разрешаются в соответствии с правом штата Калифорния (США). Такие споры находятся в исключительной компетенции судов федерального уровня или уровня штата, расположенных в округе Санта-Клара (штат Калифорния, США).[76] Google применяет стандарты GDPR[77] на территории Европейского Союза, а глобально – нацелена соответствовать с аналогичными требованиями по защите персональных данных. Несмотря на отдельные различия в юрисдикциях, глобально Google, в ответ на запрос органов государственных власти отдельных стран на раскрытие данных, может предоставить их, «если это не противоречит» законодательству страны, государственные органы которой направили запрос, что означает, что «государственное учреждение должно соблюдать те же правовые процедуры и юридические требования, которые действуют при отправке запросов местным поставщикам аналогичных услуг».[78] Следовательно, в контексте сбора цифровых доказательства в рамках уголовного дела, правила коммуникации следственных органов должны быть одинаковыми для местных и иностранных провайдеров информации, а также исполнимы и приемлемы с точки зрения стандартов, которыми руководствуются держатели крупных массивов цифровых данных.[79] В практическом плане это означает, что при законодательной регламентации правил запроса цифровой информации следует учесть лучшие международные практики по этой теме.

### 4) Переосмысление критериев допустимости цифровых доказательств

Несмотря на то, что на цифровые доказательства распространяются общие требования уголовного процессуального законодательства о допустимости доказательств, мы убеждаемся в том, что необходимо ввести дополнительные

[76] Политика конфиденциальности и Условия использования (https://policies.google.com/terms?hl=ru#toc-intro)

[77] General Data Protection Regulation (GDPR) – это правила, принятые Европейским Союзом (ЕС), для укрепления и унификации защиты данных для каждого жителя ЕС. Вступили в силу 25 мая 2018 года. GDPR регулирует сбор, хранение, использование и распространение личной информации граждан ЕС. GDPR устанавливает ряд прав для граждан в отношении их личной информации, включая право на доступ, исправление и удаление личной информации, а также право быть информированным о сборе и обработке данных. GDPR применяется к любой компании, которая обрабатывает личные данные граждан ЕС, независимо от того, где расположена компания. См.: (https://ec.europa.eu/info/law/law-topic/data-protection_en).

[78] Действия Google при получении запросов госорганов на получение пользовательских данных (https://policies.google.com/terms/information-requests)

[79] Примечательно, что в Отчете Google о доступности сервисов и данных за весь период ведения отчета (с июля 2009 года) Кыргызская Республика не указана среди стран, из которых поступили запросы государственных органов на разглашение пользовательских данных. Это означает, что в Кыргызстане вообще не практикуется обращение в Google за получением данных пользователей, включая по уголовным делам (https://transparencyreport.google.com/user-data/overview?hl=ru).

критерии допустимости цифровых доказательств. Это связано со спецификой природы цифровых доказательств, которые, как мы отмечали, могут быть легко изменены или подделаны, а обеспечение аутентичности цифровых доказательств играет крайне важную роль в отправлении справедливого правосудия. Введение дополнительных критериев допустимости цифровых доказательств может помочь обеспечить их достоверность и надежность в уголовном процессе. Эти критерии могут включать разные меры, в том числе общую регламентацию процесса сбора, исследования, оценки и документирования цифровых доказательств, требование обеспечения «цепочки хранения»[80], участие специалистов в следственных и судебных действиях, использование технических средств подтверждения аутентичности цифровых доказательств на всех стадиях следствия и судебного исследования, исследование показаний и заключений экспертов, введение квалификационных требований к ним и их методам, введение правил запроса и получения цифровой информации у других незаинтересованных в исходе дела лиц и др.

При этом, важно заметить, что, допуская использование средств современной технологии в отправлении правосудия в качестве критериев допустимости цифровых доказательств, необходимо обеспечить технологическую нейтральность законодательства, т.е. внедрять такие нормы, которые нейтральны к используемым технологиям и не предпочитают одну технологию над другой, а также не устаревает в долгосрочной перспективе. Законодательство по умолчанию проигрывает гонку с техническим прогрессом, и поэтому, чтобы адекватно регулировать вопросы в данной сфере, оно должно оперировать сущностными признаками явлений, а не быть привязанным к текущим технологиям.

### 5.2. Механизм интеграции цифровых доказательств в уголовное процессуальное законодательство Кыргызской Республики

Безусловно, цифровые доказательства будут интегрированы в уголовное процессуальное законодательство Кыргызской Республики посредством принятия ряда нормативных правовых актов разного содержания и юридической силы. Рассмотрев всю тематику изнутри, проанализировав действующее уголовное процессуальное законодательство и правоприменительную практику по уголовным делам, с учетом технических вопросов, неизбежно сопровождающих процесс сбора, исследования и оценки цифровых доказательств, мы предлагаем к обсуждению проекты 2 нормативных документов, нацеленных на регулирование вопросов использования цифровых доказательств в уголовных делах:

[80] Цепочка хранения – четкая и непрерывная последовательность хранения цифровых доказательств, включая документирование времени, даты и места получения, а также данных лиц, которые работали с доказательствами. Подробнее: см. раздел 2.3. настоящего исследования («Общепризнанные стандарты использования цифровых доказательств»).

1) **Проект Закона Кыргызской Республики «О внесении изменений и дополнений в Уголовно-процессуальный кодекс Кыргызской Республики»**

Данный Законопроект направлен на создание юридической базы для применения цифровых доказательств, а также методов и средств компьютерной криминалистики, применимых при сборе, исследовании и оценке цифровых доказательств. В Законопроекте предлагается внести в УПК КР новые нормы, которые определяют легальное понятие и юридическую силу цифровых доказательств в системе источников доказательств, их сущностные характеристики, а также специальные требования к допустимости цифровых доказательств. Законопроект обеспечивает единообразие терминологии, используемой при работе с цифровыми доказательствами. Законопроект вносит ряд дополнений к регламенту совершения отдельных следственных и судебных действий, которые направлены на учет специфики природы цифровых доказательств. Законопроект также создает правовую базу для широкого применения специальных знаний специалистов и экспертов в процессе доказывания обстоятельств, имеющих значение для дела. Кроме этого, Законопроект четко устанавливает роль следственного судьи в осуществлении судебного контрольного над следствием и обеспечении реализации конституционно-правовых гарантий неприкосновенности личности и его частной жизни при сборе цифровых доказательств. Отдельно, Законопроект пересматривает текущие нормы УПК КР, создавая корректную юридическую форму взаимодействия следственных органов с провайдерами цифровой информации, в том числе с теми, которые находятся вне юрисдикции Кыргызской Республики.

2) **Проект Правил сбора, изъятия, хранения и оценки цифровых доказательств**

Данные Правила подробно регламентируют пошаговые действия органов дознания и следствия, специалистов и экспертов при сборе, хранении и экспертизе цифровых доказательств по уголовным делам. В Правилах установлены основные стандарты, подлежащие соблюдению при работе с цифровыми доказательствами, включая обеспечение целостности и аутентичности цифровых доказательств, надлежащее документирование процесса работы с ними, привлечение к работе с цифровыми доказательствами лиц, обладающих специальными знаниями, подготовка органов дознания и повышение их квалификации, а также обеспечение законности на всех стадиях работы с цифровыми доказательствами. Правила дают общую классификацию цифровых доказательств, определяют стадии работы с цифровыми доказательствами (подготовка, планирование, поиск, сбор,

исследование, оценка) и юридически и технически значимые стандарты работы с ними на каждой из этих стадий.

**КЛЮЧЕВЫЕ ВЫВОДЫ:**

1. Интеграция цифровых доказательств в уголовно-процессуальное законодательство КР должна сопровождаться решением ряда принципиальных вопросов:
    - В УПК должно быть определено место цифровых доказательств в системе источников доказательств по уголовному делу.
    - Необходимо сохранить, а в отдельных случаях – расширить действие конституционно-правовых гарантий неприкосновенности тайны личной жизни в ходе уголовного судопроизводства, в том числе посредством усиления статуса следственного судьи в вопросах осуществления судебного контроля над следствием.
    - Необходимо юридически корректно определить правовой статус, права и обязанности, а также приемлемые способы коммуникации с провайдерами цифровой информации, в том числе находящимися вне пределов юрисдикции Кыргызстана.
    - Существующие критерии определения допустимости доказательств должны быть дополнены новыми критериями, применимыми исключительно к цифровым доказательствам.
2. Цифровые доказательства могут быть внедрены в уголовно-процессуальное законодательство КР посредством принятия 2 нормативных правовых актов:
    - Закон о внесении изменений и дополнений в УПК КР (создает юридическую базу для применения цифровых доказательств)
    - Правила сбора, изъятия, хранения и оценки цифровых доказательств (регламентируют пошаговые действия вовлеченных лиц при сборе, хранении и экспертизе цифровых доказательств).

## 6. ПРИЛОЖЕНИЯ

**6.1. Проект Закона Кыргызской Республики «О внесении изменения в Уголовно-процессуальный кодекс Кыргызской Республики»**

**6.2. Проект Правил идентификации, сбора, получения, хранения и исследования цифровой информации в уголовном судопроизводстве**