Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Digital Evidence in Criminal Proceedings: Challenges, Case Law, and Reform Perspectives

Shokhrukhbek SOBIROV[1]

Tashkent State University of Law

ARTICLE INFO

Article history:
Received October 2023
Received in revised form
15 November 2023
Accepted 25 November 2023
Available online
25 January 2024

Keywords:
Digital evidence,
Criminal process,
Privacy rights,
Data minimization,
Judicial oversight,
Legal reform.

ABSTRACT

The article examines the use of digital evidence in criminal proceedings, focusing on the challenges in legal practice in Uzbekistan and international standards. The introduction explores the unique features of digital data, including confidentiality and technical complexity. Key U.S. court precedents, such as Riley v. California and Carpenter v. United States, are discussed as benchmarks for protecting rights during the seizure and analysis of digital evidence. The study highlights legislative gaps in Uzbekistan, such as the absence of data minimization mechanisms and low levels of judicial oversight. Risks of data leaks and misuse during the handling of digital evidence are also detailed. In conclusion, the article provides recommendations for legislative reform: introducing data minimization principles, enhancing judicial control, employing filtering technologies, and enforcing accountability for data breaches. It argues for the modernization of legal norms to balance investigative efficiency and the protection of citizens' constitutional rights.

DOI: https://doi.org/10.47689/2181-1415-vol4- iss6-pp115-127

Jinoyat protsessida raqamli dalillar: muammolar, sud amaliyoti va islohot istiqbollari

Kalit so‘zlar:
raqamli dalillar,
jinoyat protsessi,
shaxsiy daxlsizligi huquq,
ma’lumotlarni
minimallashtirish,

ANNOTATSIYA

Maqolada jinoyat jarayonida raqamli dalillardan foydalanish ko‘rib chiqilgan bo‘lib, O‘zbekistondagi huquqiy amaliyotdagi muammolar va xalqaro standartlarga e’tibor qaratilgan. Kirish qismida raqamli ma’lumotlarning maxfiylik va texnik murakkablik kabi o‘ziga xos xususiyatlari tahlil qilinadi. Riley v.

[1] Independent Applicant, Tashkent State University of Law.

sud nazorati,
qonunchilik islohoti.

California va Carpenter v. United States kabi AQShning asosiy sud pretsedentlari raqamli dalillarni musodara qilish va tahlil qilish jarayonida huquqlarni himoya qilish uchun me’zon sifatida ko‘rib chiqiladi. Tadqiqotda O‘zbekistondagi qonunchilikdagi bo‘shliqlar, jumladan, ma’lumotlarni minimallashtirish mexanizmlarining yo‘qligi va sud nazoratining past darajasi ta’kidlangan. Raqamli dalillar bilan ishlash jarayonida ma’lumotlarning sizib chiqishi va suiiste’mol qilinishi xavflari batafsil yoritiladi. Xulosa qismida qonunchilik islohoti bo‘yicha tavsiyalar taqdim etiladi: ma’lumotlarni minimallashtirish tamoyillarini joriy etish, sud nazoratini kuchaytirish, filtratsiya texnologiyalaridan foydalanish va ma’lumotlarning sizib chiqishi uchun javobgarlikni ta’minlash. Ushbu maqola tergov samaradorligi va fuqarolarning konstitutsiyaviy huquqlarini himoya qilish o‘rtasidagi muvozanatni ta’minlash uchun huquqiy normalarni modernizatsiya qilish zarurligini asoslaydi.

Цифровые доказательства в уголовном процессе: вызовы, судебная практика и перспективы реформирования

Ключевые слова:
цифровые доказательства, уголовный процесс, права на неприкосновенность частной жизни, минимизация данных, судебный контроль, реформа законодательства.

АННОТАЦИЯ

Статья рассматривает использование цифровых доказательств в уголовном процессе, акцентируя внимание на сложностях правоприменительной практики в Узбекистане и международных стандартах. Введение анализирует особенности цифровых носителей информации, такие как конфиденциальность и техническая сложность. Приведены ключевые судебные прецеденты США, включая дела Riley v. California и Carpenter v. United States, которые формируют стандарты защиты прав при изъятии и анализе цифровых данных. Также детализированы проблемы законодательства Узбекистана, включая отсутствие механизма минимизации данных и низкий уровень судебного контроля. Рассмотрены риски утечек и злоупотреблений при работе с цифровыми доказательствами. В заключении представлены рекомендации по реформированию законодательства: внедрение принципа минимизации данных, усиление судебного контроля, применение фильтрационных технологий и установление ответственности за утечку данных. Статья обосновывает необходимость модернизации правовых норм, чтобы сбалансировать эффективность расследований и защиту конституционных прав граждан.

ВВЕДЕНИЕ

В эпоху стремительного развития цифровых технологий правоприменительная практика сталкивается с новыми вызовами, связанными с использованием электронных доказательств в уголовном процессе. Мобильные устройства, компьютеры и другие цифровые носители содержат огромные объемы личной информации: сообщения, фотографии, данные о местоположении, финансовые документы и многое другое. Этот объем данных, помимо своей значимости для расследований, делает обыски цифровых устройств особенно инвазивными, что создает угрозу конфиденциальности личности.

Одной из ключевых проблем становится необходимость соблюдения баланса между эффективностью правоохранительных органов и защитой конституционных прав граждан. В таких странах, как США, этот вопрос уже получил свое развитие благодаря судебным прецедентам, таким как дела **Riley v. California** и **Carpenter v. United States**, где судьи признали, что цифровые устройства содержат данные, которые требуют повышенной защиты.

В Узбекистане и других странах с развивающимся законодательством в области цифровых доказательств эти вопросы находятся в стадии дискуссий. Существующие уголовно-процессуальные нормы часто разрабатывались для работы с физическими доказательствами, что делает их малоэффективными в условиях цифровой эпохи. Данный пробел приводит к рискам нарушений конституционных прав граждан, включая права на защиту частной жизни, персональных данных и тайны переписки.

МЕТОДЫ

Для проведения исследования и формирования рекомендаций использовались следующие подходы:

1. **Анализ законодательства**:

- Проведен сравнительный анализ УПК РУз и законодательства США, регулирующего обыски цифровых устройств. Рассмотрены процессуальные требования к изъятию и анализу цифровых доказательств, а также их соответствие конституционным правам граждан

2. **Судебные прецеденты**:

- Исследованы ключевые дела в США: **Riley v. California** (2014) и **Carpenter v. United States** (2018), в которых Верховный суд определил, что цифровые устройства требуют особого правового подхода.

3. **Сравнительный анализ правоприменительной практики**:

- Рассмотрены процедуры, связанные с изъятием и обработкой цифровых носителей, в Узбекистане и США включая особенности фильтрации данных и минимизации излишнего доступа к личной информации.

4. **Кейс-анализ**:

- Примеры из практики, подтверждающие актуальность вопроса, такие как случаи, когда отсутствие четкой регламентации привело к нарушениям прав граждан.

5. **Рекомендации по реформированию**:

- Разработаны рекомендации для изменения национального законодательства с учетом международного опыта и специфики цифровых данных.

РЕЗУЛЬТАТЫ

1. Специфика цифровых доказательств

Техническая сложность и необходимость специальных знаний: Для работы с цифровыми доказательствами часто требуются глубокие технические знания и доступ к специализированным инструментам и программному обеспечению. Экспертам в области кибербезопасности и цифровой криминалистики необходимо уметь извлекать, интерпретировать и анализировать данные, сохраняя их целостность. Для этого применяются сертифицированные методы и стандарты (например, стандарты, описанные в руководствах Европола, Интерпола и ENISA), позволяющие установить так называемый «цифровой след» и выстроить непрерывную цепочку хранения доказательств (chain of custody).

Необходимость сохранения целостности и подлинности (аутентичности) данных: Цифровые данные должны быть зафиксированы таким образом, чтобы исключить возможность их несанкционированного изменения после изъятия. Методы фиксации включают криптографические хеши (например, SHA-256), создание дубликатов носителей (bit-by-bit копии) и использование аппаратно-программных комплексов «Write-Blocker» для предотвращения записи. Таким образом, гарантируется, что исследуемые данные являются подлинными и неизмененными, что является ключевым фактором их допустимости в суде.

Глобальный и распределенный характер данных: В отличие от традиционных, локально ограниченных физических улик, цифровые доказательства могут храниться в различных юрисдикциях – на серверах в других странах, в облачных хранилищах или на зашифрованных сетевых ресурсах. Это усложняет процесс правового получения данных, требуя международного сотрудничества, использования механизмов взаимной правовой помощи (MLAT) и соблюдения законов о защите данных в разных государствах.

Противодействие со стороны фигурантов и использование инструментов анонимности: Участники противоправной деятельности могут активно скрывать или усложнять доступ к цифровым доказательствам: использовать шифрование, VPN, анонимные сети (например, Tor), криптовалютные транзакции, а также специальные инструменты для уничтожения или изменения данных. Это требует от следственных органов применения сложных методов цифровой криминалистики, а также постоянного совершенствования навыков и технологий.

Стандарты, методологии и руководство по обращению с цифровыми доказательствами: Международные организации, такие как Совет Европы, Европол, Интерпол и различные кибербезопасные агентства (например, ENISA), разрабатывают руководство и стандарты, определяющие надлежащие практики сбора, анализа, хранения и представления цифровых доказательств. Эти стандарты включают в себя рекомендации по обеспечению юридической значимости материалов, а также по снижению риска их оспаривания в суде.

Примером руководства может служить «Good Practice Guide for Digital Evidence» (Великобритания), а также документы, подготовленные Европейской сетью судебных цифровых криминалистических экспертиз (European Network of Forensic Science Institutes, ENFSI), которые помогают унифицировать подходы к работе с цифровыми материалами, обеспечивая их надежность и применимость в различных юрисдикциях.

Дополняя пример о смартфонах, можно отметить, что современные методы расшифровки и анализа мобильных устройств требуют использования специализированных криминалистических решений (Cellebrite, Magnet AXIOM, XRY), соблюдения принципов неизменности доказательств и документирования каждого шага в процессе извлечения и анализа данных. Это не только технически сложно, но и юридически ответственно, поскольку любое нарушение процедуры может привести к недопустимости доказательств в суде.

Пример: современные смартфоны могут содержать до 70 различных категорий информации, включая личные переписки, данные банковских приложений, электронную почту, сведения о местоположении, медиафайлы, а также историю посещений веб-сайтов. Исследователи отмечают, что с развитием функционала мобильных устройств объем и разнообразие хранимых на них данных постоянно растут. Согласно обзору, проведенному Barmpatsalou и соавторами (2018), данные смартфона могут охватывать геолокационные логи, резервные копии в «облаке», поведенческие паттерны, временные метаданные приложений и другие, менее очевидные источники. Quick и Choo (2014) подчеркивают, что объем доступной информации нередко исчисляется десятками гигабайт, что затрудняет эффективный поиск и выделение релевантных данных, а также повышает риск нарушения конфиденциальности. Кроме того, разнородность операционных систем, применяемых методов шифрования и разнообразие используемых приложений усложняют процесс извлечения данных и их последующего анализа (Baggili et al., 2015).

Таким образом, современные смартфоны представляют собой не только богатый источник потенциально ценных для расследования сведений, но и поднимают ряд дополнительных вопросов, связанных с защитой персональных данных, масштабируемостью и эффективностью инструментов криминалистического анализа, а также с юридической допустимостью полученной информации. Это превращает их в источник огромного количества данных, выходящих за рамки необходимого для расследования, и требует аккуратного, стандартизированного подхода к извлечению, систематизации и оценке цифровых доказательств.

2. Судебные прецеденты

В США судебные органы сыграли ключевую роль в установлении стандартов защиты конфиденциальности при работе с цифровыми доказательствами. Правовые прецеденты, сформированные Верховным судом, существенно повлияли на то, как правоохранительные органы могут получать доступ к данным, хранящимся на цифровых устройствах и в сетях связи.

Дело Riley v. California (2014): Верховный суд США постановил, что обыск содержимого мобильного телефона без ордера нарушает Четвертую поправку. Суд подчеркнул, что современные смартфоны содержат не просто отдельные цифровые фрагменты, а целую «цифровую историю жизни», включая медицинские записи, переписку в мессенджерах, фотографии, электронные билеты, банковские сведения и личные документы. Исследования, опубликованные после вынесения решения, отмечают важность этого прецедента в контексте постоянно растущего объема персональных данных, хранящихся на мобильных устройствах (Henderson, 2015; Kerr, 2014). Таким образом, обыски смартфонов стали приравниваться по степени вторжения в личную жизнь к тщательной ревизии личных бумаг и корреспонденции.

Значение: Это решение подчеркнуло, что использование цифровых технологий требует более строгих процедур защиты конфиденциальности, чем традиционные обыски. Законодатели и правоохранительные органы вынуждены учитывать новые стандарты при разработке инструкций и регламентов для изъятия цифровых данных.

Дело Carpenter v. United States (2018): Верховный суд США признал незаконным сбор данных о местоположении мобильного телефона (Cell-Site Location Information, CSLI) без ордера. Суд отметил, что такая информация способна рисовать детализированный портрет повседневной жизни человека, отражая его маршруты, места пребывания и даже социальные связи (Carpenter v. United States, 2018). Научные публикации указывают, что данное решение активно повлияло на практику сбора и анализа данных о местоположении, поскольку оно ограничивает правоохранительные органы в использовании масштабных баз данных сотовых операторов без судебного надзора (Solove, 2018; Kerr, 2018).

Значение: Суд постановил, что данные о местоположении требуют такой же правовой защиты, как личные бумаги, что является важным шагом в защите конфиденциальности в цифровую эпоху. Это создает юридический прецедент для более тщательного рассмотрения других типов массовых цифровых данных, используемых в расследованиях.

Эти прецеденты формируют основу для будущего регулирования цифровых обысков. В научной литературе отмечается, что правовые органы должны искать баланс между эффективностью расследований и защитой фундаментальных прав на неприкосновенность частной жизни (Slobogin, 2015; Tokson, 2018). Решения по делам Riley и Carpenter подчеркивают, что доступ к цифровым устройствам и службам должен быть строго регламентирован, основываться на принципе наличия ордера и осуществляться под судебным контролем.

3. Проблемы текущего законодательства РУз.

В Республике Узбекистан, законодательство в области цифровых доказательств отстает от современных вызовов. Несмотря на проводимые в последние годы реформы, Уголовно-процессуальный кодекс (УПК) Республики Узбекистан до сих пор не содержит детального регламентирования порядка изъятия, обработки и использования электронных (цифровых) доказательств в уголовном процессе. В результате этого:

Устаревшие нормы УПК Узбекистана в контексте цифровых доказательств:

Действующий УПК, принятый в 90-е годы и неоднократно обновлявшийся, в основном ориентирован на традиционные, физические носители информации. Отсутствует четкое нормативное определение электронных доказательств, а также процессуальные механизмы, учитывающие специфику изъятия и анализа данных, хранящихся на цифровых устройствах. Это приводит к тому, что следственные органы применяют общие правила обыска и выемки, не делая различий между физическими и цифровыми объектами, что может приводить к процессуальным коллизиям и неясностям.

Отсутствие механизмов фильтрации данных:

При изъятии цифровых устройств в Узбекистане отсутствуют чёткие нормы, ограничивающие объем и характер извлекаемой информации. Как отмечают исследователи, это может приводить к тому, что органам следствия доступен весь массив данных, включая личную переписку, фотографии, конфиденциальную

информацию и электронную корреспонденцию, не имеющую отношения к расследуемому делу. Подобная ситуация создает риск нарушения права на неприкосновенность частной жизни, гарантированного Конституцией и Законом «О персональных данных» (ЗРУ-547 от 2 июля 2019 г.), который устанавливает общие правила защиты личной информации, но не содержит конкретных норм о процессуальных гарантиях при изъятии цифровых доказательств.

Низкий уровень судебного контроля:

В практике Узбекистана, по данным некоторых исследователей, суды редко обеспечивают должный контроль за процедурами получения цифровых доказательств, поскольку законодательство не содержит четких норм, позволяющих устанавливать специальные ордера или разрешения для доступа к электронным носителям. Отсутствие специализированных судебных процедур, аналогичных тем, что установлены решениями Верховного суда США (например, Riley v. California и Carpenter v. United States), затрудняет защиту прав подозреваемых и третьих лиц, чьи данные могут быть случайно изъяты или проанализированы.

Пример из практики: Если следователь в Узбекистане изымает смартфон подозреваемого, то, при отсутствии норм о фильтрации и ограничении объема изымаемых данных, возможно получение доступа к личной переписке, в том числе с адвокатом или врачом. Таким образом, незащищённость цифровых данных ставит под угрозу сохранение профессиональных тайн и конфиденциальности информации. Подобные ситуации являются индикатором необходимости модернизации УПК и разработки подзаконных актов, устанавливающих чёткий протокол работы с цифровыми доказательствами.

4. Риски утечек и злоупотреблений

При изъятии цифровых устройств возникает реальная опасность утечки данных, поскольку следователи нередко получают доступ к значительному объему информации, не связанной с расследуемым делом. Современная судебно-следственная практика зачастую позволяет получать полный образ накопителя или памяти устройства, включая личную корреспонденцию, фотографии, медицинские записи, финансовую информацию, а также данные о третьих лицах. Исследователи указывают, что подобное «неконтролируемое» изъятие данных создает вероятность злоупотреблений, таких как использование конфиденциальных сведений для политического или экономического давления, шантажа или передачи данных третьим сторонам (Kerr, 2020).

Кроме того, отсутствие четких механизмов фильтрации данных, часто упоминаемых как «неотносимые» или «нерелевантные» к делу, увеличивает риск нарушения прав человека на неприкосновенность частной жизни. Эксперты в области цифровых доказательств подчеркивают, что правоохранительные органы должны не только документировать и обосновывать необходимость доступа к определенным категориям данных, но и использовать методы избирательного извлечения и скрининга, чтобы минимизировать потенциальный ущерб для граждан (Wexler, 2020). В противном случае возникает ситуация, при которой может произойти случайная или намеренная утечка информации, не имеющей отношения к расследованию, но способной нанести вред репутации или правам людей.

Таким образом, необходимость тщательно продуманных правовых механизмов, регламентов и внутренних протоколов становится все более очевидной. Они должны предусматривать как меры по предотвращению нецелевого сбора и использования данных, так и механизмы судебного контроля и ответственности за нарушения. Международный опыт и экспертные рекомендации подчеркивают важность внедрения принципов «минимизации данных» (data minimization) и «ограничения по целевому назначению» (purpose limitation) в практику правоохранительных органов, работающих с цифровыми доказательствами.

ОБСУЖДЕНИЕ

1. Необходимость принципа минимизации

В Республике Узбекистан, как и в ряде других постсоветских государств, правовое регулирование порядка получения и использования цифровых доказательств находится на стадии формирования. Хотя действующий Уголовно-процессуальный кодекс (УПК) Республики Узбекистан и претерпел ряд изменений, он все еще не содержит детальных норм, регламентирующих применение принципа минимизации при работе с цифровыми доказательствами. Это означает, что четкие рамки, позволяющие ограничить объем изымаемых данных только теми, что непосредственно относятся к расследуемому делу, фактически отсутствуют.

В Узбекистане, по данным исследователей, до сих пор не выработаны процессуальные механизмы, обеспечивающие целевой доступ к конкретным категориям данных, например, к определенной переписке за конкретный период или к определенным типам файлов. Такая ситуация создает риск «перегрузки информацией» и повышает вероятность получения следственными органами доступа к избыточной, нерелевантной или конфиденциальной информации, не связанной с предметом расследования.

Принцип минимизации, предполагающий четкое определение границ доступа к данным, их категории и временные рамки, мог бы быть закреплен в национальном законодательстве путём внесения изменений в УПК и принятия подзаконных актов. Такие меры могли бы основываться на международном опыте и рекомендациях правозащитных организаций, где подчеркивается важность защиты личных данных, а также баланса между эффективностью расследования и неприкосновенностью частной жизни.

Проблема в контексте Узбекистана:

В Узбекистане отсутствуют четкие правила, регулирующие объем и характер изымаемой с цифровых устройств информации. Фактически следственные органы имеют широкие полномочия, позволяющие изымать полные образы жестких дисков, содержимое смартфонов или аккаунтов в социальных сетях без механизма точечного ограничения доступа. Это может привести к сбору нерелевантных данных, которые, помимо нарушения приватности, потенциально создают иные угрозы – от утечки конфиденциальной информации до нарушения адвокатской или врачебной тайны.

Пример:

Если в ходе обыска смартфона подозреваемого следователь получает доступ к банковским приложениям и истории финансовых транзакций, не связанных с рассматриваемым делом, такой необоснованно широкий доступ к цифровым данным создает риск утечки не относящейся к делу финансовой информации.

Это не только подрывает права граждан на конфиденциальность, но и демонстрирует необходимость законодательно закрепленных принципов минимизации, которые позволяли бы ограничивать объем и характер изымаемых данных чёткими процессуальными рамками.

2. Двухступенчатый процесс обыска

Современные обыски цифровых устройств должны включать два ключевых этапа:

1. **Физическое изъятие устройства:** На этом этапе устройство изымается, тщательно упаковывается и опечатывается с целью предотвращения несанкционированного доступа или изменения данных. Правильная фиксация состояния устройства, включая использование сертифицированных методов сохранения целостности (например, write-blockers или точных битовых копий), считается критически важной для последующей допустимости доказательств в суде (Casey & Turnbull, 2014).

2. **Детализированный анализ данных:** Доступ к содержимому устройства должен предоставляться только после получения дополнительного судебного разрешения (warrant), которое ограничивает объем данных, подлежащих анализу, и определяет релевантные временные рамки, типы файлов или категорий контента (Kerr, 2015). Такой подход отражает применение «принципа минимизации» и «целенаправленных запросов», уже обсуждаемое в современной правовой доктрине, чтобы избежать масштабной и неселективной проверки всей информации на устройстве (Wexler, 2020).

Сравнение с США:

В США практика двухэтапного обыска уже активно применяется, в том числе благодаря прецедентам, сформированным судебными решениями Верховного суда. В деле *Riley v. California (2014)* Верховный суд подчеркнул, что смартфоны содержат «цифровую историю жизни» владельца, включающую личную переписку, фотографии, медицинские записи и финансовые документы, и что доступ к этим данным без отдельного ордера нарушает Четвертую поправку. После *Riley* правоохранительные органы всё чаще вынуждены использовать так называемые «два ордера»: один для изъятия устройства, другой – для последующей выборочной проверки его содержимого в соответствии с узко очерченными критериями (Kerr, 2020).

Исследователи отмечают, что такая двухуровневая модель снижает риск неоправданного вмешательства в частную жизнь: при втором этапе рассмотрение «фильтрационных команд» или «специалистов» может помочь отделить релевантные материалы от нерелевантных, тем самым не предоставляя следствию доступ ко всему массиву данных (Ferguson, 2018).

Ситуация в Узбекистане:

В отличие от США, в Узбекистана законодательство и правоприменительная практика пока не предусматривают четко выраженный двухступенчатый подход к обыску цифровых устройств. Отсутствие подобных процедур повышает риск нарушения конфиденциальности. Следственные органы могут получить полный доступ к устройству без необходимости получения отдельного судебного решения на анализ конкретных категорий данных, что ведет к чрезмерному сбору информации и вторжению в личную жизнь (Popova, 2018; Balashova, 2019).

3. Судебный контроль и фильтрация данных

Одной из наиболее эффективных мер защиты прав граждан при обыске цифровых устройств является усиление судебного контроля за процессом. Исследователи в области права и цифровой криминалистики отмечают, что это может быть достигнуто за счет более строгих процедур получения ордеров и внедрения технологических решений, ограничивающих доступ к нерелевантным данным (Kerr, 2015; Wexler, 2020).

Конкретные меры включают:

- **Обязательное получение ордера перед анализом данных:** Судебные органы должны выдавать отдельные ордера, четко определяющие категории информации, к которым может быть осуществлен доступ. Это гарантирует, что следователи не смогут просматривать весь объем данных на устройстве, а лишь ту их часть, которая непосредственно связана с расследованием.
- **Применение специальных программных средств фильтрации:** Современные программные инструменты способны автоматически исключать нерелевантные данные из анализа. Например, если ордер распространяется только на электронные письма, связанные с конкретной датой или словосочетанием, программное обеспечение может отсеивать личные фотографии, финансовые документы или переписку с адвокатом, не имеющие отношения к делу. Такие «технологии минимизации» позволяют значительно снизить риск вторжения в личную жизнь и сократить объем случайно изъятой информации (Kerr, 2015).

Пример:

Если следователи получили ордер на доступ к электронной переписке подозреваемого в период с 1 по 10 апреля, программное обеспечение фильтрации будет извлекать только письма за этот период. Личные фотографии, хранившиеся на устройстве, или переписка с адвокатом за другие даты будут автоматически исключены из поля зрения следствия, сохраняя неприкосновенность частной жизни и конфиденциальность.

4. Риски злоупотреблений и утечек данных

Изъятие цифровых устройств сопряжено с рисками, связанными с утечками данных и злоупотреблениями. В отсутствие четкой регламентации собранная информация может выйти за рамки расследуемого дела, оказаться в руках третьих лиц или использоваться для оказания давления на подозреваемых. Исследователи в области цифровой криминалистики и права отмечают, что отсутствие детальных процессуальных норм и «использовательских ограничений» (use restrictions) повышает вероятность неправильного или нецелевого использования собранных данных (Kerr, 2015).

Пример: Если при изъятии устройства предпринимателя следственные органы получают доступ к информации, составляющей коммерческую тайну (финансовые отчеты, данные о клиентах, бизнес-стратегии), то при отсутствии четких правовых механизмов контроля эта информация может быть передана недобросовестным конкурентам или использована для шантажа. Подобные сценарии подчеркивают необходимость усиления правовых гарантий и технических мер, направленных на предотвращение злоупотреблений.

Рекомендации:

- **Внедрение ответственности за утечку данных**: Законодательство должно содержать четко прописанные санкции за несанкционированный доступ, копирование или распространение информации, изъятой с цифровых устройств. Ответственность должна распространяться как на должностных лиц правоохранительных органов, так и на третьих лиц, получивших информацию незаконным путем.
- **Установление строгих процедур хранения и доступа к изъятым цифровым устройствам**: Исследования подчеркивают важность внедрения «принципа минимизации» и ограничений по использованию данных, не относящихся к делу (Kerr, 2015; Wexler, 2020). Например, можно применять программные средства, которые дают следователям доступ лишь к определенным категориям файлов или временным периодам, указанным в ордере. Такие меры снижают риск несанкционированного ознакомления с конфиденциальной информацией и предотвращают ее утечку.

Таким образом, чёткое законодательное регулирование и внедрение технологических решений, обеспечивающих целевое и ограниченное использование данных, являются ключом к защите прав граждан и поддержанию доверия к правовым институтам.

ЗАКЛЮЧЕНИЕ

В условиях стремительного развития цифровых технологий уголовно-процессуальное законодательство все чаще сталкивается с необходимостью учитывать специфику электронных доказательств. Цифровые носители потенциально предоставляют широкий спектр ценных данных для расследования, однако при их изъятии и анализе возникает риск массового и неконтролируемого сбора личной информации, не относящейся к делу. Отсутствие четких законодательных норм и судебных стандартов в данной сфере создает возможности для злоупотреблений, утечек данных, нарушения адвокатской и коммерческой тайны, а также ущемления конституционных прав граждан.

Международный опыт, в частности практика США по делам Riley v. California и Carpenter v. United States, продемонстрировал важность принципа минимизации данных и укрепления судебного контроля за обысками цифровых устройств. Применение двухступенчатого подхода – изъятие устройства с последующим анализом данных исключительно в рамках строго определенного судебным ордером круга информации – способно существенно снизить риски превышения полномочий. Кроме того, внедрение программных фильтров, ограничивающих доступ к нерелевантным данным, позволит эффективно защищать личную жизнь и конфиденциальность.

Для реформирования национального законодательства и правоприменительной практики целесообразно:

1. Закрепить принцип минимизации данных, предусматривающий четкое указание категорий информации в ордерах на обыск.
2. Усилить судебный контроль, обеспечив невозможность анализа цифровой информации без специального разрешения суда.
3. Применять программные средства фильтрации, автоматически исключающие из исследования нерелевантные для дела данные.

4. Установить ответственность за несанкционированное использование или передачу информации, изъятой с цифровых устройств, чтобы предотвратить злоупотребления и утечки.

Реализация данных рекомендаций создаст необходимую нормативную базу, учитывающую современные вызовы цифровой эпохи. Это позволит найти баланс между эффективностью расследований и защитой прав граждан, укрепит доверие к работе правоохранительных органов, а также повысит качество правосудия в целом. Внедряя международный опыт и совершенствуя правовое регулирование в сфере цифровых доказательств, национальное законодательство сможет повысить стандарты защиты конфиденциальности, обеспечить справедливость судебных процедур и укрепить принципы правового государства в условиях стремительной цифровизации общества.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. Association of Chief Police Officers (ACPO). (2012). *ACPO Good Practice Guide for Digital Evidence.*

2. Association of Chief Police Officers (ACPO). (2012). *ACPO Good Practice Guide for Digital Evidence.* (Дополненное издание).

3. Carpenter v. United States, 138 S. Ct. 2206 (2018).

4. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd ed.). Academic Press.

5. Casey, E., & Turnbull, B. (2014). Digital Evidence on Mobile Devices. *Forensic Science International*, 236, 29-36. https://doi.org/10.1016/j.forsciint.2013.12.006

6. Cellebrite. (n.d.). *Digital Intelligence Solutions.* https://www.cellebrite.com/

7. Council of Europe. (2001). *Convention on Cybercrime (CETS No.185).* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

8. ENFSI (European Network of Forensic Science Institutes). (2015). *Guidelines for Best Practice in the Forensic Examination of Digital Technology.*

9. European Union Agency for Cybersecurity (ENISA). (2013). *Cyber Forensics – A Field Manual for Collecting, Handling and Analyzing Information and Evidence Related to Cybercrime.* ENISA.

10. European Union Agency for Cybersecurity (ENISA). (2015). *Tools and Methodologies to Support Cooperation with CERTs for Law Enforcement.* ENISA.

11. Europol. (2020). *First Responders Guide to Handling Electronic Evidence.* https://www.europol.europa.eu

12. Europol. (2020). *Internet Organised Crime Threat Assessment (IOCTA).* https://www.europol.europa.eu

13. Ferguson, A. G. (2018). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement.* NYU Press. Available at SSRN: https://ssrn.com

14. Henderson, S. E. (2015). *Riley v. California: Carding a Path Out of the Cellar.* SSRN-id2586464. Retrieved from https://ssrn.com/abstract=2586464

15. Kerr, O. S. (2014). *Foreword: Accounting for Technological Change.* Harvard Law Review, 36 Harv. J.L. & Pub. Pol'y 403. Also available at SSRN: SSRN-id2628586. Retrieved from https://ssrn.com/abstract=2628586

16. Kerr, O. S. (2018). *Carpenter v. United States and the Fourth Amendment: A Preliminary Analysis.* Harvard Law Review Blog. Retrieved from https://blog.harvardlawreview.org/carpenter-v-united-states-and-the-fourth-amendment-a-preliminary-analysis/

17. Kerr, O. S. (2020). Decryption Originalism: The Lessons of Burr. *Harvard Law Review*, 134, 905-970. Available at SSRN: https://ssrn.com

18. Kerr, O. S. (2020). Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data. *Texas Tech Law Review.* Available at SSRN: https://ssrn.com/abstract=3561285

19. Kshetri, N. (2019). *Cybercrime and Cybersecurity in the Global South.* Palgrave Macmillan.

20. Magnet Forensics. (n.d.). *Magnet AXIOM.* https://www.magnetforensics.com

21. National Institute of Standards and Technology (NIST). (2006). *Guide to Integrating Forensic Techniques into Incident Response (SP 800-86).* U.S. Department of Commerce.

22. National Institute of Standards and Technology (NIST). (2014). *Guidelines on Validating Forensic Tools and Methods (NISTIR 8006).* U.S. Department of Commerce.

23. Popova, I. A. (2018). Improving the Use of Electronic Evidence in the Criminal Process: Legal Regulation and Practice. *Izvestiya of Saratov University. New Series. Series: Economics. Management. Law*, 18(2), 239–243. Available at SSRN: https://ssrn.com

24. Riley v. California, 134 S. Ct. 2473 (2014).

25. Slobogin, C. (2015). *Policing as Administration.* William & Mary Law Review, 165(3), 865–886. Retrieved from https://scholarship.law.wm.edu/wmlr/vol165/iss3/5/

26. Solove, D. J. (2018). *Carpenter v. United States and the Mosaic Theory.* GWU Law School Public Law Research Paper No. 2018-60. Retrieved from https://ssrn.com/abstract=3245527

27. Sommer, P., & Taylor, M. (2016). *Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness.* British Standards Institution.

28. Tokson, M. (2018). *Carpenter and the Mosaic Theory.* Yale Journal of Law & Technology, 20(2), 540–560. Retrieved from https://digitalcommons.law.yale.edu/yjolt/vol20/iss2/4

29. Tor Project. (n.d.). *About.* https://www.torproject.org/about/

30. U.S. Department of Justice. (n.d.). *Mutual Legal Assistance Treaties.* https://www.justice.gov/criminal-mlats/

31. Wexler, R. (2020). Privacy as Privilege: Law Enforcement's Breakable Shield. *University of Pennsylvania Law Review.* Available at SSRN: https://ssrn.com/abstract=3674899

32. Балашова, А. А. (2020). Электронные носители информации и их использование в уголовно-процессуальном доказывании. Москва: Академия управления МВД РФ.

33. Закон Республики Узбекистан «О персональных данных» (ЗРУ-547 от 2 июля 2019 г.). Доступно на: https://lex.uz

34. Уголовно-процессуальный кодекс Республики Узбекистан. Доступно на: https://lex.uz