Югай Людмила Юрьевна
Ўзбекистон Республикаси ИИВ Академияси Олий ўқув юртидан кейинги таълим факультети докторанти, юридик фанлари бўйича фалсафа доктори (PhD)
Гаджиев Хагани Мохуббат ўғли
Ўзбекистон Республикаси Ички ишлар вазирлиги Эксперт-криминалистика Бош маркази бош эксперти

РАҚАМЛИ ТЕХНОЛОГИЯЛАР СОҲАСИДАГИ ЖИНОЯТЛАР БЎЙИЧА КОМПЬЮТЕР-ТЕХНИКА ЭКСПЕРТИЗА УСЛУБИЁТИ

Югай Людмила Юрьевна
Доктор философии (PhD) по юридическим наукам, докторант Факультета послевузовкого образования Академии МВД Республики Узбекистан
Гаджиев Хагани Мохуббат оглы
Главный эксперт Главного эксперно-криминалистического центра МВД Республики Узбекистан

МЕТОДИКА КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ ПО ПРЕСТУПЛЕНИЯМ В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Yugai Ludmila
Doctor of Philosophy (PhD) in Law, The Academy of the MIA of the Republic of Uzbekistan,
Gadjiev Hagani
Head Expert at Main Forensic Center of the Ministry of Internal Affairs of the Republic of Uzbekistan xagani89@gmail.com

METHODS OF COMPUTER-TECHNICAL EXPERTISE ON CRIMES IN THE FIELD OF DIGITAL TECHNOLOGIES

Аннотация. *Мақолада компьютер-техника экспертизасининг концепцияси ва моҳияти, ахборот технологиялари соҳасидаги жиноятлар учун рақамли далилларни қидириш, тадқиқот қилиш методикаси асосида компьютер маълумотларини олиш ва унинг ташувчиларини ўрганиш хусусиятлари очиб берилган. Мақолада компьютер-техника экспертизасини ўтказиш усуллари бўйича хорижий ва миллий амалиётнинг қиёсий таҳлили ёритилган. Илмий ишда эксперт тадқиқот усулларини танлаганида қонунчилик томонидан илгари сурилган талабларнинг асосий рўйхати келтирилган. Муаллифлар ушбу турдаги суд экспертизасини такомиллаштириш бўйича таклиф ва тавсиялар ишлаб чиқдилар.*

Калит сўзлар: *компьютер-техника экспертизаси, эксперт методологияси, экспертиза объектлари, ахборот ташувчилар, ахборот таҳлили.*

Annotation. *The article reveals the concept and essence of computer-technical expertise, the features of obtaining computer information and studying its carriers based on the methodology of searching, securing and researching digital evidence for crimes in the field of information technology. A comparative analysis of foreign and national practice in the field of methods of production of computer-technical expertise is carried out. The paper provides a fundamental list of requirements put forward by the court proceedings when an expert chooses methods of examination. The authors have formulated proposals and recommendations for improving this type of forensic examination.*

Keywords: *computer-technical expertise, expert methodology, admissibility, objects of expertise, information carriers, information analysis.*

Аннотация. *Статья раскрывает понятие и сущность компьютерно-технической экспертизы, особенности получения компьютерной информации и изучения ее носителей на основе методики поиска, закрепления и исследования цифровых доказательств по преступлениям в сфере информационных технологий. Проводится сопоставительный анализ зарубежной и национальной практики в области методики производства компьютерно-технической экспертизы. В работе приводится основополагающий перечень требований, выдвигаемый судопроизводством при выборе экспертом методов производства экспертизы. Авторами сформулированы предложения и рекомендации по совершенствованию данного вида судебной экспертизы.*

Ключевые слова: *компьютерно-техническая экспертиза, экспертная методика, допустимость, объекты экспертизы, носители информации, анализ информации.*

На современном этапе в Республике Узбекистан также, как и во всем мире особую актуальность приобретает вопрос цифровой трансформации преступности. Проблема заключается в том, что злоумышленники используют информационные технологии как орудие совершения и сокрытия преступления в своих преступных целях. Преступления в сфере информационных технологий вышли за пределы национальных границ и стали особым видом транснациональной преступности, требующим адекватного ответа со стороны правоохранительных органов. Преступления в сфере информационных технологий имеют высокую степень латентности (скрытности) – большая часть преступлений остается даже не зарегистрированной.

Анализ правоприменительной практики показывает, что из всех зарегистрированных за 2021 год преступлений с использованием средств компьютерной техники в Республике Узбекистан хищение путем присвоения или растраты (ст.167 УК) составляет ***7%,*** мошенничество (ст.168 УК) – ***68%,*** кража (ст.169 УК) – ***24,5%,*** незаконный (несанкционированный) доступ к компьютерной информации (ст.278^2 УК) – **1%,** изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе, а также к сетям телекоммуникаций (ст.278^3 УК) – **1%,** модификация компьютерной информации (ст.278^4 УК) – **1%,** создание, использование или распространение вредоносных программ (ст.278^6 УК) – **1%**, незаконный (несанкционированный) доступ к сети телекоммуникаций (ст.278^7 УК) – **3%**.

Изучение мнений ученых-криминалистов и экспертной практики, свидетельствует о том, что в настоящее время наблюдается виртуализация преступности, т.е. переход общественно опасных деяний в информационную среду, исключающую физический контакт преступника и жертвы, обеспечивающую «традиционную», классическую преступность *современными информационными технологиями* в виде систем конспирации и скрытой связи. Преступления такого рода будут оставлять значительно больше цифровых следов и требовать от преступника технической компетентности, что, несомненно, повлияет и на механизм следообразования [1].

В связи с этим особое значение приобретает компьютерно-техническая экспертиза. Компьютерно-техническая экспертиза (далее по тексту – КТЭ) – это самостоятельный род судебных экспертиз, относящийся к классу инженерно-технических экспертиз, проводимый в целях: определения статуса объекта как компьютерного средства, выявления и изучения его роли в расследуемом преступлении, а также получения доступа к информации на электронных носителях с последующим всесторонним ее исследованием [2].

Основная цель КТЭ – поддержать или опровергнуть гипотезу в уголовном или гражданском суде [3].

Задачами исследования являются поиск, обнаружение, анализ и оценка информации, с целью завершить целостное построение доказательственной базы путем окончательного разрешения большинства диагностических и идентификационных вопросов, связанных с компьютерной информацией.

Анализ экспертной практики свидетельствует о том, что с момента открытия в 2018 году отдела и лаборатории цифровой экспертизы в Главном экспертно-криминалистическом центре МВД Республики Узбекистан, количество поступивших на исследование объектов в 2019 г. по сравнению с 2018 г. наблюдается рост на 70%. А в 2020 г. по сравнением с 2019 г. 90%. При этом в 2021 г. положительная динамика сохраняется на 150% больше по сравнению с 2020 г.

Вышеуказанные показатели свидетельствуют о растущей актуальности на сегодняшний день данного вида судебных экспертиз.

В связи с тем, что программно-технические характеристики объектов КТЭ находятся в постоянном развитии и совершенствовании, необходимо постоянное обновление судебно-экспертной методики проведения данного вида исследования. Одно из главных отличий компьютерно-технической экспертизы от многих видов традиционной экспертизы (к примеру, дактилоскопической) является тот факт, что для дачи полного, достоверного, научно обоснованного заключения возможно использование методического обеспечения (экспертных методик) двадцатилетней давности, что абсолютно категорически **неприменимо** для компьютерно-технической экспертизы.

Под экспертной методикой принято понимать совокупность методов, используемых при производстве экспертизы.

Так, методы, используемые экспертами при производстве экспертизы, должны удовлетворять перечню требований, выдвигаемому национальным судопроизводством: законности; обоснованности; достоверности получаемых результатов; безопасности; эффективности; экономичности; этичности и допустимости. Наиболее важным параметром при выборе метода исследования является – допустимость. Определяющим фактором при оценке того или иного метода на допустимость является научная обоснованность и удовлетворение метода новейшим достижениям области современных научных технологий [4].

Но также стоит отметить, что при выборе методики исследования каждая страна следует своим собственным стандартам, протоколам и процедурам в области цифровой криминалистики.

К примеру 2006 году Национальный институт стандартов и технологий США в своем Руководстве по интеграции криминалистических методов в планы реагирования на инциденты (Guide to Integrating Forensic Techniques into Incident Response)(SP 800-86) (Kent et al., 2006, 3-1) предложил модель цифровой криминалистики, состоящую из четырех этапов [5]:

И так рассмотрим более подробнее криминалистический процесс, который проводят специалисты и эксперты [6], в четыре этапа:

На первом этапе происходит сбор как информации самой по себе, так и носителей компьютерной информации. Сбор должен сопровождаться атрибутированием (пометкой), указанием источников и происхождения данных и объектов. В процессе сбора должны обеспечиваться сохранность и целостность (неизменность) информации, а в некоторых случаях также ее конфиденциальность. При сборе иногда приходится предпринимать специальные меры для фиксации недолговечной (волатильной) информации, например, текущих сетевых соединений или содержимого оперативной памяти компьютера.

На втором этапе производится экспертное исследование собранной информации (объектов-носителей). Оно включает извлечение/считывание информации с носителей, декодирование и вычленение из нее той, которая относится к делу. Некоторые исследования могут быть автоматизированы в той или иной степени. Но работать головой и руками на этом этапе эксперту все равно приходится. При этом также должна обеспечиваться целостность информации с исследуемых носителей.

На третьем этапе избранная информация анализируется для получения ответов на вопросы, поставленные перед экспертом или специалистом. При анализе должны использоваться только научные методы, достоверность которых подтверждена.

Четвертый этап включает оформление результатов исследования и анализа в установленной законом и понятной неспециалистам форме.

Также необходимо отметить, что в ряде зарубежных стран (США, Франция, Республика Корея, Япония и др.) – компьютерно-криминалистическая экспертиза не существует в качестве отдельного процессуального действия, имеющего определенные временные границы назначения, проведения и дачи заключения. Вместо назначения данного вида экспертизы, которое занимает определенные законом процессуальные сроки, инициатор исследования (следователь, оперативный работник), как правило, обладающий специальными познаниями в области информационно-коммуникационных технологий и цифровой криминалистики, самостоятельно проводит исследование объектов и составляет **Report** (отчет). Данный документ отражает основные результаты, полученные в ходе исследования, и используется в суде качестве доказательства по делу.

В Республике Узбекистан также, как и в странах СНГ, главной процессуальной формой применения специальных знаний и умений в области новейших компьютерных технологий в процессе расследования является судебная экспертиза. Вызов эксперта, назначение и производство судебной экспертизы осуществляется в порядке, установленном ст. 67, 68, 172, 173, 174, 175, 176, 177, 178-180, 184 УПК Республики Узбекистан [7].

Основанием для производства КТЭ является постановление дознавателя, следователя, прокурора или определение суда. После чего в соответствии законом Республики Узбекистан «О судебной экспертизе» эксперт должен предоставить инициатору исследования научно обоснованное заключение с подробным ответом на поставленный вопрос.

Следует отметить, что благодаря применению научно обоснованной экспертной методики при исследовании цифровых носителей информации специалистами ГЭКЦ МВД Республики Узбекистан для следственных подразделений органов внутренних дел, Службы государственной безопасности и прокуратуры оказывается содействие в расследовании множества преступлений, совершенных с применением средств информационно-коммуникационных технологий.

Постановление Президента Республики Узбекистан №ПП-122 «О мерах по дальнейшему совершенствованию экспертно-криминалистической деятельности органов внутренних дел с широким внедрением достижений современной науки» от 08 февраля 2022 года предусматривает внедрение новых видов исследований в области экспертизы цифровых баз данных, экспертизы облачных сервисов в сети Интернет, фоноскопической экспертизы, что в свою очередь позволит расширить масштаб судебно-экспертной деятельности в борьбе с преступлениями в сфере информационных технологий.

Современные возможности аппаратно-программных комплексов и программных обеспечений в области цифровой криминалистики позволяют сократить время для производства КТЭ за счет быстрого и эффективного восстановления утраченных данных на цифровых носителях информации, использования мощных инструментов поиска и анализа информации.

Таким образом, возможности использования результатов КТЭ при предварительном следствии можно представить в следующих направлениях:

– для уточнения информации об использовании компьютерной техники (ноутбука, компьютера), мобильного телефона для хранения и распространения файлов, содержащих идеи религиозного экстремизма, сепаратизма и фундаментализма, детской порнографии, наркотических средств и психотропных веществ;

– для подтверждения факта взаимодействия преступника и потерпевшего посредством приложений обмена сообщениями в сети Интернет;

– для извлечения и восстановления истории посещения сайтов в сети Интернет.

При этом, имея положительный опыт применения научно обоснованной экспертной методики экспертной практике имеется ряд проблем в организации производства КТЭ судебно-экспертными учреждениями.

Инфраструктура цифровой криминалистики находится в настоящее время в Республике Узбекистан на стадии своего становления. Сегодня в практике судопроизводства по делам, сопряженным с использованием компьютерных средств, принимают участие судебные эксперты ГЭКЦ МВД и СГБ Республики Узбекистан, которые осуществляют свою деятельность в центральных аппаратах министерства (ведомства).

По данным ГЭКЦ МВД Республики Узбекистан в 2021 году наибольшее количество назначенных постановлений о проведении компьютерно-технической экспертизы по возбужденным уголовным делам приходится на преступления в составе статей ч. 3 ст. 169, ч. 2 ст. 141^2, ст. 165, ч. 2 ст. 182, ст. 210, ч. 3 ст. 244^1 УК Республики Узбекистан.

Необходимо отметить, что прогрессирующая динамика роста применения информационных технологий в указанных видах преступлений вызвала увеличение запросов следственных и оперативных аппаратов в ГЭКЦ МВД Республики Узбекистан, на производство компьютерно-технической экспертизы.

Кроме того, на первоначальном этапе рост количества преступлений с использованием цифровых технологий обусловил комплекс проблем, вызванных недостаточным ресурсным обеспечением (финансовым, кадровым, материально – техническим, методическим) КТЭ. Возможности судебно-экспертных учреждений не позволяли в полном объеме удовлетворять потребности правоохранительных органов и судов Республики Узбекистан в проведении компьютерно-технических экспертиз.

При этом, на сегодняшний день уголовно-процессуальная правоприменительная практика в Республике Узбекистан, связанная с цифровой/электронной информацией, содержащейся на электронных носителях, «адаптирована» в рамках традиционных видов доказательств, электронная/цифровая информация не выделена как самостоятельный источник доказательства, электронные/цифровые носители информации не имеют статуса как объекта исследования эксперта. Такой подход нуждается в критической оценке, поскольку не учитывает природу процессуальную особенность появления и закрепления в материалах уголовного дела электронных/цифровых доказательств.

С учетом изложенного, исходя из анализа национальной и зарубежной судебно-экспертной практики по формированию доказательственной базы в настоящее время представляется целесообразным предложить следующую систему качества производства компьютерно-технической экспертизы:

1. Создать на уровне региональных экспертно-криминалистических подразделений в структуре УВД областей, МВД Республики Каракалпакстан, отделов и лабораторий цифровой экспертизы, оснащенных современным экспертно-криминалистическим оборудованием и техническими средствами в области цифровой криминалистики;

2. Обеспечить обучение сотрудников экспертно-криминалистических подразделений по современным видам криминалистической экспертизы в ведущих зарубежных смежных ведомствах, центрах и высших образовательных учреждениях;

3. Для нужд уголовно-процессуального регулирования необходимо на законодательном уровне внедрить и использовать следующие понятия: «цифровое/электронное доказательство», «электронный документ», «цифровой носитель информации», а также закрепление в УПК порядка процессуального документирования цифровой (электронной) информации, имеющей доказательственное значение.

В заключении хотелось бы отметить, что производство компьютерно-технических экспертиз по киберпреступлениям осложняется тем, что с постоянным развитием информационных технологий количество цифровых устройств, накапливающих, хранящих и передающих данные, растут в геометрической прогрессии, что ведет к увеличению числа уголовных дел, связанных с использованием средств компьютерной техники как орудия совершения и сокрытия преступления. Открываются новые направления данного вида исследований, позволяющих восстанавливать следовую картину расследуемых преступлений путем экспертного исследования объектов КТЭ. Экспертам в области цифровой криминалистики для дачи полноценного и научно обоснованного ответа на вопросы следственных органов и суда необходимо постоянное повышение квалификации, совершенствование навыков, обновление имеющихся знаний и использование соответствующей настоящему времени методической литературы.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. Грибунов О.П. (2019) Криминалистическая теория причинности в контексте установления механизма следообразования: философские и теоретические аспекты. Вестник Томского государственного университета. 446. 207–211.

2. Усов А.И. (2002) Концептуальные основы судебной компьютерно-технической экспертизы: дис... д-ра юрид. наук (DSc), – С. 402.

3. Компьютерно-техническая экспертиза. Режим доступа: https://ru.wikipedia.org/wiki Википедия (wikipedia.org).

4. Усов А.И. (2003) Судебно-экспертное исследование компьютерных средств и систем. Основы методического обеспечения, – С. 368.

5. Kent K., Chevalier S., Grance T., Dang H. (2006) Guide to Integrating Forensic Techniques into Incident Response. Recommendations of the National Institute of Standards and Technology (NIST), Publ. 800–86.

6. Федотов Н.Н. (2007) Форензика – компьютерная криминалистика. С. 34.

7. Уголовно-процессуальный кодекс Республики Узбекистан Режим доступа: https://lex.uz/docs/111463/.

8. Расулев А.К. «Компьютерные преступления: уголовно-правовые и криминологические аспекты». (2006).

9. Расулев, Абдулазиз Каримович. «Криминологическая характеристика преступлений в сфере информационных (компьютерных) преступлений». Вопросы современной юриспруденции 2 (53) (2016).

10. Rasulev A.K. «Improvement of criminal-legal and criminological measures of fight against crimes in the sphere of information technologies and safety: Doctoral (DSc) dissertation abstract on legal sciences». (2018).