"JOURNAL OF SCIENCE-INNOVATIVE RESEARCH IN UZBEKISTAN" JURNALI
VOLUME 04, ISSUE 04, 2026. APRIL
ResearchBib Impact Factor: 9.654/2024 ISSN 2992-8869

ТРЕБОВАНИЯ К СПЕЦИАЛИСТУ ПО РАССЛЕДОВАНИЮ КИБЕРПРЕСТУПЛЕНИЙ

Б. Х. Хамидов
Старший преподаватель кафедры криминалистики и судебной экспертизы, Ташкентский государственный юридический университет, PhD
Е.С.Крюкова
доцент кафедры криминалистики Юридического факультета Московского государственного университета им. М.В. Ломоносова, кандидат юридических наук.

Аннотация. *Стремительное развитие цифровых технологий не только открыло новые возможности для развития общества, но и повысило риск совершения киберпреступлений. Их расследование требует высокого уровня технической и правовой подготовки. В данной статье анализируются требования, предъявляемые к специалистам, участвующим в расследовании киберпреступлений, с акцентом на национальное законодательство, международные стандарты (ISO/IEC 27037:2012) и сравнительную практику. Обосновывается, что только компетентные и прошедшие переподготовку специалисты в области цифровой криминалистики способны обеспечить эффективное проведение следственных действий и надлежащее обращение с доказательствами.*

Ключевые слова: *киберпреступность, расследование, цифровая криминалистика, специалист, доказательства, ISO/IEC 27037:2012*

Введение

Цифровизация общественной жизни в Узбекистане значительно ускорилась благодаря государственным реформам в сфере информационно-коммуникационных технологий. Хотя данная трансформация повышает эффективность, она также способствует росту киберпреступности — сложных правонарушений, совершаемых с использованием интернета, компьютеров и цифровых устройств. Их выявление, расследование и предупреждение требуют междисциплинарных знаний и специализированной подготовки. В

связи с этим роль специалиста в следственных действиях приобретает особо важное значение.

Развитие цифровых технологий, в свою очередь, приводит к расширению и усложнению отношений в цифровой среде. Сегодня в результате проводимых в стране реформ в данной сфере цифровизируются все области общественной жизни, и эти процессы одновременно порождают различные проблемы в сфере правоохранительной деятельности. В частности, совершенствование законодательства и правоприменительной практики в области расследования киберпреступлений становится все более актуальным.

Следует отметить, что в последние годы в целях регулирования практики расследования киберпреступлений государством принят ряд нормативно-правовых актов, в частности:

Постановление Президента Республики Узбекистан от 22 августа 2022 года № ПҚ–357 «О мерах по выводу сферы информационно-коммуникационных технологий на новый этап в 2022–2023 годах»;

Постановление Президента Республики Узбекистан от 21 июня 2024 года № ПҚ–229 «О мерах по организации научно-исследовательской деятельности в сфере цифровой криминалистики»;

Постановление Президента Республики Узбекистан от 22 января 2025 года № ПҚ–17 «О мерах по внедрению системы подготовки профессиональных кадров в сфере противодействия преступлениям, совершаемым с использованием цифровых технологий»;

Постановление Президента Республики Узбекистан от 30 апреля 2025 года № ПҚ–153 «О мерах по дальнейшему усилению борьбы с преступлениями, совершаемыми с использованием информационных технологий»;

Постановление Президента Республики Узбекистан от 30 апреля 2025 года № ПҚ–155 «О комплексных мерах по цифровой трансформации системы органов внутренних дел».

Принятие указанных постановлений стало одним из важных шагов в регулировании данной сферы.

Основная часть

В настоящее время цифровые технологии глубоко проникли практически во все сферы нашей жизни. С одной стороны, это повышает удобство и

эффективность, с другой — порождает новые виды угроз, в частности киберпреступления. Киберпреступления представляют собой правонарушения, совершаемые с использованием интернета, компьютеров и цифровых средств, а их выявление, расследование и предупреждение отличаются высокой сложностью и требуют высокого уровня профессиональной подготовки. В связи с этим на специалистов, работающих в данной области, возлагается большая ответственность и предъявляются особые требования.

А. А. Эйсман отмечает, что специальные знания — это «знания не общеизвестные и не общедоступные», которыми располагает ограниченный круг специалистов. В свою очередь, З. И. Соколовский уточняет, что под специальными знаниями следует понимать совокупность сведений, полученных в результате профессиональной подготовки и создающих для их обладателя возможность решения задач в определенной области.

Прежде всего, специалист должен обладать глубокими знаниями о природе, механизмах и современных технических средствах киберпреступлений. Он должен иметь достаточные знания в области компьютерных сетей, операционных систем, криптографии, интернет-протоколов и структур баз данных. В современных условиях цифровой среды специалист должен обладать не только теоретическими знаниями, но и уметь подтверждать свои навыки на практике.

В зарубежных странах специалисты (в том числе представители частного сектора) также наделяются полномочиями участвовать в расследовании. Специалист может выполнять следующие задачи:

предоставлять первичную информацию о состоянии цифрового устройства и уровне информационной безопасности;

давать предварительные и последующие сведения о системной и сетевой архитектуре (конфигурации);

вырабатывать методические рекомендации по выбору тактики следственных действий;

принимать меры по нейтрализации средств удаления или уничтожения цифровых данных, а также кибератак;

выявлять данные, хранящиеся в облачных сервисах;

оказывать содействие в выявлении и фиксации в протоколах цифровых доказательств (следов), имеющих значение для дела;

выявлять цифровые доказательства (следы) и их источники, а также осуществлять их копирование;

оказывать практическую помощь в документировании последовательности действий, выполненных на цифровом устройстве;

анализировать и исследовать доказательства, имеющие значение для дела;

давать научно обоснованные заключения по результатам исследований;

предоставлять разъяснения по своим выводам в ходе следствия и судебного разбирательства.

В то же время участие специалиста при допросе подозреваемого или обвиняемого способствует быстрому и полному раскрытию преступления, а также установлению способа и механизма его совершения.

Следует подчеркнуть, что сбор, проверка и оценка следов в цифровой среде требуют специальных знаний, умений и компетенций в узкопрофильной сфере. В связи с этим обеспечение участия специалиста в процессе расследования имеет принципиальное значение. Статья 204[1] действующего Уголовно-процессуального кодекса Республики Узбекистан также предусматривает, что представленные электронные данные должны приниматься должностным лицом органа доследственной проверки, дознавателем, следователем, прокурором или судом с обязательным участием специалиста.

Однако возникает закономерный вопрос: какого именно специалиста следует привлекать к участию в следственном процессе? Поскольку данная сфера носит технический характер, привлечение любого специалиста без должной квалификации может привести к методическим ошибкам. Следователь при решении данного вопроса должен учитывать профессиональную компетентность и опыт специалиста.

В этой связи исследователи Д. И. Чукова, Д. А. Медведев и М. В. Литвиненко предлагают следующие требования:

а) специалист должен обладать навыками выявления и расследования преступлений и иных правонарушений, совершаемых с использованием компьютерных технологий;

б) специалист должен уметь использовать современные программные средства, инструменты, языки программирования и системы для решения профессиональных задач;

в) специалист должен обладать навыками сбора, анализа и оценки информации, имеющей значение для применения правовых норм в сфере компьютерной информации.

У. В. Галкина считает, что применение специальных знаний при производстве следственных действий возможно посредством участия специалиста под непосредственным руководством следователя, а также эксперта при проведении судебной экспертизы.Вместе с тем, в отношении рассматриваемой категории дел большинство следственных действий не может быть эффективно проведено без участия специалиста, поскольку следователи, не обладая необходимым уровнем знаний в области компьютерных технологий, могут своими действиями привести к утрате или повреждению доказательств, которые в данном случае имеют ключевое значение.

Основной вывод автора заключается в том, что стремительное развитие компьютерных технологий приводит к постоянному усложнению и обновлению киберпреступлений; поэтому для их эффективного выявления и расследования необходимо участие специалистов в данной области, поскольку быстрое появление новых видов вирусов и вредоносных программ существенно затрудняет защиту и обработку цифровой информации.

А. Р. Давронов считает, что успешное расследование преступлений, совершаемых с использованием цифровых технологий, требует комплексного подхода, основанного на тесном взаимодействии научных разработок, практической деятельности правоохранительных органов и технической экспертизы в области информационных технологий. По его мнению, эффективность расследования во многом зависит от уровня подготовки специалистов, участвующих в процессуальных действиях, а также от их способности применять современные цифровые инструменты при работе с доказательствами. В этой связи автор подчеркивает необходимость формирования системы подготовки специалистов нового типа, обладающих одновременно юридическими знаниями и практическими навыками в сфере цифровой криминалистики.

Согласно международному стандарту ISO/IEC 27037:2012, специалист должен обладать соответствующей технической и юридической квалификацией. В соответствии с данным стандартом специалист должен иметь достаточную подготовку в области обработки цифровых доказательств для выполнения следственных задач, а также уметь демонстрировать свои навыки и компетенции при работе с информацией, представленной в цифровой форме (идентификация, сбор, изъятие, хранение, обеспечение сохранности, уничтожение и др.) в соответствующих сферах. Иными словами, он должен понимать и уметь применять соответствующие процессы и методы обращения с доказательствами из цифровых источников.

Заключение

Критерий компетентности также обеспечивает специалисту возможность эффективно использовать средства цифровой криминалистики. В противном случае даже самые современные инструменты цифровой криминалистики не смогут гарантировать качество получаемой цифровой информации (доказательств) при отсутствии у специалиста необходимой компетенции.

В целях повышения эффективности участия специалиста в расследовании киберпреступлений представляется целесообразным:

Во-первых, внедрить систему обязательной специализированной подготовки и переподготовки специалистов в области цифровой криминалистики, направленную на формирование устойчивых практических навыков работы с цифровыми доказательствами.

Во-вторых, разработать механизм профессиональной сертификации специалистов, подтверждающий их компетентность и уровень подготовки для участия в следственных действиях.

В-третьих, установить четкие критерии отбора специалистов, включая наличие профильного образования, практического опыта и знаний действующего законодательства.

В-четвертых, совершенствовать процессуальный статус специалиста путем более четкого определения его прав, обязанностей и ответственности.

В-пятых, закрепить на законодательном уровне положение о том, что участие специалиста при проведении следственных действий с цифровыми устройствами и данными не является обязательным во всех случаях, а

определяется исходя из конкретных обстоятельств дела, уровня подготовки следователя и сложности проводимых действий.

При этом следует учитывать, что наличие у следователя специальных знаний, навыков и практического опыта (в том числе полученных в ходе предыдущей экспертной деятельности) позволяет ему самостоятельно проводить отдельные следственные действия с цифровыми доказательствами без обязательного привлечения специалиста.

Кроме того, сам факт участия специалиста не всегда гарантирует полноту и правильность получения цифровых доказательств, поскольку ключевое значение имеет уровень его профессиональной компетентности и соблюдение методических требований.

Предлагаемый подход позволит избежать излишних процессуальных ограничений, повысить самостоятельность следователя и обеспечить более гибкое и эффективное использование специальных знаний в уголовном процессе.

В целом, с учетом изложенного и исходя из характера уголовного дела, целесообразно привлекать в качестве специалистов лиц, прошедших переподготовку в области цифровой криминалистики, имеющих высшее образование, ранее участвовавших в аналогичных делах в качестве специалистов, обладающих практическим опытом и хорошо ориентирующихся в действующем законодательстве.

Список литературы

1. Постановление Президента Республики Узбекистан № ПҚ–357 (22 августа 2022 года). О мерах по выводу сферы информационно-коммуникационных технологий на новый этап в 2022–2023 годах. Ташкент.

2. Постановление Президента Республики Узбекистан № ПҚ–229 (21 июня 2024 года). О мерах по организации научно-исследовательской деятельности в сфере цифровой криминалистики. Ташкент.

3. Постановление Президента Республики Узбекистан № ПҚ–17 (22 января 2025 года). О мерах по внедрению системы профессиональной подготовки кадров в сфере противодействия преступлениям, совершаемым с использованием цифровых технологий. Ташкент.

4. Постановление Президента Республики Узбекистан № ПҚ–153 (30 апреля 2025 года). О мерах по дальнейшему усилению борьбы с

преступлениями, совершаемыми с использованием информационных технологий. Ташкент.

5. Постановление Президента Республики Узбекистан № ПҚ–155 (30 апреля 2025 года). О комплексных мерах по цифровой трансформации системы органов внутренних дел. Ташкент.

6. Уголовно-процессуальный кодекс Республики Узбекистан (с изменениями и дополнениями). Статья 204¹.

7. ISO/IEC 27037:2012. Информационные технологии — Методы обеспечения безопасности — Руководство по идентификации, сбору, получению и сохранению цифровых доказательств. Международная организация по стандартизации (ISO), Женева.

8. Chukova, D.I., Medvedev, D.A., & Litvinenko, M.V. (2019). Проблемы привлечения специалистов при расследовании компьютерных преступлений. Москва: Издательство Московского государственного юридического университета.

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

10. Baryamureeba, V., & Tushabe, F. (2004). The Enhanced Digital Investigation Process Model. Proceedings of the Digital Forensics Research Workshop (DFRWS).

11. У.В. Галкина. Участие специалиста, как обязательное условие производства отдельных следственных действий при расследовании преступлений в сфере компьютерной информации. Криминологический журнал, (4), 43-46. 2020. doi: 10.24411/2687-0185-2020-10070

12. А. Р. Давронов. Участие специалиста в области информационных технологий в следственных действиях по уголовным делам // Актуальные проблемы социально-гуманитарных наук. Том 5, специальный выпуск 7. – С. 148–155. – 2025.