Процедурные аспекты обыска с изъятием цифровых устройств: порядок привлечения специалиста при изъятии электронных носителей; роль понятых при копировании данных с изымаемых устройств; оформление протокола: обязательные реквизиты и типичные ошибки

Александров Сергей Алексеевич
аспирант Московского финансово-промышленного университета "Синергия", kliolcom2021@yandex.ru

Рассматриваются процессуальные особенности проведения обыска с изъятием цифровых устройств в рамках уголовного судопроизводства. Раскрываются условия и порядок привлечения специалиста при изъятии электронных носителей информации, анализируется значение его участия для сохранности и неизменности цифровых данных. Отдельное внимание уделяется роли понятых при копировании информации с изымаемых устройств с учетом специфики электронных доказательств. Анализируются требования к оформлению протокола обыска, его обязательные реквизиты, а также типичные ошибки, допускаемые на практике и способные повлечь признание полученных доказательств недопустимыми. Обосновывается необходимость строгого соблюдения уголовно-процессуальных норм и учета технических особенностей цифровой информации при производстве следственных действий.

Ключевые слова: обыск, цифровые устройства, электронные носители информации, специалист, понятые, протокол следственного действия.

Доказательства являются центральным институтом уголовного судопроизводства, целью которого устанавливается подтверждение или опровержение виновности, или подтверждение невиновности лица, подозреваемого (обвиняемого) в совершении преступления. В соответствии с последовательно получаемыми органами предварительного расследования доказательствами строится архитектура уголовного дела, осуществляется планирование и выдвижение версий, их проверка на состоятельность, определяется процессуальная судьба участников уголовного дела, реализуется назначение уголовного судопроизводства в целом.

По мнению А.Р. Белкина, «доказательства являются средствами убеждения в истинности того ли иного предположения. А установление истины в процессе предварительного расследования осуществляется путем доказывания обстоятельств, совокупность которых составляет предмет исследования по данному делу» [2, с. 19]. С данным доводом соглашается и ряд других авторов [3; 6]. Несмотря на в большей степени философский подход к определению доказательств, следует отметить достоинство последнего, так как оно уточняет сущностную взаимосвязь между доказательством, необходимостью установления обстоятельств по делу и процессом доказывания.

Нормативное определение доказательств как правовой категории содержится в ст. 74 Уголовно-процессуального кодекса Российской Федерации (далее - УПК РФ) [5]. Так, доказательства

- это «любые сведения, на основе которых суд, прокурор, следователь, дознаватель в порядке, определенном настоящим Кодексом, устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела».

Доказательства, имея определенное фактическое содержание, не могут существовать вне формы, в связи с чем законодатель закрепляет определенные источники доказательств в ч. 2 ст. 74 УПК РФ [5]. Процесс собирания доказательств строго регламентирован уголовно-процессуальным законодательством, любое отступление от установленной нормы необходимо рассматривать как нарушение, которое будет иметь соответствующие правовые последствия;

- признание недопустимым и исключение из массива доказательств. Другим последствием признания доказательства, полученным незаконно, будет являться так называемый эффект «плодов отравленного дерева», когда производные от него доказательства также будут исключены из массива доказательств. В связи с этим особенно важно соблюдение законодательно установленных правил собирания доказательств.

Развитие высоких цифровых технологий обусловило появление в уголовном судопроизводстве принципиально новых способов доказывания, связанных с изъятием и исследованием электронных носителей информации, копированием компьютерной информации с различных электронных хранилищ, которые в настоящее время получили чрезвычайно широкое распространение [4, с. 77] и стали

частью обычной жизни. Соответственно, законодатель должен оперативно реагировать на данные изменения и определить правовой статус таких предметов и способов работы с ними в рамках правового поля.

Обыск с изъятием цифровых устройств является одним из наиболее сложных следственных действий, поскольку связан с обращением с электронными носителями информации, обладающими специфическими свойствами. Цифровые данные могут быть легко изменены, уничтожены либо утрачены в результате неквалифицированных действий, что обуславливает повышенные требования к процессуальному порядку их изъятия и фиксации.

Порядок привлечения специалиста при изъятии электронных носителей информации имеет принципиальное значение для обеспечения сохранности данных. В соответствии с уголовно-процессуальным законодательством специалист привлекается в случаях, когда для обнаружения, закрепления и изъятия электронных данных требуются специальные знания. На практике специалист обеспечивает корректное отключение цифровых устройств, предотвращение несанкционированного доступа к информации, а также осуществляет копирование данных с соблюдением требований неизменности их содержания. Отсутствие специалиста либо формальный характер его участия нередко приводит к утрате доказательственной ценности полученной информации [1, с. 150].

Роль понятых при копировании данных с изымаемых устройств также имеет существенное значение. Понятые призваны удостоверить факт и порядок проведения следственного действия, в том числе процесс копирования цифровой информации. Однако специфика электронных данных зачастую делает невозможным для понятых фактическую оценку содержания копируемой информации. В этой связи их участие носит в большей степени процессуально-гарантийный характер и направлено на подтверждение соблюдения установленной процедуры, а не на контроль технической стороны копирования.

Особое внимание должно уделяться оформлению протокола обыска. Протокол является основным процессуальным документом, фиксирующим ход и результаты следственного действия. К обязательным реквизитам относятся дата, время и место проведения обыска, сведения обо всех участниках, основания для его проведения, подробное описание изымаемых цифровых устройств, их технические характеристики, а также указание на применение технических средств и участие специалиста. При копировании данных в протоколе должны быть отражены используемые программы и носители, объем и формат скопированной информации.

К типичным ошибкам оформления протокола относятся неполное описание цифровых устройств, отсутствие сведений о специалисте, формальное указание на участие понятых без отражения их фактических действий, а также отсутствие данных о способе копирования информации. Подобные нарушения могут повлечь признание протокола ненадлежащим доказательством и исключение цифровых данных из доказательственной базы по делу [1, с. 151].

Таким образом, обыск с изъятием цифровых устройств требует строгого соблюдения процессуальных норм и учета особенностей электронных носителей информации. Привлечение квалифицированного специалиста, надлежащее участие понятых и корректное оформление протокола являются необходимыми условиями обеспечения законности и допустимости полученных цифровых доказательств.

Дополнительно следует отметить, что при изъятии цифровых устройств особое значение имеет выбор способа обращения с электронными носителями информации. В зависимости от конкретной следственной ситуации изъятие может осуществляться как путем физического изъятия устройства, так и посредством копирования содержащихся на нем данных. Выбор конкретного способа должен быть обусловлен необходимостью обеспечения баланса между интересами расследования и соблюдением прав участников уголовного процесса, включая право на сохранность личной и служебной информации.

Практика показывает, что наибольшее количество процессуальных нарушений допускается при отсутствии четкого разграничения функций между следователем и специалистом. Следователь отвечает за процессуальное руководство обыском и принятие решений, тогда как специалист выполняет исключительно технические действия, требующие специальных знаний. Превышение специалистом своих полномочий либо фактическая передача ему функций следователя может быть расценена как существенное нарушение уголовно-процессуального закона и повлечь сомнения в допустимости полученных доказательств [3, с. 215].

Отдельного внимания заслуживает вопрос обеспечения неизменности цифровой информации после ее копирования. В целях подтверждения подлинности и целостности скопированных данных в практике все чаще используются контрольные суммы и иные средства идентификации цифровых файлов. Отражение сведений о применении таких средств в протоколе обыска способствует повышению доказательственной ценности цифровой информации и снижает риск ее оспаривания стороной защиты.

Наряду с этим существенную роль играет соблюдение прав лиц, у которых производится обыск. Изъятие цифровых устройств зачастую связано с ограничением доступа к информации, необходимой для осуществления профессиональной или предпринимательской деятельности. В этой связи следователь обязан по возможности обеспечивать копирование только той информации, которая имеет значение для уголовного дела, а также фиксировать в протоколе ходатайства и заявления участников, связанные с порядком изъятия и копирования данных.

Таким образом, последующая оценка допустимости цифровых доказательств напрямую зависит не только от факта их обнаружения, но и от корректности процессуального оформления всех действий, связанных с изъятием и копированием информации. Соблюдение разграничения полномочий, использование технических средств фиксации целостности данных и отражение всех существенных обстоятельств в протоколе позволяют минимизировать риски признания доказательств недопустимыми и способствуют достижению целей уголовного судопроизводства [6, с. 100].

В современных условиях особую актуальность приобретает вопрос фиксации хода обыска с изъятием цифровых устройств с использованием технических средств. Применение фото-, видео- и аудиозаписи позволяет более полно отразить последовательность действий следователя, специалиста и иных участников следственного действия. Такая фиксация приобретает дополнительное значение при работе с электронными носителями информации, поскольку позволяет подтвердить отсутствие вмешательства в цифровые данные и соблюдение установленного процессуального порядка.

Вместе с тем использование технических средств фиксации требует надлежащего процессуального оформления. Сведения о применяемых средствах, условиях и времени записи должны быть отражены в протоколе обыска. Отсутствие указаний на факт видеозаписи либо несоответствие между зафиксированными в протоколе сведениями и фактическим ходом следственного действия может вызвать сомнения в достоверности полученной информации и стать основанием для ее критической оценки судом.

Отдельного внимания заслуживает проблема соотношения оперативности проведения обыска и необходимости соблюдения всех процессуальных гарантий при работе с цифровыми устройствами. Стремление к быстрому получению информации нередко приводит к упрощению процедуры изъятия электронных носителей, что выражается в отказе от копирования данных на месте либо в игнорировании требований к детальному описанию совершаемых действий. Подобный подход способен негативно сказаться на последующей оценке доказательств и осложнить их использование в судебном разбирательстве.

Значимым аспектом является и вопрос последующего хранения изъятых цифровых устройств и носителей информации. Нарушение условий хранения, отсутствие учета доступа к электронным данным либо ненадлежащее документирование передачи носителей между должностными лицами создают риски утраты либо изменения информации. В этой связи особую роль приобретает фиксация в материалах уголовного дела сведений о передаче, упаковке и опечатывании цифровых носителей, а также о лицах, ответственных за их сохранность [7, с. 50].

Таким образом, эффективность обыска с изъятием цифровых устройств определяется не только результатами обнаружения информации, но и качеством процессуального сопровождения всех последующих действий. Комплексный подход, включающий техническую фиксацию, соблюдение процессуальных гарантий и надлежащее документирование, позволяет обеспечить надежность цифровых доказательств и их устойчивость при судебной проверке.

Литература

1. Андреева Ю. И. Электронные доказательства в уголовном процессе // Закон и право. - 2025. – С. 147-152.
2. Белкин А.Р. Теория доказывания в уголовном судопроизводстве: в 2 ч. / А.Р. Белкин. - 2-е изд. - Москва : Юрайт, 2019. - Ч. 1. - 184 с.
3. Лукошкина С. В. Проблемы изъятия электронного носителя информации в контексте участия специалиста и назначения судебных экспертиз / С. В. Лукошкина // Всероссийский криминологический журнал. - 2024. - Т. 18, № 2. - С. 210–217.
4. Слифиш М. В. Доказывание в уголовном процессе Российской Федерации: учеб. пособие. - М. : ИНФРА-М, 2024. - 255 с.
5. Уголовно-процессуальный кодекс Российской Федерации. М.: Проспект, 2024. - 512 с.
6. Электронные доказательства в уголовном судопроизводстве: учеб. пособие для вузов / отв. ред. С. В. Зуев. - М. : Юрайт, 2022. - 193 с.
7. Яковлева Н. Г. Использование цифровых доказательств в уголовном судопроизводстве Российской Федерации // Вестник Тверского государственного университета. Серия: Право. - 2024. № 4 (80). - С. 45–52.

Procedural aspects of searches involving the seizure of digital devices: the procedure for engaging a specialist during the seizure of electronic data carriers; the role of attesting witnesses in copying data from seized devices; drafting the protocol: mandatory details and typical errors

Alexandrov S.A.

Moscow Financial and Industrial University "Synergy"

The article examines procedural issues related to searches involving the seizure of digital devices in criminal proceedings. The conditions and procedure for engaging a specialist during the seizure of electronic data carriers are analyzed, with emphasis on ensuring the integrity and preservation of digital information. Special attention is paid to the role of attesting witnesses during the copying of data from seized devices, taking into account the specific nature of electronic evidence. The requirements for drafting a search protocol, its mandatory details, and typical mistakes made in practice that may lead to the recognition of evidence as inadmissible are considered. The necessity of strict compliance with criminal procedural norms and consideration of the technical features of digital information is substantiated.

Keywords: search, digital devices, electronic data carriers, specialist, attesting witnesses, procedural protocol.

References

1. Andreeva Yu. I. Electronic evidence in criminal proceedings // Law and Right. - 2025. - Pp. 147-152.
2. Belkin A.R. Theory of evidence in criminal proceedings: in 2 parts / A.R. Belkin. - 2nd ed. - Moscow: Yurait, 2019. - Part 1. - 184 p.
3. Lukoshkina S. V. Problems of seizure of electronic information carriers in the context of participation of a specialist and appointment of forensic examinations / S. V. Lukoshkina // All-Russian Criminological Journal. - 2024. - Vol. 18, No. 2. - Pp. 210-217.
4. Slifish M. V. Evidence in criminal proceedings of the Russian Federation: textbook. manual. - M.: INFRA-M, 2024. - 255 p.
5. Criminal Procedure Code of the Russian Federation. M.: Prospect, 2024. - 512 p.
6. Electronic Evidence in Criminal Proceedings: A Textbook for Universities / Ed. S. V. Zuev. - M.: Yurait, 2022. - 193 p.
7. Yakovleva N. G. Use of Digital Evidence in Criminal Proceedings of the Russian Federation // Bulletin of Tver State University. Series: Law. - 2024. No. 4 (80). - P. 45–52.