Искакова Б. Е., *научный сотрудник центра по исследованию проблем расследования преступлений НИИ, магистр юридических наук, майор полиции*

(Карагандинская академия МВД РК им. Б. Бейсенова, г. Караганда, Республика Казахстан)

Особенности производства выемки электронных носителей информации при расследовании экстремистских и террористических преступлений

Аннотация. В статье анализируется проблема применения норм уголовно-процессуального законодательства РК, регламентирующих изъятие электронных носителей информации при производстве следственных действий по экстремистским и террористическим преступлениям. Рассмотрен порядок изъятия электронного носителя информации как доказательства по уголовным делам. Обозначены проблемные аспекты определения места электронных носителей в системе доказательств по экстремистским и террористическим преступлениям. Проводится анализ криминалистических аспектов выемки электронных носителей информации в ходе расследования преступлений в Республике Казахстан, предлагаются пути решения существующих в этой области проблем. Автор акцентирует внимание на положительном опыте Российской Федерации по производству выемки электронных носителей информации в ходе расследования преступлений и пути решения существующих в этой области проблем.

Ключевые слова: выемка, изъятие, электронные носители информации, экстремизм, терроризм, специалист, копирование, ходатайства, расследование преступлений, уголовно-процессуальное законодательство.

Стремительное развитие современного информационного общества и высоких технологий, использование информации, содержащейся на электронных носителях, в качестве доказательств по уголовным делам стало актуально при расследовании не только преступлений в области компьютерной информации, экономической деятельности, но и экстремистских и террористических уголовных правонарушений.

Анализ практической деятельности правоохранительных органов, на территории Республики Казахстан разжигание национальной, религиозной розни, пропаганда и вербовка в экстремистские и террористические организации осуществляются различными методами. При этом использование ими Интернет-среды для террористических целей стало намного шире, сами же они при этом остаются в безопасности. В силу трансграничного характера Интернета противодействие его использованию в террористических целях является проблемой, которая требует совместных усилий государства, бизнеса и общественных организаций [1].

В связи с появлением новых способов совершении экстремистских и террористических преступлений, связанных с применением современных технологий, в ходе проведения осмотра, обыска и выемки возникает необходимость изъятия электронных носителей информации, которые впоследствии могут быть использованы в доказывании.

В соответствии со ст. 1 Закона Республики Казахстан «Об информатизации» от 24 ноября 2015 г. электронным носителем является материальный носитель, предназначенный для хранения информации в электронной форме, а также записи или ее воспроизведения с помощью технических средств [2]. К наиболее распространенным материальным носителям относятся карты памяти sim [3] или flash [4], дискеты, CD, DVD, жесткие диски компьютера, сотовые телефоны, планшеты и другие информативные электронные устройства, с помощью которых можно получить информацию о записях в телефонной книге, журналах вызовов, текстовых сообщениях, контактах в электронной почте, переписке в различных социальных сетях, изображениях, аудио и видео-файлах и других действиях с телефоном.

На электронных носителях может быть обнаружена информация, запрещенная законом к распространению, содержащая экстремистские и террористические материалы, электронная корреспонденция участников преступления, касающаяся его организации и исполнения,

сведения о связях преступников и используемых средствах коммуникации, а также планируемых преступлениях.

Важно, что на таких носителях может оставаться информация из предварительно удаленных пользователем файлов, которые при использовании специального программного обеспечения может быть восстановлена. Чтобы доказать преступление, в котором использовались социальные сети, следователю необходимо получить доступ к файлам либо фрагментам из переписки, которые помогут представлять интерес для расследования. Данные информации могут быть изъяты при производстве обыска и выемки.

В Уголовно-процессуальном кодексе Республики Казахстан процессуальный порядок производства обыска и выемки регламентирован ст. 254 и должен соблюдаться лицом, осуществляющим досудебное расследование, по мотивированному постановлению. Постановление о производстве обыска, а также выемки документов, содержащих государственные секреты или иную охраняемую законом тайну, должно быть санкционировано следственным судьей [5].

Процессуальный порядок получения доказательной информации электронных носителей информации при производстве по уголовным делам в УПК РК не регламентирован, поэтому остается открытым вопрос об уровне компетентности лиц, осуществляющих досудебное расследование, в частности наличии у них знаний и опыта, необходимых для качественного извлечения электронных данных и с различных накопителей, на которых они содержались.

Практика показывает, что процесс изъятия электронных носителей информации, осмотр иихописание в протоколах следственных действий вызывает затруднения у следователей и органов дознания.

Применение рекомендаций по сохранению компьютерной информации в практической деятельности вызывает затруднения, так как любая новая ситуация по-своему уникальна, и действия следователя, приемлемые в большинстве случаев, в некоторых ситуациях могут нанести непоправимый ущерб. Поэтому лицо, осуществляющее выемку электронных носителей, должно иметь не только соответствующую квалификацию, но и осознавать суть процессов, происходящих в компьютерной системе, так как в ходе изъятия и хранения следователю необходимо разбираться в принципах записи, хранения и удаления информации каждого из носителей. Указанные требования являются высокими, что подтверждает необходимость обязательного участия специалиста при изъятии электронных носителей.

Согласно УПК РК в качестве специалиста для участия в производстве по уголовному делу может быть привлечено незаинтересованное в деле лицо, обладающее специальными знаниями, необходимыми для оказания содействия в собирании, исследовании и оценке доказательств путем разъяснения участникам уголовного процесса вопросов, входящих в его специальную компетенцию, а также применения научно-технических средств. Специалистами являются также педагог, психолог, участвующие в следственных и иных процессуальных действиях с участием несовершеннолетнего, а равно врач, участвующий в следственных и иных процессуальных действиях, за исключением случаев назначения его экспертом.

Т. И. Абдурагимова и И. В. Трущенков считают, что для технически грамотного производства указанных следственных действий недостаточно наличия у специалиста поверхностных знаний в сфере компьютерных технологий, которыми обладает большинство пользователей персонального компьютера, в том числе следователи и специалисты-криминалисты. Нужны специалисты со знаниями в таких областях, как: функционирование операционных систем, основы доступа и сохранения содержимого оперативной памяти, организация компьютерных сетей, поиск скрытой компьютерной информации [6].

Необходимо понимать, что участие специалиста направлено на:

– правильное проведение изъятия электронных носителей информации;

– осуществление копирования информации с электронных носителей;

– обеспечение их хранения в последующем.

Электронные носители информации изымаются целиком (системные блоки, ноутбуки, сотовые телефоны, планшеты) и направляются на экспертизу в тех случаях, если копирование информации не производится.

Копирование информации — это процесс создания цифровой копии информационного объекта. В качестве объекта копирования могут выступать файлы и папки, разделы жёсткого диска и диск целиком, базы данных, сайты. Копирование производится на другие электронные носители информации, предоставленные законным владельцем изъятых носителей информации. Об осуществлении копирования информации и передаче ее на электронные носители составляется протокол.

Электронные носители информации хранятся в опечатанном виде, обеспечивающем их сохранность и сохранность информации. Следователь ни в коем случае не должен допускать других лиц к содержимому изъятых носителей на компьютерной технике, производить на них запись любых файлов, т. е. на экспертизу они должны быть направлены именно в том виде, в котором были обнаружены и изъяты. Законодатель Российской Федерации, например, подчеркивая актуальность данной проблемы, внес в ст. 183 УПК РФ изменения, регламентирующие основания и порядок производства выемки: «При производстве выемки изъятие электронных носителей информации производится с участием специалиста. По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в выемке, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации. При производстве выемки не допускается копирование информации, если это может воспрепятствовать расследованию преступления, либо, по заявлению специалиста, повлечь за собой утрату или изменение информации. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации в протоколе делается запись» [7].

В условиях постоянного развития технических средств и появления новых технологий хранения информации представляется необходимым увеличение штата специалистов в области современных информационных технологий, которые могли бы участвовать в следственных действиях в составе следственно-оперативных групп, так как извлечение и копирование электронных носителей информации может осуществить только специалист, обладающий специальными знаниями в области компьютерной техники.

В связи с этим считаем необходимым перенять положительный опыт Российской Федерации по производству выемки и ввести в уголовно-процессуальное законодательство Республики Казахстан соответствующие изменения, а именно п. 4-3 ст. 254 УПК РК изложить в следующей редакции: «При производстве выемки электронных носителей информации участвует специалист, обладающий специальными знаниями в области компьютерной техники. В присутствии законного владельца либо обладателя электронных носителей информации специалист осуществляет копирование информации с изъятого электронного носителя информации. Не допускается копирование информации, если это может воспрепятствовать расследованию преступления, а также по заявлению специалиста повлечь за собой утрату или изменение информации».

Түйін

Мақалада экстремистік және террористік қылмыстарды тергеу барысында электрондық ақпаратты тасымалдаушылардан көшіріп алуды реттейтін Қазақстан Республикасының Қылмыстық іс жүргізу заңнамасының нормаларын қолдану мәселесі талданады. Ресей Федерациясының қылмыстарды тергеу барысында электронды бұқаралық ақпарат құралдарының көшіріп алынуын және осы саладағы бар проблемаларды шешу жолындағы оң тәжірибесін қабылдау ұсынылады.

Resume

The article analyzes the problem of applying the norms of the Criminal Procedural Legislation of the Republic of Kazakhstan regulating the seizure of electronic information carriers in the process of investigating extremist and terrorist crimes. It is proposed to adopt the positive experience of the Russian Federation in the production of the seizure of electronic media during the investigation of crimes and the ways of solving existing problems in this field.

Список использованной литературы:

1. Терроризм и Интернет: Мат-лы международ. науч.-практ. конф. // Электронный ресурс: http://online.zakon.kz/Document/?doc_id=358948 39#pos=0;0.

2. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 г. № 418-V // https://online.zakon.kz

3. SIM-карта (англ. Subscriber Identification Module — модуль идентификации абонента) — идентификационный модуль абонента, применяемый в мобильной связи // Электронный ресурс:https://ru.wikipedia.org/wiki/SIM-%D0%BA%D0%B0%D1%80%D1%82%D0%B0.

4. Ка́рта па́мяти (иногда неправильно — флеш-ка́рта) — компактное электронное запоминающее устройство, используемое для хранения цифровой информации. Современные карты памяти изготавливаются на основе флеш-памяти, хотя принципиально могут использоваться и другие технологии. Карты памяти широко используются в электронных устройствах, включая цифровые фотоаппараты, сотовые телефоны, ноутбуки, портативные цифровые аудиопроигрыватели // Электронный ресурс: https://ru.wikipedia.org/ wiki/%D0%9A%D0% B0%D1 %80%D1%82%D0%B0_%D0%BF%D0%B0%D0%BC%D1%8F%D1%82%D0%B8.

5. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. № 231-V ЗРК // Казахстанская правда. 2014. 10 июля.

6. Абдурагимова Т. И., Трущеноков И. В. К вопросу о производстве обыска и выемки в целях обнаружения объектов для проведения судебной компьютерной экспертизы. http://www.proexpertizu.ru/general_questions/711/.

7. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ (ред. от 29.07.2017 г., с изм. от 14.11.2017) (с изм. и доп., вступ. в силу с 01.09.2017) // Электронный ресурс: http://www.consultant.ru/document/cons_doc_LAW_34481/.