работника по контролю за поведением пациента при оказании МП (например, длительной фиксация пациента с психическим расстройством привела к развитию сердечно-сосудистой недостаточности); 6) отсутствует надлежащий контроль за поведением пациента при оказании МП, когда смерть наступает от несчастного случая. Например, врач, изучая результаты рентгенографии, не замечает, что пациент, изначально находившейся в бессознательном состоянии, начал шевелиться, упал с каталки и получил смертельную черепно-мозговую травму.

Таким образом, в случае смерти лица, нуждающегося в МП, при проведении предварительного расследования следует выделять модели:

при неоказании медицинской помощи: 1) неявка медицинского работника по вызову; 2) отказ медработника от общения с больным;

при ненадлежащем оказании МП: 1) причиняются повреждения сверх необходимых; 2) возникают приводящие к смерти осложнения; 3) не выявлено заболевание (травма), приведшее к смерти; 4) отсутствует контроль за состоянием или поведением пациента, либо такой контроль проводится ненадлежащим образом.

Кузнецова Е. Н.

ЦИФРОВЫЕ СЛЕДЫ В КРИМИНАЛИСТИКЕ

Кузнецова Елизавета Николаевна, студентка 3 курса Уральского государственного юридического университета имени В. Ф. Яковлева, г. Екатеринбург, Россия, kuznetsova.elizaveta.nikolaevna@gmail.com

Научный руководитель: старший преподаватель Матвеев М. М.

Современное общество не может существовать без «цифры»: мы все время находимся в цифровом пространстве. Именно это неосязаемое цифровое пространство в XXI в. для криминалистики и для борьбы с преступностью в целом является основным источником «следовой картины» последствий преступного деяния. При совершении преступлений в сети Интернет непосредственный контакт преступника и потерпевшего в большинстве случаев исключается. Полностью уничтожить следы пребывания в коммуникационной сети невозможно, но существуют современные новые способы маскировки, поэтому каждый год растет преступность в информационной сфере. Согласно статистике МВД о состоянии преступности за январь–август 2022 г. зарегистрировано 334,1 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. К таким преступлениям относятся распространение экстремистской и иной запрещенной информации посредством сети Интернет, участие в схемах кражи электронных денег, Интернет и SMS-мошенничества, участие в группах смерти и т. д. Однако криминалистика не стоит на месте и находит новые приемы и способы раскрытия преступлений.

Новые объекты экспертного исследования возникли в связи с развитием цифровых технологий, поскольку информация об объектах сохраняется в

компьютерных средствах и системах в неявном виде, и для обеспечения возможности ее восприятия необходимо использовать специальные средства.

Соответственно, перед следователем в процессе операций по обнаружению, фиксации и изъятию цифровой информации возникает дополнительная задача, т. е. ему необходимо определить распространение потенциальной доказательственной информации, что предполагает идентификацию ее источника.

Поисковая деятельность следователя заключается в собирании доказательственной и ориентирующей криминалистически значимой информации, получить которую можно следующими способами:

- с использованием технических средств (таких как ПК, ноутбук, электронный планшет и др.) осуществляется поиск информации для посещения страницы пользователя социальной сети (в данном случае следствие интересует ID);
- в соответствии с ч. 7 ст. 185 Уголовно-процессуального кодекса Российской Федерации (УПК) следователь по решению суда вправе провести осмотр и выемку сведений, которые могут содержаться в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях; однако ст. 186.1 УПК позволяет лишь получить информацию о соединениях между абонентами и (или) абонентскими устройствами, поэтому актуальным становится так называемое электронное «наблюдение» – производство, которое в настоящее время недостаточно регламентировано законодателем.
- поиск информации о пользователях социальной сети и (или) мессенджеров осуществляется с помощью электронно-вычислительных мощностей.

Таким образом, цифровой след представляет собой криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде в процессе ее возникновения, обработки, хранения и передачи. Говоря о проблемных вопросах изъятия цифровых следов, стоит отметить, что процедура фиксации и изъятия таких следов из социальных сетей и мессенджеров требует определенного порядка, связанного со спецификой данных объектов. Несоблюдение правил работы с такими доказательствами может привести к признанию полученных цифровых данных из сети Интернет или электронных носителей информации недостоверными и, как следствие, недопустимыми доказательствами по делу.

Ломако В. А.

ГРАФОЛОГИЯ:КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ

Ломако Валерия Александровна, студентка 4 курса Белорусского государственного университета, г. Минск, Беларусь, lerslomako20@gmail.com

Научный руководитель: канд. юрид. наук, доцент Хлус А. М.

Графология в широком понимании является областью знаний, изучающей личность, ее характер на основе почерка, его особенностей и закономерностей развития. Графология в криминалистическом понимании