При исследовании объективных факторов Э. Р. Гареева выделила следующие основания:

а) социально-экономические условия (встречаются случаи, когда допрашиваемые лица не имеют дохода, следовательно, они дают ложные показания, итогом которых является денежное вознаграждение со стороны виновного лица);

б) непрофессионализм следователя (в случаях настойчивости, некорректности следователя, допрашиваемые лица могут иметь желание доставить неприятности следователю);

в) психологические или физические воздействия со стороны заинтересованных лиц (получение угроз с требованиями изменить показания или вовсе отказаться от них).

И. А. Оточина, Л. И. Рукабер исследовали только социальные факторы, а именно:

1) свойства восприятия и памяти свидетеля (некоторая информация может быть изложена полно и точно, а другая лишь в общих чертах);

2) психическое и физическое состояние (усталость, волнение и др. состояния, которые неблагоприятно влияют на показания);

3) патологические дефекты психики и нервной системы (как правило, сведения, которые были получены сразу после совершения преступления, являются более точными, без вымышленных деталей.

Таким образом, факторы формирования ложных показаний можно разделить на две группы: субъективные (личностные) и объективные. К субъективным фактором следует отнести: 1) характер и темперамент личности; 2) эмоциональное, психическое, физическое состояние; 3) наличие различных отношений (родственных, дружелюбных, служебных и др.); 4) патологические дефекты психики и нервной системы. К объективным факторам следует отнести: 1) социально-экономические условия; 2) непрофессионализм следователей; 3) психологические или физические воздействия со стороны заинтересованных лиц.

Лузгин И. И., Середа А. Е.

АКТУАЛЬНЫЕ ВОПРОСЫ СБОРА КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ В РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Лузгин Иван Иванович, Середа Александр Евгеньевич аспиранты кафедры криминалистики Белорусского государственного университета, г. Минск, Беларусь, luzgin@bsu.by, sereda1993law-minsk@yandex.by

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

Расследование киберпреступлений представляет собой трудоемкий процесс, в рамках которого возникает больше вопросов, чем ответов. В ряде случаев применяется стратегия расследования, включающая следующие

элементы: идентификация источников криминалистически значимой информации (1); сбор идентифицированных источников (2); изъятие информации (3); анализ собранной информации и ее использование (4).

Идентификация источника доказательств – это наиболее значимый шаг в расследовании киберпреступлений. По состоянию на 2021 г., уровень технологического развития позволил используемым электронным девайсам находиться в состоянии постоянного взаимного информационного подключения (interconnection), что придает расследованию своеобразную специфику. К примеру, социальные сети (далее – соцсети) могут содержать и распространять релевантную информацию о девайсе и о его пользователе, которая является потенциальным доказательством.

Источниками же доказательств могут быть смартфоны, компьютеры, ноутбуки, планшеты и др. Для расследования киберпреступления может быть необходимо иметь доступ к интернет-истории подозреваемого, аккаунтам в соцсетях, деталям об осуществленных им действиях онлайн, в том числе содержанию почты, онлайн-переводам и иным данным.

Нередко при расследовании киберпреступлений из имеющихся данных могут быть только ссылка на аккаунт в соцсетях или URL-адрес, который связан каким-либо образом с совершенным преступным деянием или девайсом (в данном случае выступающим орудием преступления).

Сбор источников доказательств в расследовании киберпреступлений отличается от сбора доказательств (или их источников) при расследовании иных видов преступных деяний, так как иногда следователям не удается изъять физический носитель информации для изучения и анализа. В таких случаях сбор доказательств происходит путем работы с вебсайтами, созданием скриншотов, сохранением чистого HTML кода с последующей распечаткой и приобщением к материалам дела, и т. д. Однако сохранение чистого HTML не гарантирует сохранения релевантных метаданных.

В связи с этим необходимо использовать специализированное программное обеспечение (далее – ПО), которое также будет подтверждать соответствие полученных данных истине. Следующим этапом выступает изъятие доказательства из источника (и его процессуальное оформление).

Изъятие доказательства из источника совершается посредством применения специализированного ПО при работе с самим девайсом или с URL-адресом, аккаунтом в соцсетях. При этом выделяется несколько подходов для осуществления этого действия в зависимости от типа устройства.

Существует два подхода к изъятию данных с персонального компьютера и ноутбука: Live Acquisition (девайс включен и доступна RAM), Offline Acquisition (девайс выключен и накопители памяти извлечены для создания копии для исследования (image copy).

Изъятие данных из смартфонов несколько отличается; используются следующие подходы: Logical Acquisition (специализированное ПО

взаимодействует с девайсом и находит искомую информацию; однако метод не работает если файлы были удалены или же девайс заблокирован), Physical Acquisition (ПО копирует файлы в накопителе данных с возможностью реставрации удаленных элементов, сообщений и GPS локаций).

Значимым аспектом является то, что исследователь не работает с источником потенциальных доказательств (primary evidence) напрямую (компьютер, смартфон и др.), а в соответствии с процессуальными нормами создает точную копию содержащихся в нем данных (secondary evidence), с которыми проводит необходимые действия с целью закрепления полученной информации как доказательства.

Основной трудностью данного этапа является то, что, как было отмечено ранее, не всегда у исследователя имеется изъятый для изучения девайс. В таких случаях исследуется релевантный URL или аккаунт в соцсетях. Целью исследователя является получение и анализ метаданных. Метаданные – это то что не видит (или не замечает) пользователь, но тем не менее является цифровым следом его активности (ID, дата создания поста в соцсетях, ID комментария, геолокация и многое другое).

Анализ полученных данных и их использование. Информация изымается из источников и анализируется посредством использования специализированного ПО (Belkasoft Evidence Center, BlackLight, Internet Evidence Finder, Magnet AXIOM, UFED Cloud Analyzer и др.).

Значимыми препятствиями в расследовании киберпреступлений выступают временные рамки хранения данных и метаданных на серверах соцсетей, их условия обслуживания (Terms of Service), внутренняя политика конфиденциальности (Privacy Policy), распространенное использование VPN, подставных аккаунтов в соцсетях, анонимизация пользователей и др.

В целях улучшения качества расследования и показателей раскрываемости киберпреступлений представляется целесообразным:

1) разработка ПО и баз данных, которые позволяют загружать актуальные для большинства популярных соцсетей документы, регулирующие использование предоставленной им пользователями информации (Terms of Service, Privacy Policy).

Целью данного ПО выступает автоматизация процесса запроса необходимой информации и регулирование процесса загрузки данных для целей расследования (без нарушения положений, прописанных в нормативных документах компаний, которым принадлежат соцсети);

2) создание закрытой базы данных на основе информации Интернет-провайдера, основной целью которой будет выступать контроль использования VPN с целью оптимизации временных затрат на выявление лиц, использующих VPN в сети Интернет.

Ввиду активного использования VPN киберпреступниками, необходимо предпринимать меры по выявлению лиц, пользующихся данной технологией и

связывать подставные IP-адреса, которые VPN предоставляет в пользование, с лицами, активно скрывающимися за ними;

3) разработка нормативных правовых актов, позволяющих на локальном и международном уровнях регулировать взаимодействие между правоохранительными органами, осуществляющими расследование определенного киберпреступления, и компаниями, которым принадлежат значительные информационные ресурсы (Google, Twitter, Facebook и т. д.).

Мешечко Л. А.

КОНФЛИКТ: КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ

Мешечко Любовь Александровна, студентка 3 курса Белорусского государственного университета, г. Минск, Беларусь, lyubovmeshechko301@gmail.com

Научный руководитель: канд. юрид. наук, доцент Красиков В. С.

В процессе расследования любого преступления возникают определенные отношения между следователем и иными лицами, участвующими в уголовном процессе. Одной из важнейших задач следователя является полное, всестороннее, объективное и оперативное расследование преступлений. Для решения данной задачи используются определенные способы воздействия на лицо.

Отношения, складывающиеся в досудебном производстве по уголовным делам, могут иметь бесконфликтный либо конфликтный характер. Конфликт рассматривается как противостояние интересов двух и более сторон в отношениях. Лицо, вовлеченное в конфликт, осуществляет определенную деятельность по достижению своей цели. Так, в процессе расследования может быть использовано психическое или физическое воздействие на участника уголовного процесса (например, подозреваемого, обвиняемого). Допустимость физического воздействия определяется соответствием действий лица законодательству определенного государства. При использовании методов психического воздействия влияние происходит на волю, эмоции лица с целью побудить его предоставить какую-либо информацию, совершить какие-либо действия.

Дискуссионным является вопрос допустимости обмана как способа воздействия на лицо. Под обманом следует понимать поступки, действия, вводящие других лиц в заблуждение. Обман может быть выражен как в прямой форме, так и в косвенной, когда выражения сами по себе ложными не являются, но использованы в таком контексте, что вводят в заблуждение лицо, участвующее в уголовном процессе. Считаем, что форма выражения обмана не влияет на допустимость либо недопустимость этого способа воздействия. От того, что обман подан в более сложной форме, не делает его более допустимым.