и активного содействия расследованию совершенного преступления, а также преступлений прошлых лет, оставшихся нераскрытыми. Использование положительных свойств личности, обращение следователя к положительным качествам собеседника во многих случаях приносит пользу. Каждому человеку свойственно стремление к самоуважению, и поэтому, апеллируя к честности, порядочности допрашиваемого, к его заслугам в прошлом, авторитету в коллективе, его личному и социальному статусу, его можно убедить быть откровенным, правдивым. Метод выжидания применяется к лицам, у которых происходит борьба мотивов, один из которых побуждает к даче ложных показаний или отказу от дачи показаний, а другой – к признанию своей вины, раскаянию в содеянном. Такая борьба мотивов может проявиться достаточно сильно при умелом тактическом воздействии следователя. Учитывая колебания допрашиваемого, следователь, сообщая определенные сведения, умышленно «закладывает» в его сознание такую информацию, которая должна обеспечить победу позитивных мотивов, и затем делает перерыв в допросе, выжидая, когда допрашиваемый сам откажется от мотивов, побуждающих его к даче ложных показаний.

Синтез традиционных коммуникативных методов, HUMINT и технологического профайлинга повышает эффективность следствия, однако требует строгого соблюдения правовых норм. Перспективы связаны с разработкой этических стандартов и обучением специалистов междисциплинарным компетенциям.

Звягин Д.С.,

кандидат технических наук
Воронежский институт МВД России

Особенности сбора и фиксации цифровых следов при противодействии киберпреступности

Цифровые следы – любой набор данных, способных подтвердить факт, время, участников и способ совершения противоправного действия в информационной среде. Их надлежащее обращение определяет успех расследования: даже один некорректный шаг может сделать доказательство недопустимым в суде.

Современная практика опирается на принцип «порядка летучести» (order of volatility): сначала фиксируют самые изменчивые артефакты (содержимое регистров процессора, оперативную память, сетевые соединения), затем – стабильные (логи, файлы на диске, резервные копии). Такой подход закреплен в международных руководствах, включая RFC 3227 и ISO/IEC 27037.

В целом технологический процесс сбора и фиксации цифровых следов при противодействии киберпреступности можно представить в виде следующего алгоритма:

1) идентификация: определение потенциальных носителей данных (стационарные и мобильные устройства, облачные сервисы, IoT-узлы, криптовалютные кошельки);

2) сбор: тщательное копирование бит-к биту с применением write-blockers и фиксированием хеш-контрольных сумм (SHA-256/512);

3) фиксация: создание неизменяемых образов, их дублирование и хранение в контролируемой среде;

4) документирование цепочки хранения: непрерывная запись всех действий, дат, исполнителей, стволов данных и контрольных сумм. Эти шаги прямо описаны в RFC 3227.

Следует отметить, что в России порядок изъятия цифровых носителей определяется ст. 164 и 183 УПК РФ; в международной практике применимы Будапештская конвенция и NIST SP 800-86. При этом инструменты для форензики должны проходить валидацию (методические рекомендации МВД РФ и ГОСТ Р ISO/IEC 27037-2021).

Современные вызовы и угрозы определяют трансформацию процедур сбора и фиксации цифровых следов:

– шифрование по умолчанию (E2EE-мессенджеры, TLS 1.3) усложняет онлайн-сбор; требуются live-memory-dump и извлечение ключей из RAM;

– децентрализованные платформы (блокчейн, Fediverse) – отсутствие единого оператора затрудняет обеспечение целостности и аутентичности;

– большие объемы данных требуют автоматизированной триаж-селекции и применения ИИ для выстраивания доказательств в приоритетном порядке.

Представляется, что лучшими практиками форензики в современных условиях являются следующие:

– использование стандарта ISO/IEC 27037 как «зонтичного» документа для процедур от идентификации до хранения;

– применение криптозащищенных журналов действий (immutable logs, blockchain-хеш-анкеры) для усиления доверия к цепочке хранения;

– внедрение регулярных ученй с моделированием утечек и скриптовой автоматизации фиксации RAM и сетевых дампов;

– поддержка квалификации экспертов.

Эффективное противодействие киберпреступности опирается на методически выверенный процесс сбора и фиксации цифровых следов. Его основа – баланс технологической точности, правовой чистоты и оперативности. Следование признанным стандартам, надежная цепочка хранения и постоянное обновление инструментов – ключ к тому, чтобы электронные доказательства выдержали проверку в суде и способствовали справедливому разбирательству.