ВЕСТНИК
КЕМЕРОВСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
СЕРИЯ: ГУМАНИТАРНЫЕ И ОБЩЕСТВЕННЫЕ НАУКИ

оригинальная статья

https://elibrary.ru/wdrlvy

Использование специальных знаний в области исследования компьютерной информации при расследовании преступлений, связанных со склонением к самоубийству или содействием совершению самоубийства

Ермошкин Дмитрий Александрович

Экспертно-криминалистический центр УВД на ММ ГУ МВД России по г. Москве, Россия, Москва

eLibrary Author SPIN: 1816-3171

ermosh.dmitr@mail.ru

Аннотация: На территории Российской Федерации наблюдается устойчивая тенденция увеличения киберпреступлений. Цель – провести комплексный анализ возможностей применения специальных знаний в сфере исследования компьютерной информации при расследовании преступлений, предусмотренных статьей 110.1 Уголовного кодекса Российской Федерации (склонение к совершению самоубийства или содействие совершению самоубийства). В работе выделены и систематизированы конкретные формы использования специальных знаний, а также обоснована с точки зрения криминалистической тактики необходимость привлечения к участию в производстве следственных действий и оперативно-розыскных мероприятий специалистов в области исследования цифровой информации при расследовании рассматриваемого состава преступлений. На основе судебно-следственной практики сформулирован перечень цифровой криминалистически значимой информации, подлежащей установлению в ходе проведения следственных действий, оперативно-розыскных мероприятий, а также судебных компьютерных (компьютерно-технических) экспертиз и исследований. Данный перечень включает цифровые следы, позволяющие идентифицировать пользователей и устройства, а также установить информацию, подтверждающую факты целенаправленного деструктивного психологического воздействия на потерпевшего. В результате сформулирован ряд основополагающих организационно-тактических и процессуальных тактических рекомендаций привлечения специалистов в области исследования цифровой информации. Соблюдение данных рекомендаций, по мнению автора, является ключевым условием для обеспечения эффективности, полноты и объективности предварительного расследования по делам данной категории, что способствует не только доказыванию события преступления, но и установлению круга лиц, причастных к его совершению.

Ключевые слова: специальные познания, компьютерная экспертиза, компьютерно-техническая экспертиза, содействие совершению самоубийства, склонение к совершению самоубийства, исследование компьютерной информации

Цитирование: Ермошкин Д. А. Использование специальных знаний в области исследования компьютерной информации при расследовании преступлений, связанных со склонением к самоубийству или содействием совершению самоубийства. *Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки*. 2025. Т. 9. № 4. С. 615–623. https://doi.org/10.21603/2542-1840-2025-9-4-615-623

Поступила в редакцию 23.09.2025. Принята после рецензирования 15.10.2025. Принята в печать 15.10.2025.

full article

Computer Expertise in Criminal Investigation: Crimes Related to Promoting or Aiding Suicide

Dmitry A. Ermoshkin

Forensic Center, Department of Internal Affairs of the Moscow Metro, Ministry of Internal Affairs of Russia, Russia, Moscow

eLibrary Author SPIN: 1816-3171

ermosh.dmitr@mail.ru

Abstract: Encouraging or aiding a suicide attempt is a crime (Article 110.1, Criminal Code of the Russian Federation). In connection with the current surge in cybercrimes, computer information research offers new procedural and criminalistic solutions in suicide-related investigations. The article offers a comprehensive categorization

BULLETIN
KEMEROVO STATE UNIVERSITY
SERIES: HUMANITIES AND SOCIAL SCIENCES

of expert knowledge and criminalistic tactics in digital information research to be used in criminal investigation. Based on legal and investigative practice, the author formulated a checklist for forensic computer experts. This list includes digital traces that lead to particular users and devices, as well as retrieving confirmation of deliberate destructive psychological influence. The checklist of organizational, tactical, and procedural principles for engaging computer specialists in criminal investigation provides effective, thorough, and objective pre-trial investigation for this category of crime. Apart from contributing to *corpus delicti*, it also identifies all implicated in encouraging of aiding a suicide attempt.

Keywords: special knowledge, computer expertise, computer-technical expertise, assistance in committing suicide, inducement to commit suicide, computer information research

Citation: Ermoshkin D. A. Computer Expertise in Criminal Investigation: Crimes Related to Promoting or Aiding Suicide. *Vestnik Kemerovskogo gosudarstvennogo universiteta. Seriia: Gumanitarnye i obshchestvennye nauki*, 2025, 9(4): 615–623. (In Russ.) https://doi.org/10.21603/2542-1840-2025-9-4-615-623

Received 23 Sep 2025. Accepted after review 15 Oct 2025. Accepted for publication 15 Oct 2025.

Введение

Повсеместно на территории Российской Федерации продолжается тенденция роста киберпреступлений. Так, по данным ГИАЦ МВД России, в 2024 г. зарегистрировано 765365 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 13,1 % больше, чем в 2023 г.[1] Почти половина таких преступлений (48,2 %) относится к категориям тяжких и особо тяжких (369267). Четыре преступления из пяти (84,8 %) совершаются с использованием сети Интернет (649064), больше половины (59,8 %) – с использованием средств мобильной связи или компьютерной техники (388382)[2]. В свою очередь, набольшее число преступлений с использованием информационно-телекоммуникационных технологий совершено в сфере экономики (486281). Однако не исключаются и иные составы преступлений, предусмотренные Уголовным кодексом Российской Федерации (УК РФ).

В виду повсеместного использования в обществе новых форм коммуникации, предполагающих мгновенную передачу сообщений между двумя и более сторонами через сеть Интернет, посредством социальных сетей или систем мгновенного обмена сообщениями (далее – мессенджеры), вполне логичен переход механизма совершения преступлений некоторых составов из реального в виртуальный мир.

Наибольший интерес с точки зрения интеграции информационно-телекоммуникационных технологий (ИТТ) в механизм совершения преступления представляют общественно опасные деяния, совершенные против жизни и здоровья. Так, в 2017 г. в 16 главу УК РФ были внесены следующие изменения: добавлена часть 2 в ст. 110 УК РФ; включены 2 самостоятельные статьи: 110.1, 110.2 УК РФ[3]. Каждая из трех норм предусматривает в качестве квалифицирующего признака побуждение к совершению самоубийства в информационно-телекоммуникационных сетях (ИТС) (включая сеть Интернет) [1–2].

Значительную сложность в расследовании представляют общественно опасные деяния, выраженные в склонении человека к самоубийству или содействии совершению самоубийства (ст. 110.1. УК РФ). Данный факт обусловлен трудностью выявления такого рода преступлений, поскольку отраженные в рассматриваемом составе способы склонения и содействия носят латентный характер воздействия на человека, нежели в смежных составах [3, с. 39]. Также дополнительные проблемы вызывает выявление и последующее расследование фактов склонения к самоубийству в ИТС, поскольку основной объем доказательственной информации содержится в виртуальной среде. Как справедливо указывают в МВД России, до 60 % киберпреступлений являются латентными[4].

Еще одним негативным аспектом, усложняющим процесс расследования преступлений, выступают действия, оказываемые как со стороны злоумышленника, склоняющего к самоубийству, так и со стороны жертвы, пытающейся скрыть факт психологического воздействия на нее. Действия

[1] Состояние преступности в России за январь-декабрь 2024 года. МВД России ФКУ «Главный информационно – аналитический центр», 2025. С. 28. URL: https://portal.tpu.ru/SHARED/n/NIKOLAENKOVS/student/risk_management/Sbornik_UOS_2024.pdf (дата обращения: 10.08.2025).

[2] Там же. С. 29–30.

[3] О внесении изменений в Уголовный кодекс РФ. ФЗ № 248-ФЗ от 29.07.2017. *СПС КонсультантПлюс*.

[4] Комплексный анализ состояния преступности в Российской Федерации по итогам 2024 года и ожидаемые тенденции ее развития. ФГКУ «ВНИИ МВД России», 2025. С. 54–55. URL: https://mvd.ru/upload/site163/folder_page/007/886/399/Kompleksnyy_analiz_-_2024.pdf (дата обращения: 10.08.2025).

злоумышленников, направленные на сокрытие совершения преступлений, досконально продуманы и в случае их реализации могут привести к полному уничтожению криминалистически значимой информации. Так, из приговора Татарского районного суда Новосибирской области по обвинению Б. в совершении деяния, предусмотренного пунктами «а», «г», «д» ч. 3 ст. 110.1 УК РФ, следует, что обвиняемый, склоняя несовершеннолетнего Л. к совершению самоубийства, требовал от последнего ежедневного удаления переписки из социальной сети ВКонтакте[5]. Что же касается противодействия, оказываемого со стороны потерпевшего, то в контексте рассматриваемого состава данный факт объясняется характеристикой личности жертв склонения к самоубийству, которыми в большинстве случаев являются несовершеннолетние [4] в возрасте 12–17 лет [5]. Несовершеннолетние потерпевшие, опасаясь наказания со стороны родителей или опекунов, удаляют всю переписку, в которой злоумышленник склоняет суицидента к совершению самоубийства. Тем самым они уничтожают данные, имеющие отношение к раскрытию и расследованию преступления, что, в свою очередь, выступает фактором, затрудняющим процесс расследования.

Очевидным негативным фактором, влияющим на количество и качество полученных в ходе предварительного следствия доказательств, свидетельствующих о побуждении к совершению самоубийства в ИТС, является отсутствие у соответствующих должностных лиц, осуществляющих расследование преступлений, специальных знаний в области исследования компьютерной (цифровой) информации.

Цель исследования – провести комплексный анализ возможностей применения специальных знаний в сфере исследования компьютерной информации при расследовании преступлений, предусмотренных статьей 110.1 Уголовного кодекса Российской Федерации (склонение к совершению самоубийства или содействие совершению самоубийства).

Результаты

В процессе расследования преступлений, связанных со склонением к самоубийству или содействием совершению самоубийства с использованием ИТТ, особенности применения специальных знаний обусловлены необходимостью получения полного доступа к переписке между жертвой и злоумышленником в социальных сетях и мессенджерах. В данном случае нельзя не согласиться с позицией Е. Р. Россинской и Т. А. Саакова о необходимости участия специалиста в следственных действиях, предполагающих изъятие цифровой информации или объектов, являющихся носителями подобного рода информации (ПК, мобильного телефона, электронного планшета и т.д.) [6, с. 111].

Привлечение сведущих лиц в рассматриваемой области научных знаний позволит обнаружить на цифровых устройствах, имеющих отношение к раскрытию и расследованию преступлений, следующую криминалистически значимую информацию:

1. О личности подозреваемого, склонявшего жертву к совершению самоубийства или оказывающего содействие совершению самоубийства.

2. О личности жертвы, в отношении которой предпринимались действия, направленные на склонение к совершению самоубийства, или действия, выраженные в содействии совершению самоубийства.

3. Информацию, подтверждающую факт склонения лица к самоубийству или содействия совершению самоубийства.

Склонение к совершению самоубийства в ИТС выражается в умышленном воздействии на сознание и волю лица с целью формирования у него осознанного намерения причинить себе смерть [7, с. 64], осуществляемого посредством переписки или пересылки текстов, видео- и аудиофайлов суицидальной направленности. В свою очередь, содействие совершению самоубийства в сети Интернет обусловлено оказанием помощи лицу, уже имеющему устойчивое намерение совершить самоубийство, выраженной в советах, указаниях, предоставлении информации, средств и орудий совершения самоубийства, либо устранением препятствий к его совершению или обещанием скрыть средства и орудия совершения самоубийства. При этом перечисленные способы содействия должны осуществляться путем взаимодействия злоумышленника с жертвой посредством ИТС.

Нельзя не согласиться с рядом исследователей [8; 9], обоснованно выделяющих две формы привлечения сведущих лиц, обладающих специальными знаниями в области исследования компьютерной информации, к расследованию преступлений: непроцессуальная и процессуальная.

Непроцессуальная форма реализуется посредством привлечения специалиста (эксперта) к участию в таких оперативно-розыскных мероприятиях, как исследование предметов и документов [10] (например, компьютерное исследование мобильного телефона жертвы) или получение компьютерной информации (например, получение оперативно значимой информации из телефона волонтера организации по выявлению в сети Интернет групп суицидальной направленности).

[5] Приговор Татарского районного суда Новосибирской области от 10.02.2018 по уголовному делу № 1-46/2018.

BULLETIN
KEMEROVO STATE UNIVERSITY
SERIES: HUMANITIES AND SOCIAL SCIENCES

К форме непроцессуального участия также можно отнести доэкспертную оценку материалов уголовного дела[6], которая проводится в целях тщательного отбора объектов, имеющих значение для процесса доказывания, предоставления необходимого и достаточного объема материалов, направляемых для проведения экспертизы, а также правильной формулировки вопросов, которые необходимо будет решить эксперту[7]. Такая оценка может осуществляться в виде консультативного взаимодействия следователя с экспертом или в ходе производства отдельных следственных действий.

В свою очередь, **процессуальная форма** заключается в привлечении сведущего лица в качестве эксперта или специалиста непосредственно к участию в производстве следственных действий. Так, эксперт в области исследования компьютерной информации может быть привлечен в качестве специалиста к участию в обыске, осмотре места происшествия или осмотре предметов, вещей и документов. Наиболее частым вариантом процессуальной формы привлечения эксперта к расследованию преступлений является назначение судебной компьютерной (компьютерно-технической) экспертизы.

Привлечение специалиста (эксперта) в области исследования компьютерной информации целесообразно осуществлять еще на этапе рассмотрения материала проверки по факту побуждения к совершению самоубийства. Данный факт обусловлен двумя основными причинами. Во-первых, следователю или сотруднику органа дознания, осуществляющему рассмотрение материала проверки, необходимо установить наличие достаточных данных, указывающих на признаки состава преступления, что в большинстве случаев представляется возможным благодаря получению из телефона жертвы криминалистически значимой информации, свидетельствующей о склонении к самоубийству или содействии совершению самоубийства. Во-вторых, на рассматриваемом этапе установить личность злоумышленника путем применения специальных знаний гораздо проще, поскольку преступник может быть еще не осведомлен о факте выявления правоохранительными органами общественно опасного деяния. Если в первом случае очевидно применение специальных знаний сотрудниками экспертно-криминалистических подразделений, то для решения вопроса об установлении личности злоумышленника наиболее целесообразным видится привлечение сотрудников отделов специальных технических мероприятий, деятельность которых, помимо прочего, направлена на борьбу с преступностью в ИТС.

В целях выявления лица, склоняющего к самоубийству или содействующего совершению самоубийства, возможно применение методов OSINT-технологий (Open Source Intelligence – разведка по открытым данным [11; 12]). Принцип работы OSINT заключается в поиске, сборе и анализе информации, находящейся в открытых источниках сети Интернет [13; 14, с. 63]. Исследование и развитие OSINT-методов является перспективным направлением в работах как зарубежных, так и отечественных ученых [15–23]. Благодаря OSINT-инструментам, имеющимся в распоряжении правоохранительных органов, за считанные часы можно установить информацию о личности злоумышленника, даже в том случае, когда для совершения общественно опасных деяний используются сфальсифицированные аккаунты в социальных сетях или мессенджерах. Нередко OSINT-инструментами пользуются для установления личности потерпевших. Так, в ходе осмотра мобильного устройства жертвы или злоумышленника велика вероятность выявления чатов или групп суицидальной направленности, в которых осуществлялось склонение к совершению самоубийства. Сотрудниками следствия должны быть предприняты безотлагательные меры по выявлению всех участников данных чатов или виртуальных сообществ. Самым действенным способом решения такой задачи является направление соответствующего поручения сотрудникам подразделений специальных технических мероприятий оперативного блока правоохранительных органов, которые посредством OSINT-анализа могут установить участников, интересующих следствие чатов или групп в социальных сетях и мессенджерах. К сожалению, информация, полученная с помощью OSINT, не может являться доказательством по уголовному делу, поскольку, на наш взгляд, не соответствует критерию допустимости.

Не стоит пренебрегать привлечением специалиста в области исследования компьютерной информации на этапе изъятия соответствующей техники. Данный факт обусловлен необходимостью преодоления противодействия процессу расследования, которое может заключаться в мгновенном уничтожении компьютерной информации, в том числе дистанционными методами (например, при выключении

[6] Информационное письмо «О вопросах применения норм уголовно-процессуального законодательства Российской Федерации, регламентирующих порядок назначения судебных экспертиз». Генеральная прокуратура Российской Федерации, 2023.

[7] Методические (практические) рекомендации по осмотру и изъятию электронных носителей информации в целях доэкспертной оценки материалов и целесообразности назначения судебной компьютерной экспертизы. ЭКЦ МВД России, 2024. С. 1–3.

 https://doi.org/10.21603/2542-1840-2025-9-4-615-623

устройства или при повторном его подключении к сети Интернет в ходе его осмотра). Поэтому для защиты от нежелательного удаления информации обязательным условием является не только блокирование любой возможности подключения компьютера или мобильного устройства к сети Интернет, но и соответствующая упаковка устройств или копирование образа операционной системы.

Негативно повлиять на ход дальнейшего исследования компьютерной информации также может выключение устройства перед его изъятием [24, с. 55]. Существует вероятность удаления несохраненных данных, например истории браузера или сообщений мессенджера с отключенной настройкой сохранения. Кроме того, при включении устройства установленные программы могут потребовать авторизации для доступа к данным. В случае если изъятию подлежит компьютер с загруженной оперативной системой и имеются основания полагать, что часть данных может быть зашифрована, перед отключением устройства необходимо создать копию образа оперативной памяти для дальнейшего анализа[8].

Зачастую перед изъятием персональных компьютеров или мобильных устройств сотрудники подразделений предварительного расследования, проводящие обыск, осуществляют сброс паролей учетных записей в целях возможности в дальнейшем (например, в ходе осмотра предметов) получить беспрепятственный доступ к памяти изъятого устройства. Однако сброс пароля может привести к невозможности восстановления доступа к данным, которые привязаны к учетной записи. Например, большинство браузеров (Chrome, Яндекс. Браузер, Firefox) при изменении пароля не отображают список сохраненных учетных данных пользователя для ресурсов Сети.

При производстве отдельных следственных действий, таких как осмотр места происшествия, обыск или осмотр предметов, с участием специалиста в области исследования электронных носителей информации возможно частичное извлечение и просмотр данных, содержащихся на интересующих устройствах. В качестве примера можно привести приговор Ленинского районного суда г. Тюмени по обвинению Я. в совершении преступления, предусмотренного пунктами «а», «в», «д» ч. 3 ст. 110.1 УК РФ[9], где указано, что в ходе осмотра мобильного телефона обвиняемого производилось извлечение информации с помощью аппаратно-программного комплекса "UFED Touch 2"[10]. Среди информации, извлеченной с мобильного телефона, принадлежащего Я., имелось:

- папка "Instagram"[11], в которой содержатся различные диалоги, связанные с обсуждением поиска «кураторов»;
- папка "Viber", в которой расположена переписка с контактом «Мама», где данный контакт интересуется о переписках дочери в группах суицидальной направленности;
- папка "WhatsApp", где содержится переписка из диалога «Некое», в котором обвиняемый Я. склонял несовершеннолетних к совершению самоубийства.

Несмотря на наличие положительного опыта извлечения с устройств злоумышленников информации, интересующей следствие, необходимо понимать, что в ходе проведения перечисленных следственных действий отсутствует реальная возможность получения всех данных, имеющихся на цифровом устройстве. Например, восстановление удаленных файлов в большинстве случаев возможно только на этапе производства судебной экспертизы, поскольку требуется снятие физического образа[12] накопителя данных, установленного в устройстве, что занимает значительный период времени (от 5 часов) [25]. Извлечение информации из цифровых устройств (непосредственно перед их изъятием) должно носить исключительно характер оперативного получения криминалистически значимой информации и ни в коем случае не должно подменять производство судебной компьютерной (компьютерно-технической) экспертизы.

Процессуальный порядок назначения судебных экспертиз отражен в ст. 95 Уголовно-процессуального кодекса Российской Федерации. Что касается назначения судебных компьютерных (компьютерно-технических) экспертиз, как уже было отмечено ранее, немаловажную роль играет доэкспертная оценка материалов уголовного дела, которая, в первую очередь, направлена на конкретизацию вопросов, выносимых на разрешение эксперта.

[8] Там же. С. 5–6.

[9] Приговор Ленинского районного суда г. Тюмени от 26.11.2020 по уголовному делу № 1-1299/2020.

[10] Переносной автономный аппаратно-программный комплекс для копирования (съема) информации вне лаборатории из мобильных и иных «умных» устройств связи.

[11] Компания *Meta Platforms*, владеющая социальными сетями *Facebook* и *Instagram* и онлайн-мессенджером *WhatsApp*, признана экстремистской организацией, ее деятельность запрещена на территории РФ. *Meta Platforms, the parent company of Facebook, Instagram and WhatsApp Messenger, is banned in the Russian Federation as an extremist organization.*

[12] Точная посекторная копия образа или дампа памяти.

BULLETIN
KEMEROVO STATE UNIVERSITY
SERIES: HUMANITIES AND SOCIAL SCIENCES

Типичными объектами компьютерной экспертизы, назначаемой в рамках расследования преступлений, предусмотренных п. «д» ч. 3 ст. 110.1 УК РФ, являются:

1. Мобильные устройства (смартфоны, планшеты и др.) и персональные компьютеры, принадлежащие жертве преступления – лицу, которое склоняли к совершению самоубийства или которому содействовали в совершении самоубийства.

2. Мобильные устройства (смартфоны, планшеты и др.) и персональные компьютеры, принадлежащие злоумышленнику – лицу, которое склоняло к самоубийству или содействовало совершению самоубийства.

3. Мобильные устройства (смартфоны, планшеты и др.) и персональные компьютеры, принадлежащие лицам, признанным свидетелями по уголовному делу. В данном случае к таковым могут относиться близкие родственники или лица из ближайшего круга общения жертвы или злоумышленника, с которыми велась (или могла вестись) переписка об обстоятельствах расследуемого события.

В рамках производства судебной компьютерной (компьютерно-технической) экспертизы по уголовным делам, связанным со склонением к самоубийству или содействием совершению самоубийства, с перечисленных выше устройств можно извлечь следующую информацию:

1. Переписки между злоумышленником и жертвой (или жертвами) в социальных сетях или мессенджерах. Следственная и судебная практика свидетельствует, что наиболее частыми мессенджерами, используемыми для склонения к совершению самоубийства, являются Telegram или WhatsApp, наиболее распространенной социальной сетью – ВКонтакте [26, с. 13]. Однако могут встречаться случаи переписки посредством SMS-сообщений.

2. Видео-, фото-, аудиофайлы, которые могли быть использованы для склонения к совершению самоубийства или содействия совершению самоубийства, а также указывающие на популяризацию самоубийства. В следственной практике имеют место случаи, когда обвиняемые в склонении к совершению самоубийства, выбрав в качестве способа реализации преступного умысла геймифицированную форму психологического воздействия [27, с. 35], заключающуюся в выполнении заданий, заставляли жертв просматривать видеозаписи суицидального характера длительностью более 23 часов. Нередко подобные видеозаписи изготавливались непосредственно злоумышленниками.

3. История запросов и посещаемых сайтов в интернет-браузерах. Данный вид информации интересен предварительному следствию в нескольких аспектах. Во-первых, злоумышленник в целях формирования более успешного механизма совершения преступления, выраженного в склонении к совершению самоубийства, мог осуществлять поиск информации, размещенной в открытом доступе в сети Интернет, описывающей наиболее эффективные способы психологического воздействия на потенциальных жертв. Во-вторых, подозреваемый мог осуществлять поиск контента суицидальной направленности в целях его демонстрации жертвам для усиления механизма психологического воздействия. В-третьих, посредством анализа истории интернет-запросов можно проследить, какими мессенджерами и социальными сетями пользовался злоумышленник в целях реализации преступного умысла. В-четвертых, по результатам исследования истории запросов интернет-браузеров следователь может более детально изучить личность как обвиняемого в склонении к самоубийству, так и жертвы, в том числе детали личности рассматриваемых участников уголовного судопроизводства, о которых те могут утаивать. Данный перечень криминалистически значимой информации, которую можно получить благодаря извлечению из исследуемых устройств журнала поиска интернет-браузеров, не является исчерпывающим.

4. Журнал входящих и исходящих звонков мобильного телефона или мессенджеров, установленных на мобильных устройствах. Имеют место случаи, когда злоумышленники в комплексе со склонением лиц к совершению самоубийства путем переписки в социальных сетях или мессенджерах используют методы воздействия на жертву, основанные на непосредственном внушении суицидальных мыслей путем голосового общения в реальном времени, т. е. посредством телефонных переговоров. Так, из показаний несовершеннолетнего потерпевшего Л. следует, что «куратор» звонил ему примерно раз в два-три дня, в 2–3 часа ночи[13].

5. Наличие связи между аккаунтами в социальных сетях или мессенджерах на исследуемых устройствах, а также с другими пользователями социальных сетей или мессенджеров. Данный вид получаемой информации, в первую очередь, облегчает поиск переписок между аккаунтами, используемыми подозреваемым, и аккаунтами иных лиц, в том числе состоящими в одном диалоге (или группе). Так, следователь, получив «образ» памяти исследуемого мобильного телефона, с помощью специального программного обеспечения, которое является общедоступным для правоохранительных органов, может проследить связи, выраженные

[13] Приговор Татарского районного суда Новосибирской области от 10.02.2018 по уголовному делу № 1-46/2018.

 https://doi.org/10.21603/2542-1840-2025-9-4-615-623

в переписках, между злоумышленником и различными группами (диалогами) в социальных сетях или мессенджерах, в том числе с другими аккаунтами. Преимуществом извлечения данной информации является:

- возможность установления соучастников совершенного преступления и определения формы соучастия;
- возможность установления иных жертв общественно опасного деяния, выразившегося в склонении к совершению самоубийства;
- возможность установления иных так называемых групп смерти, о которых ранее не было известно следствию.

Полученная по результатам производства компьютерной (компьютерно-технической) экспертизы информация обязательно должна пройти как индивидуальную оценку на соответствие критериям относимости, допустимости и достоверности, так и в комплексе с иными доказательствами по уголовному делу оценку на предмет достаточности.

Заключение

Выделим ряд основных тактических рекомендаций привлечения специалистов в рассматриваемой области науки и техники, способствующих эффективному расследованию преступлений, связанных со склонением к самоубийству или содействием совершению самоубийства.

Во-первых, привлечение специалистов (экспертов) в сфере изучения цифровой информации необходимо осуществлять еще на этапе рассмотрения материала проверки по факту побуждения к совершению самоубийства. Данный факт обусловлен оказываемым со стороны злоумышленника противодействием расследованию, которое может выражаться в уничтожении криминалистически значимой информации.

Во-вторых, применение специальных знаний в области исследования компьютерной информации не всегда связано с привлечением к расследованию сотрудников экспертно-криминалистических подразделений. Существенную помощь в расследовании преступлений, сопряженных с использованием информационно-телекоммуникационных технологий, могут оказать специалисты подразделений специальных технических мероприятий.

В-третьих, не стоит пренебрегать доэкспертной оценкой материалов уголовного дела, направляемых на компьютерное (компьютерно-техническое) экспертное исследование. Такой вид непроцессуального участия специалиста (эксперта) существенно упростит применение специальных знаний на последующих этапах расследования преступления.

Конфликт интересов: Автор заявил об отсутствии потенциальных конфликтов интересов в отношении исследования, авторства и / или публикации данной статьи.
Conflict of interests: The author declared no potential conflict of interests regarding the research, authorship, and / or publication of this article.

Литература / References

1. Сидорова Е. З. К вопросу разграничения смежных составов преступлений, связанных с побуждением к совершению самоубийства. *Век качества*. 2021. № 1. С. 140–152. [Sidorova E. Z. On the question of delimitation of the adjacent structures of the crimes connected with inducement to suicide commission. *Age of Quality*, 2021, (1): 140–152. (In Russ.)] https://elibrary.ru/ejfkns
2. Ильин Н. Н. Вопросы квалификации и расследования доведения до самоубийства несовершеннолетних с помощью сети Интернет. М.: Московская академия Следственного комитета, 2022. 88 с. [Ilyin N. N. *Issues of qualification and investigation of driving minors to suicide using the Internet*. Moscow: Moscow Academy of the Investigative Committee, 2022, 88. (In Russ.)] https://elibrary.ru/phqtyc
3. Сергеев К. А. Уголовно-правовые и процессуальные особенности расследования преступлений, предусмотренных ст. 110, 110. 1 УК РФ. *Вестник Южно-Уральского государственного университета. Серия: Право*. 2020. Т. 20. № 2. С. 37–41. [Sergeev K. A. Criminal law and procedural features of the investigation of the investigation of the offenses under articles 110, 110.1 of the Criminal Code of the Russian Federation. *Bulletin of the South Ural State University. Series: Law*, 2020, 20(2): 37–41. (In Russ.)] https://doi.org/10.14529/law200206
4. Биткова А. А. Криминалистическая характеристика жертв доведения до самоубийства и склонения к его совершению. *Молодежь, наука и цивилизация*: Междунар. студ. науч. конф. (Красноярск, 19 мая 2022 г.) Красноярск: СибЮИ МВД России, 2022. С. 476–479. [Bitkova A. A. Forensic characteristics of victims of suicide aid and promotion. *Youth, science, and civilization*: Proc. Intern. Stud. Sci. Conf., Krasnoyarsk, 19 May 2022. Krasnoyarsk: SibLI MVD of Russia, 2022, 476–479. (In Russ.)] https://doi.org/10.51980/978-5-7889-0327-9_2022_23_13_476

5. Лемешев К. А. Характеристика несовершеннолетних потерпевших при доведении до самоубийства. *Научные междисциплинарные исследования*. 2020. № 8-2. [Lemeshev K. A. Characteristics of minor victims when driving to suicide. *Scientific Interdisciplinary Research*, 2020, (8-2). (In Russ.)] URL: https://cyberleninka.ru/article/n/harakteristika-nesovershennoletnih-poterpevshih-pri-dovedenii-do-samoubiystva (дата обращения: 10.08.2025).
6. Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров. *Криминалистика: вчера, сегодня, завтра*. 2020. № 3. С. 106–123. [Rossinskaya E. R., Saakov T. A. The problems of collecting digital footprints of crimes in social networks and messengers. *Forensics: Yesterday, today, tomorrow*, 2020, (3): 106–123. (In Russ.)] https://doi.org/10.24411/2587-9820-2020-10060
7. Филиппова С. В. Склонение к совершению самоубийства или содействие совершению самоубийства: уголовно-правовая характеристика и проблемы квалификации: дис. ... канд. юрид. наук. М., 2020. 209 с. [Filippova S. V. *Suicide aid or promotion: Criminal law characteristics and qualification issues*. Cand. Law. Sci. Diss. Moscow, 2020, 209. (In Russ.)]
8. Епифанов А. Е. Участие специалиста в следственных и процессуальных действиях (аспекты уголовного судопроизводства). *Правовое государство: теория и практика*. 2025. № 2. С. 68–74. [Epifanov A. E. Specialist participation in investigative and procedural actions (aspects of criminal proceedings). *The Rule-of-Law State: Theory and Practice*, 2025, (2): 68–74. (In Russ.)] https://doi.org/10.33184/pravgos-2025.2.8
9. Дьяконова О. Г. Формы участия специалиста в судопроизводстве. *Вестник Университета имени О. Е. Кутафина (МГЮА)*. 2016. № 8. С. 15–31. [Dyakonova O. G. Forms of specialist participation in the proceedings. *Courier of the Kutafin Moscow State Law University (MSAL)*, 2016, (8): 15–31. (In Russ.)] https://elibrary.ru/xrfrbl
10. Казиев З. Г. Формы и содержание содействия специалистов в проведении оперативно-розыскных мероприятий. *Вестник Института законодательства Республики Казахстан*. 2008. № 3. С. 65–68. [Kaziev Z. G. Forms and content of expert assistance in investigation activities. *Vestnik Instituta zakonodatelstva Respubliki Kazahstan,* 2008, (3): 65–68. (In Russ.)] https://elibrary.ru/ywmsap
11. Glassman M., Kang M. J. Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, 2012, 28(2): 673–682. https://doi.org/10.1016/j.chb.2011.11.014
12. Ромачев Р. В., Стригунов К. С., Го Ф. Политика аутсорсинга разведывательных услуг в США. *Международная жизнь*. 2022. № 6. С. 58–65. [Romachev R. V., Strigunov K. S., Go F. Policy of outsourcing intelligence services in the USA. *Mezdunarodnaa zizn'*, 2022, (6): 58–65. (In Russ.)] https://elibrary.ru/vrwwdz
13. Vaughan A. The role of OSINT in criminal investigations: Leveraging open-source data to combat cybercrime and organized criminal activities. *Cybersecurity Undergraduate Research Showcase*, 2024, 10. https://doi.org/10.25776/bvp5-c844
14. Иванов В. Ю. Использование OSINT в раскрытии и расследовании преступлений. *Вестник Уральского юридического института МВД России*. 2023. № 1. С. 62–66. [Ivanov V. Yu. Using OSINT in detecting and investigation crimes. *Bulletin of the Ural Law Institute of the Ministry of the Interior of Russia*, 2023, (1): 62–66. (In Russ.)] https://elibrary.ru/vpimwc
15. Дворянкин О. А. OSINT, Pentest и Нетсталкинг – информационные технологии интернета. *Национальная ассоциация ученых*. 2022. № 84-2. С. 6–13. [Dvoryankin O. A. OSINT, Pentest and Netstalking – Internet information technologies. *Nacionalnaja associacija uchenyh*, 2022, (84-2): 6–13. (In Russ.)] https://elibrary.ru/lqlpwz
16. Луговик В. Ф. Преемственность и новации в оперативно-розыскной науке. *Актуальные проблемы борьбы с преступлениями и иными правонарушениями*. 2006. № 6. С. 52–54. [Lugovik V. F. Continuity and innovations in operational-search science. *Aktualnye problemy borby s prestuplenijami i inymi pravonarushenijami*, 2006, (6): 52–54. (In Russ.)] https://elibrary.ru/ylamsm
17. Афонькин Г. П., Смирнов Е. В., Чемерчев Д. В. Основы противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий. *Полицейский вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации*. 2021. № 1. С. 10–17. [Afonkin G. P., Smirnov E. V., Chemerchev D. V. Fundamentals of countering crimes committed using information and telecommunication technologies. *The basics of countering crimes committees u sing information and telecommunication technologies*, 2021, (1): 10–17. (In Russ.)] https://elibrary.ru/gjddrd

18. Бельдеубаева Д. Р. Применение OSINT технологий в качестве повышения эффективности деятельности органов внутренних дел. *Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем*: Всерос. науч.-практ. конф. (Воронеж, 11 июня 2020 г.) Воронеж: ВИ МВД России, 2020. С. 160–161. [Beldeubaeva D. R. OSINT technologies as a means of improving the efficiency of internal affairs bodies. *Current issues of operation of security systems and protected telecommunication systems*: Proc. All-Russian Sci.-Prac. Conf., Voronezh, 11 Jun 2020. Voronezh: VI of the MIA of Russia, 2020, 160–161. (In Russ.)] https://elibrary.ru/nheoxa
19. Van Puyvelde D., Tabárez Rienzi F. The rise of open-source intelligence. *European Journal of International Security*, 2025, 1–15. https://doi.org/10.1017/eis.2024.61
20. Galan J. J., Carrasco R. A., Latorre A. Military applications of machine learning: A bibliometric perspective. *Mathematics*, 2022, 10(9). https://doi.org/10.3390/math10091397
21. Szymoniak S., Foks K. Open Source Intelligence opportunities and challenges: A review. *Advances in Science and Technology Research Journal*, 2024, 18(3): 123–139. https://doi.org/10.12913/22998624/186036
22. Avrahami Z., Zwilling M., Hajaj C. Leveraging OSINT for advanced proactive cybersecurity: Strategies and solutions. *IEEE Access*, 2025, 154229–154250. https://doi.org/10.1109/ACCESS.2025.3603868
23. Батоев В. Б. О технологии поиска по открытым источникам "OSINT" в оперативно-розыскной деятельности. *Вестник Уфимского юридического института МВД России*. 2023. № 2. С. 66–71. [Batoev V. B. On the Open Source search technology "OSINT" in operational investigative activities. *Bulletin of Ufa Law Institute of MIA of Russia*, 2023, (2): 66–71. (In Russ.)] https://elibrary.ru/hthorh
24. Семенов А. Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации. *Сибирский юридический вестник*. 2004. № 1. С. 53–55. [Semenov A. Yu. Some aspects of detection, seizure, and examination of traces arising during the commission of crimes in the field of computer information. *Siberian Law Herald*, 2004, (1): 53–55. (In Russ.)] https://elibrary.ru/piegnn
25. Кувычков С. И. О современных проблемах проведения судебно-компьютерных экспертиз в ходе предварительного расследования. *Юридическая наука и практика: Вестник Нижегородской академии МВД России*. 2016. № 2. С. 293–298. [Kuvychkov S. I. About modern problems of the forensic computer examinations during the preliminary investigation. *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2016, (2): 293–298. (In Russ.)] https://elibrary.ru/wcmdkp
26. Коновалова К. В., Суренская М. С. Доказательства из мессенджеров в работе следователя. *Слово в науке*. 2022. № 10. С. 12–17. [Konovalova K. V., Surenskaya M. S. Evidence from messengers in crime investigation. *Word in Science*, 2022, (10): 12–17. (In Russ.)] https://elibrary.ru/yjwufx
27. Авешникова А. А. Об уголовной ответственности за склонение несовершеннолетних к самоубийству. *Российский следователь*. 2019. № 1. С. 33–37. [Aveshnikova A. A. On the criminal liability for inducement of minors to suicide. *Russian Investigator*, 2019, (1): 33–37. (In Russ.)] https://elibrary.ru/ytxouh