ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 343.98:004

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ ПРОТИВ ПОЛОВОЙ НЕПРИКОСНОВЕННОСТИ ПРИ ПРИМЕНЕНИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Внуков Вячеслав Иванович,
доцент, кандидат юридических наук,
Волгоградский государственный университет,
г. Волгоград, Россия
vnukov@volsu.ru

Гаврилова Элеонора Дмитриевна,
студент, Волгоградский государственный университет,
г. Волгоград, Россия
spd-231_663337@volsu.ru

Аннотация

Авторы исследует актуальные проблемы расследования преступлений против половой неприкосновенности несовершеннолетних в цифровой среде. Отмечается концентрация доказательств в цифровой среде: в мессенджерах и закрытых интернет-сообществах, распространяющих деструктивный контент. Обуславливается необходимость применения комбинированного подхода, сочетающего судебно-речеведческие экспертизы и использование высокотехнологичными методами преодоления шифрования архивов, содержащих преступный контент. Подчеркиваются риски, связанные с изъятием доказательств в случае использования полно-дискового шифрования и иных методов защиты информации, указывается на необходимость разработки усовершенствованных криминалистических методик в целях повышения эффективности и безопасности изъятия цифровых следов.

Ключевые слова: цифровая криминалистика, преступления против половой неприкосновенности несовершеннолетних, шифрование данных, изъятие цифровых следов, хеш-сумма.

INVESTIGATION OF CRIMES AGAINST SEXUAL INTEGRITY IN THE USE OF INFORMATION TECHNOLOGY

Vnukov Vyacheslav Ivanovich,
Associate Professor, Candidate of Law, Volgograd State University,
Volgograd, Russia
vnukov@volsu.ru

Gavrilova Eleonora Dmitrievna,

student, Volgograd State University,
Volgograd, Russia
spd-231_663337@volsu.ru

ABSTRACT

The author explores the current problems of investigating crimes against the sexual integrity of minors in the digital environment. There is a concentration of evidence in the digital environment: in messengers and closed online communities that spread destructive content. There is a need for a combined approach combining forensic speech expertise and the use of high-tech methods to overcome encryption of archives containing criminal content. The author emphasizes the risks associated with the seizure of evidence in the case of using full-disk encryption and other methods of information protection. In conclusion, the author points out the need to develop improved forensic techniques in order to increase the efficiency and security of digital trace removal.

Keywords: digital forensics, crimes against the sexual integrity of minors, data encryption, digital trace removal, hash sum.

В связи с повсеместным распространением цифровых технологий в юридической литературе большое внимание уделяется различным аспектам совершенствования криминалистической техники и методики расследования преступлений, совершенных с использованием информационных технологий. Отмечается необходимость разработки и применения специальных криминалистических методов противодействия киберпреступлениям [1, с. 170]. Кроме того, в последнее время довольно распространенной в научной литературе является формулировка «цифровая» или «компьютерная» криминалистика [2, с. 276], выделение которой как раздела обуславливается необходимостью разработки новых способов анализа, сохранения, а также регистрации законодательства: к примеру, для определения сетевых протоколов, используемых преступником при совершении преступления в цифровой среде, а также выявления дополнительных способов шифрования, при котором IP-адрес посещаемой пользователем страницы либо остается скрытым от провайдера, либо «маскируется» под иные сервисы.

Безусловно, цифровой прорыв не только обуславливает возникновение отдельных видов киберпреступлений (например, кибермошенничество, DoS-атаки), но также способствует упрощению совершения и других преступлений, и отрицать необходимость совершенствования методов расследования преступлений в цифровой среде в целом – нецелесообразно. Именно поэтому в контексте настоящего исследования предлагается обратить внимание на некоторые проблемные аспекты расследования преступлений против половой неприкосновенности, совершаемых с использованием цифровых технологий.

На настоящий момент основной массив информации, необходимой для расследования предусмотренных ст. 133 и 135 УК РФ преступлений сконцентрирован в цифровой среде: социальных сетях и мессенджерах. Мессенджер «Telegram» сегодня является одним из крупнейших поставщиков так называемого треш-контента, направленного на негативное воздействие на психику несовершеннолетних. Несмотря на то, что службами поддержки так или иначе предоставлена возможность сообщить о наличии на странице деструктивного контента (кнопка «пожаловаться» с возможностью

указания причины и бот «Search Report»), с каждым днем возрастает количество закрытых каналов, члены которого оформляют доступ к «эксклюзивному» преступному контенту (в том числе, порнографическим материалам). Наиболее уязвимыми к подобному контенту являются несовершеннолетние, не всегда обладающие необходимыми навыками критического мышления для отграничения преступного от неприступного [3, с. 311], а также иногда воспринимающие деструктивное поведение как эталон вследствие неустойчивости и внушаемости психики.

Не исключено также использование информационных технологий не только в качестве непосредственного способа совершения преступлений, охватываемых главой 18 УК РФ, но и в целях подготовки к совершению преступлений: например, лицо вступает в переписку в несовершеннолетней, путем психологических манипуляций вступает с ней в доверительные отношения, затем отправляет порнографические материалы.

Полагаем, что одним из традиционных, но эффективных способов повышения эффективности расследования подобных преступлений является проведение судебно-речеведческих экспертиз (далее - СРЭ). В уголовном процессе под СРЭ подразумевают анализ продуктов речевой деятельности с целью установления фактов, имеющих значения для уголовного дела [4, с. 41], а список возможных вопросов, поставленных перед экспертом, не является исчерпывающим. Во многом именно поэтому применение данного вида экспертизы позволит установить, носили ли отправленные подозреваемым сообщения сексуальный подтекст, написаны ли сообщения развратного характера одним лицом: наличествуют ли типовые слова или «слова-маркеры», позволяющие установить авторство, определить общий стиль речи и способ построения предложений и. т. д. К примеру, это может быть актуальным в ситуациях, когда лицо отрицает свое авторство в отношении «развратных сообщений», отправленных им потерпевшей с «запасного» аккаунта, когда установить их авторство иными способами не представляется возможным. На наш взгляд, не следует недооценивать потенциал судебно-речеведческих экспертиз при расследовании данного вида преступлений, концентрируя внимание лишь на правильном и полном изъятии доказательств с компьютера подозреваемого: необходим комбинированный подход.

Между тем, технологическая сторона вопроса так или иначе продолжает играть важную роль при расследовании преступлений, предусмотренных ст. 135 УК РФ. Правоохранительные органы могут испытывать трудности с обеспечением правильного и полного изъятия материалов с электронных носителей информации и иных удаленных серверов, в связи с чем потребуется привлечение IT-специалиста, обеспечивающего грамотное изъятие или копирование оставленных лицом цифровых следов. Лицо может использовать различные способы шифрования с целью скрыть архивы во внутренней файловой системе, содержание порнографические материалы (в том числе, ранее полученные в связи с совершением им насильственных действий сексуального характера данные).

Например, применяется полно дисковое шифрование BitLocker, FileVault, с помощью программы VeraCrypt создается файл-контейнер – облачное хранилище, замаскированное под обычный файл, прочитать содержимое, которого сразу без пароля не представляется возможным, используются методы стенографии – внедрения текстового сообщения в аудио или видеофайлы. Технологически-сложные и многоуровневые способы шифрования данных могут быть незаметны для человека, не обладающего квалификацией в рассматриваемой сфере, именно поэтому проблема традиционно решается привлечением специалиста к участию в следственных действиях.

В случае, когда следственными органами изымается дамп оперативной памяти устройства - содержимое рабочей памяти одного процесса, ядра или всей операционной

системы, становится возможным извлечение ключа шифрования, необходимость же получения буквенно-цифровой комбинации пароля отпадает. Ключ шифрования, как правило, расположен в оперативной памяти компьютера, поэтому при его изъятии как электронного носителя информации следственным органам нельзя допустить безвозвратной потери информации, относимой к делу. Процесс изъятия устройства несет риски: к примеру, при механическом вскрытии корпуса при попытке изъятия устройства может сработать встроенный датчик, зачищающий критически важные данные.

Само изъятие может быть осуществлено путем подключения к компьютеру устройства с установленным программным обеспечением, направленным на захват физической памяти компьютера (например, Magnet RAM Capture). При принятии подобного решения на следователя ложится большая ответственность, поскольку данное действие может привести к полной потере всех возможных доказательств при срабатывании различных систем защиты: материнская плата компьютера фиксирует подачу питания на USB и блокирует доступ.

В контексте исследования довольно интересным также представляется способ холодной перезагрузки (Cold Boot Attack), заключающийся в изъятии физических данных с компьютера путем быстрого чередования выключения питания без использования средств операционной системы и последующее включение [5, с. 84]. Отмечается, что уже после включения производится сохранение текущего состояния оперативной памяти в файл. Применяя данный метод, криминалист должен быть уверен, что система не защищена TPM – специальным криптографическим модулем, обеспечивающим безопасность системы.

Кроме того, доступ к дампу памяти сам по себе позволяет определить, какие программы и документы открывал пользователь в последнее время. Получается, при проведении следственного действия тесно затрагивается право частной жизни лица. В данном случае подозреваемый, безусловно, может реализовывать свое процессуальное право на обжалование, но изучение данный вопрос находится в плоскости уголовного процесса.

Таким образом, использование каждого из указанных методов связано с риском утраты возможных доказательств. Задача криминалиста – предположить возможный способ защиты, обойти систему USB-защиты, используя, к примеру, средства, не вызывающие срабатывание защитных систем. В случае же установки на компьютере специальной защиты, изъятие представляется куда более рискованным и не всегда целесообразным.

Изъятие лишь части сведений также несет в себе определенные риски, связанные с подменой или повреждением файла в момент копирования. По данному вопросу отметим, что один из универсальных инструментов – расчет и указание хеш-суммы файла – так называемого цифрового идентификатора, использование которого позволяет проверить, тождественны ли изъятые данные тем, что находятся на устройстве (например, хеш-сумма будет кардинально отличаться в случае, если файл оказался поврежденным в процессе изъятия).

В контексте исследования, на наш взгляд, возникает проблема, связанная с соблюдением принципа процессуальной экономии в уголовно-процессуальной деятельности, под которым принято понимать необходимость рационального использования процессуальных средств и форм для быстрого разрешения дела [6, с. 65]. Неоднократно подтверждено, что при расследовании преступлений, совершенных с использованием информационных технологий необходимо приложить большой круг усилий, привлечь компетентных специалистов в IT-области.

Можно предположить, что при расследовании преступлений против половой неприкосновенности несовершеннолетних не совсем целесообразно изъятие электронных носителей информации (в большинстве случаев, связанных с рисками их полной потери),

особенно когда присутствуют иные доказательства, изобличающие виновного. Однако с каждым годом совершенствуются способы шифрования данных во внутренней системе устройств, используемые в процессе совершения различных преступлений. Игнорировать необходимость совершенствования доказательственного значения электронных носителей информации не следует. Требуется дальнейшая проработка криминалистической методики в сфере расследования цифровых преступлений в целом, и преступлений против половой неприкосновенности несовершеннолетних, в частности.

Список литературы:

1. Болтенкова Ю. В. Особенности расследования преступлений, совершаемых с использованием IT-технологий в сфере компьютерной информации // Поколение будущего: Взгляд молодых ученых – 2022: сборник научных статей 11-й Международной молодежной научной конференции, Курск, 10–11 ноября 2022 года. Том 2. – Курск: Юго-Западный государственный университет, 2022. – С 170–174. – EDN YZQBVM.
2. Саханова, Н. Т. Будущее цифровой криминалистики: новые методы расследования киберпреступлений / Н. Т. Саханова, А. Г. Жумагулов // Современные проблемы уголовного процесса: пути решения: Сборник материалов Международной научно-практической конференции, Уфа, 03–04 апреля 2025 года. – Уфа: Уфимский юридический институт Министерства внутренних дел Российской Федерации, 2025. – С. 276-281. – EDN VEMWCY.
3. Лебедева, В. С. Влияние социальных медиа на формирование преступного поведения несовершеннолетних / В. С. Лебедева // Вопросы российской юстиции. – 2024. – № 31. – С. 310-319. – EDN XVRERM.
4. Галяшина, Е. И. Феномен судебного речеведения: наука - экспертиза - обучение / Е. И. Галяшина // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2015. – № 12(16). – С. 38-44. – EDN VVRRZN.
5. Практическое применение атаки методом холодной перезагрузки / М. В. Тимофеев, В. И. Иванов, П. Г. Дудоладова, В. В. Борыш // Проблемы и перспективы развития России: Молодежный взгляд в будущее : Сборник научных статей Всероссийской научной конференции. В 4-х томах, Курск, 17–18 октября 2018 года / Ответственный редактор А.А. Горохов. Том 3. – Курск: Юго-Западный государственный университет, 2018. – С. 84-86. – EDN YNGSBF.
6. Смолин, А. Ю. Принцип процессуальной экономии в уголовном судопроизводстве / А. Ю. Смолин // Экономическая безопасность России: политические ориентиры, законодательные приоритеты, практика обеспечения: Вестник Нижегородской академии МВД России. – 2009. – № 1. – С. 62-66. – EDN LANBDV.

References:

1. Boltenkova Yu. V. Features of the investigation of crimes committed with the use of IT technologies in the field of computer information // Generation of the Future: The View of Young Scientists - 2022: collection of scientific articles of the 11th International Youth Scientific Conference, Kursk, November 10-11, 2022. Vol. 2. - Kursk: South-West State University, 2022. - Pp. 170-174. - EDN YZQBVM.

2. Sakhanova, N. T. The Future of Digital Forensics: New Methods of Investigating Cybercrimes / N. T. Sakhanova, A. G. Zhumagulov // Modern Problems of Criminal Procedure: Solutions: Collection of Materials of the International Scientific and Practical Conference, Ufa, April 3-4, 2025. - Ufa: Ufa Law Institute of the Ministry of Internal Affairs of the Russian Federation, 2025. - Pp. 276-281. – EDN VEMWCY.
3. Lebedeva, V. S. The Influence of Social Media on the Formation of Criminal Behavior of Minors / V. S. Lebedeva // Issues of Russian Justice. – 2024. – No. 31. – Pp. 310-319. – EDN XVRERM.
4. Galyashina, E. I. The Phenomenon of Forensic Speech Theory: Science - Expertise - Training / E. I. Galyashina // Bulletin of the O.E. Kutafin Moscow State Law University (MSAL). – 2015. – No. 12(16). – Pp. 38-44. – EDN VVRRZN.
5. Practical Application of the Cold Boot Attack / M. V. Timofeev, V. I. Ivanov, P. G. Dudoladova, V. V. Borysh // Problems and Prospects of Russia's Development: A Youth Look into the Future: Collection of Scientific Articles of the All-Russian Scientific Conference. In 4 volumes, Kursk, October 17–18, 2018 / Editor-in-Chief A. A. Gorokhov. Volume 3. - Kursk: Southwestern State University, 2018. - Pp. 84-86. - EDN YNGSBF.
6. Smolin, A. Yu. The Principle of Procedural Economy in Criminal Proceedings / A. Yu. Smolin // Economic Security of Russia: Political Guidelines, Legislative Priorities, Practice of Support: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. - 2009. - No. 1. - Pp. 62-66. - EDN LANBDV.