Научная статья
УДК 34
NIION: 2022-0089-4/25-355
MOSURED: 77/27-031-2025-04-355
EDN: https://elibrary.ru/RCJNVX

Одноразовые виртуальные машины: криминалистические вызовы в деятельности правоохранительных органов

Наталья Васильевна Михайленко[1], Алексей Александрович Москвичев[2], Артем Владимирович Рудин[3]
[1,3] Московский университет МВД России имени В.Я. Кикотя, Москва, Россия
[2] Московская академия Следственного комитета Российской Федерации имени А.Я. Сухарева, Москва, Россия, moskvichev@mail.ru
[1] natamvz@internet.ru
[3] avuniversity@mail.ru

Аннотация. Исследование посвящено проблемам цифровой криминалистики — расследованию преступлений с использованием одноразовых виртуальных машин (Disposable VM). На основе анализа технологий Windows Sandbox, Qubes OS DispVM выявлены криминалистические риски утраты доказательств из-за эфемерности данных. Разработаны тактико-методические рекомендации для следователей и экспертов, включающие алгоритмы изъятия оперативной памяти, анализ артефактов гипервизора и процессуальные модели фиксации доказательств.

Ключевые слова: одноразовые виртуальные машины, цифровая криминалистика, оперативная память, гипервизор
Для цитирования: Михайленко Н. В., Москвичев А. В., Рудин А. В. Одноразовые виртуальные машины: криминалистические вызовы в деятельности правоохранительных органов // Судебная экспертиза и исследования. 2025. № 4. С. 154–159.

Original article

Disposable virtual machines: criminalistic challenges in the activities of law enforcement agencies

Natalya V. Mikhaylenko[1], Alexei A. Moskvichev[2], Artem V. Rudin[3]
[1,3] Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Moscow, Russia
[2] Moscow Academy of the Investigative Committee of the Russian Federation named after A.Ya. Sukharev, Moscow, Russia, moskvichev@mail.ru
[1] natamvz@internet.ru
[3] avuniversity@mail.ru

Abstract. The research is devoted to the problems of digital forensics — the investigation of crimes using Disposable virtual machines. Based on the analysis of Windows Sandbox and Qubes OS DispVM technologies, the forensic risks of losing evidence due to the ephemerality of data have been identified. Tactical and methodological recommendations for investigators and experts have been developed, including algorithms for removing RAM, analyzing hypervisor artifacts, and procedural models for recording evidence.

Keywords: disposable virtual machines, digital forensics, RAM, hypervisor
For citation: Mikhaylenko N. V., Moskvichev A. A., Rudin A. V. Disposable virtual machines: criminalistic challenges in the activities of law enforcement agencies. Forensic science and research. 2025;(4):154–159. (In Russ.).

Цифровая криминалистика столкнулась с беспрецедентным вызовом: технологии одноразовых виртуальных машин (Disposable VM), такие как Windows Sandbox и Qubes OS [1] DispVM, создают условия для «бесследного» совершения преступлений. Их ключевая особенность — эфемерность: все данные существуют только в оперативной памяти во время сеанса работы и автоматически уничтожаются после закрытия приложения, не оставляя на диске следов, пригодных для традиционной компьютерной экспертизы.

По оценкам Europol и UNODC, 80–90 % сложных киберпреступлений (например, создание ботнетов, криптоджекинг, многоступенчатые атаки) используют виртуализацию для сокрытия следов, тестирования вредоносного ПО и управления инфраструктурой [2].

В отчетах Group-IB и Kaspersky Lab отмечается, что 58 % ботнетов (сетей зомби-устройств) развертываются через облачные ВМ (AWS, Azure), что позволяет преступникам быстро менять IP-адреса и юрисдикции [3].

Существующие методики расследования, ориентированные на анализ статичных носителей, неэффективны против этого вызова. Актуальность настоящего исследования обусловлена необходимостью разработки принципиально новых подходов к обнаружению, фиксации и исследованию цифровых следов в условиях эфемерных сред. Цель работы — создание комплексной криминалистической методики, интегрирующей технические, процессуальные и тактические решения для противодействия преступному использованию Disposable VM. Научная новизна подтверждается тремя аспектами: впервые систематизированы артефакты Disposable VM с привязкой к жизненному циклу среды; разработана модель процессуально допустимого дампа ОЗУ; предложены верифицированные на практике алгоритмы действий для следователей и экспертов.

Современная цифровая криминалистика столкнулась с принципиально новым вызовом — распространением технологий одноразовых виртуальных машин (Disposable VM). Эти среды, изначально разработанные для целей кибербезопасности, такие как Windows Sandbox в Windows 10/11 Pro/Enterprise или Disposable VM в Qubes OS, стали инструментом сокрытия преступной деятельности. Ключевая особенность Disposable VM — их эфемерность: все пользовательские данные существуют исключительно в оперативной памяти во время сеанса работы и автоматически уничтожаются при закрытии приложения. Например, после завершения сессии Windows Sandbox на хосте остаются лишь косвенные артефакты — записи в журнале событий (Event ID 1237, 1240), файлы Prefetch и ключи реестра в ветке HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization. Этих следов недостаточно для восстановления конкретных действий пользователя: невозможно доказать факт открытия вредоносного вложения или посещения ресурсов в даркнете. В случае Qubes OS ситуация сложнее: журналы в /var/log/qubes фиксируют создание DispVM, но не сохраняют их содержимое.

При проведении обыска это создает критические риски. Рассмотрим реальный случай: у подозреваемого изымают ноутбук с активным окном Qubes OS DispVM, где запущен Tor Browser. Если следователь дает поручение выключить устройство (руководствуясь ст. 164 УПК РФ о «сохранении доказательств»), оперативная память очищается, а вместе с ней безвозвратно исчезают история браузера, скачанные файлы, учетные данные сессии. Последующая экспертиза подтвердит лишь факт использования Qubes OS через конфиги в /etc/qubes, но не сможет установить содержание деятельности — как в деле по ст. 183 УК РФ, где отсутствие дампа ОЗУ привело к прекращению уголовного преследования. Статистика МВД РФ за 2024 г. показывает: 89 % дел, связанных с Disposable VM, закрываются из-за недостатка доказательств, при этом в 74 % случаев следователи не фиксируют состояние экрана перед выключением устройства.

Для преодоления этих проблем разработан алгоритм действий при обыске. Первый шаг — немедленная визуальная фиксация: фотографирование экрана с отображением активных окон виртуальных машин (например, «окно Qubes VM: anon-whonix с запущенным Tor Browser») и внесение в протокол точного описания: «Обнаружен интерфейс гипервизора VirtualBox с запущенной виртуальной машиной Ubuntu-Live».

Второй шаг — запрет на выключение питания и срочный вызов эксперта-криминалиста для снятия дампа оперативной памяти с помощью модуля Скаут ПО «Мобильный Криминалист Эксперт Плюс». Если эксперт недоступен, устройство изымается в работающем состоянии с автономным источником питания, что должно быть отражено в протоколе: «Ноутбук изъят включенным для сохранения данных ОЗУ».

Экспертный анализ требует новых подходов. При исследовании дампа ОЗУ ключевыми объектами становятся: процессы гипервизора (vmwp.exe для Windows Sandbox, xen для Qubes), фрагменты дискового кэша виртуальной машины, сетевые сокеты. Для Windows Sandbox критичны записи в системном журнале (Event Viewer > Журналы приложений > Microsoft-Windows-Hyper-V-Worker-Admin), где Event ID 1237 фиксирует создание VM. В Qubes OS доказательственное значение имеют логи в /var/log/qubes/vm-create.log, но они не содержат деталей сессии. Экспертная практика показывает: даже при обнаружении этих артефактов выводы должны отражать уровень достоверности. Например, «установлено» — при обнаружении в памяти процесса malware.exe внутри VM; «не исключается» — при совпадении времени создания DispVM и получения фишингового письма.

Для экспертов-криминалистов разработаны четкие уровни выводов при работе с артефактами Dis-

posable VM. Уровень 1 (прямые доказательства) применяется при обнаружении в дампе ОЗУ конкретных следов деятельности: например, процесса браузера с установленным соединением на IP-адрес сервера злоумышленников или фрагментов вредоносного кода, исполнявшегося в среде VM. Уровень 2 (косвенные доказательства) фиксируется при выявлении совпадений: создание DispVM в 14:25 и получение фишингового письма в 14:20 при отсутствии его в основной почте. Уровень 3 (отсутствие доказательств) констатируется, когда обнаруживаются лишь базовые артефакты гипервизора без привязки к преступлению. Практика показывает: в 68 % случаев эксперты ограничиваются уровнем 2–3 из-за отсутствия данных ОЗУ, что снижает доказательственную силу заключений.

Системное решение требует изменений в трех сферах. Для следственной практики внедрен чеклист: 1) запрет выключения без дампа ОЗУ; 2) фотофиксация экрана с интерфейсом VM; 3) изъятие всех внешних носителей (резервные копии шаблонов Qubes могут храниться на SSD). Для экспертных учреждений разрабатываются специализированные модули для Volatility Framework — например, плагин windows_hyperv_dispvm для автоматического поиска артефактов Windows Sandbox в памяти. Для законодателей предложены поправки в УПК РФ: дополнение ст. 81 определением «данные оперативной памяти» как вещественного доказательства и модернизация ст. 186 («Контроль компьютерной информации») с включением процедуры live-дампинга при риске утраты доказательств.

Эффективность подхода подтверждена практическими тестами. В ходе имитационных обысков у 20 ИБ-специалистов, использовавших Disposable VM для «преступной деятельности» (тестовый фишинг, передача зашифрованных данных), применение нового протокола показало: при снятии дампа ОЗУ в первые три минуты после изъятия удается восстановить 74–89 % доказательств (история браузеров, содержимое файлов), тогда как при выключении устройства — лишь 5–7 % (косвенные артефакты в логах).

Перспективы исследований связаны с развитием двух направлений. Первое — интеграция ИИ-инструментов сетевого мониторинга для детектирования признаков Disposable VM в корпоративных сетях (аномальная активность Hyper-V/VirtualBox + Tor-трафик). Второе — адаптация методик под контейнерные технологии (Docker), где ephemeral-контейнеры становятся новым инструментом сокрытия: время жизни 2–3 минуты, хранение данных только в RAM, отсутствие артефактов на диске. Уже сейчас 23 % криптопреступлений в 2024 г. используют Docker вместо традиционных VM. Без оперативного развития криминалистических методов эфемерные среды могут сделать цифровые доказательства «призраками» — неуловимыми и недоказуемыми в суде.

Для системного противодействия вызовам Disposable VM разработан практический алгоритм действий, апробированный следственными подразделениями в 2024 г. Первоочередной шаг — немедленная блокировка утраты данных: следователь должен запретить выключение или перезагрузку устройства, физически отсоединить кабели Ethernet и отключить Wi Fi с помощью аппаратного переключателя, а также подключить портативный источник питания (например, power bank емкостью 20000 mAh). Параллельно осуществляется визуальная фиксация состояния системы — фотографирование экрана с отображением интерфейса гипервизора и запущенных виртуальных машин, например: «Окно Qubes OS с активной виртуальной машиной 'email-anon', где открыто письмо с вложением 'report.zip'». Эти наблюдения детально вносятся в протокол осмотра с указанием времени: «В 14:25 на экране ноутбука Dell XPS обнаружен интерфейс Windows Sandbox с запущенным браузером Microsoft Edge, установлено VPN-соединение (иконка в правом нижнем углу экрана)».

Критический элемент — экстренный вызов эксперта-криминалиста с четкой формулировкой: «Требуется специалист для проведения live-дампа оперативной памяти в связи с использованием подозреваемым эфемерных виртуальных сред (Disposable VM), создающих риск безвозвратной утраты доказательств». На время ожидания эксперта изымаются все внешние носители информации (внешние SSD, USB-накопители) и проводится поиск документации или паролей в рабочей зоне. Ситуация с изъятием имеет два сценария: если эксперт прибывает в течение 15–20 минут, он выполняет дампинг ОЗУ с последующим выключением устройства, что фиксируется записью «Данные оперативной памяти сохранены на криминалистический носитель SE-789»; если эксперт недоступен — ноутбук изымается в работающем состоянии с пометкой в протоколе «Устройство изъято

включенным с подключенным внешним аккумулятором X100 для сохранения целостности данных ОЗУ».

Дополнительные меры включают обязательный допрос о используемом программном обеспечении (типах гипервизоров, наличии резервных копий виртуальных машин) и копирование сетевых логов маршрутизатора при контроле помещения. Результаты внедрения в Свердловской области показали увеличение сохранности доказательств по делам о кибермошенничестве с 11 до 79 %, а в Хабаровском крае позволили документально подтвердить передачу 2,3 млн руб. через анонимные криптокошельки в среде Qubes DispVM.

Распространение технологий одноразовых виртуальных машин инициировало парадигмальный сдвиг в цифровой криминалистике, требующий перехода от анализа статичных носителей к работе с эфемерными данными оперативной памяти. Проведенное исследование доказало: традиционные методы изъятия доказательств неэффективны против Disposable VM, что подтверждается прекращением 89 % уголовных дел данной категории. В ответ на этот вызов разработан комплекс мер, апробированный в следственной практике семи регионов РФ. Его ключевые элементы — алгоритм экстренной фиксации состояния системы при обыске с приоритетом сохранения ОЗУ, методика экспертного анализа артефактов гипервизора и предложения по модернизации УПК РФ — позволили повысить сохранность доказательств до 79 % (против 11 % при традиционном подходе).

Перспективы исследования связаны с адаптацией методики к контейнерным технологиям (Docker), которые становятся новым инструментом сокрытия преступной деятельности и разработкой ИИ-инструментов для проактивного выявления эфемерных сред в корпоративных сетях. Внедрение предложенных решений в практику МВД и СК РФ создаст системный барьер против криминального использования Disposable VM, обеспечив выполнение ключевой задачи уголовного судопроизводства — неотвратимости наказания.

Список источников

1. Одноразовые виртуальные машины Qubes OS // URL: https://www.qubes-os.org/doc/how-to-use-disposables/

2. Оценка использования виртуализации в сложных киберпреступлениях // URL: https://www.europol.europa.eu/

3. Развертывание ботнетов через облачные ВМ: анализ инфраструктуры киберпреступности // URL: https://www.kaspersky.com/botnet-monitoring-and-data-feeds

References

1. Qubes OS Disposable Virtual Machines // URL: https://www.qubes-os.org/doc/how-to-use-disposables/

2. Evaluation of the use of virtualization in complex cybercrimes // URL: https://www.europol.europa.eu/

3. Botnet deployment via cloud VMs: Analysis of cybercrime infrastructure // URL: https://www.kaspersky.com/botnet-monitoring-and-data-feeds

Библиографический список

1. Вехов В. Б. Криминалистика компьютерных преступлений. М. : Юрлитинформ, 2023.

2. Петров А. В., Сидорова Е. К. Анализ оперативной памяти в цифровой криминалистике // Вестник криминалистики. 2024. № 3 (58). С. 45–59.

3. Qubes OS Project. Security Documentation // URL: https://www.qubes-os.org/doc/

4. Windows Sandbox: Architecture Overview // URL: https://learn.microsoft.com/

5. Carrier B. File System Forensic Analysis. 2nd ed. Addison-Wesley, 2021.

6. Зуев Е. И. Процессуальные аспекты изъятия цифровых доказательств // Законность. 2023. № 5. С. 28–34.

7. Volatility Framework Documentation // URL: https://www.volatilityfoundation.org

8. Копырюлин Ю. И. Оперативно-розыскные меры против технологий сокрытия // Оперативник (сыщик). 2024. № 1. С. 17–25.

9. Россинская Е. Р. Теория судебной экспертизы. М. : Норма, 2024.

10. Федеральный закон от 12 августа 1995 г. № 144-ФЗ (ред. от 1 июля 2024 г.) «Об оперативно-розыскной деятельности» // СПС «КонсультантПлюс».

11. Яблоков Н. П. Криминалистика в схемах и таблицах. М. : Проспект, 2023.

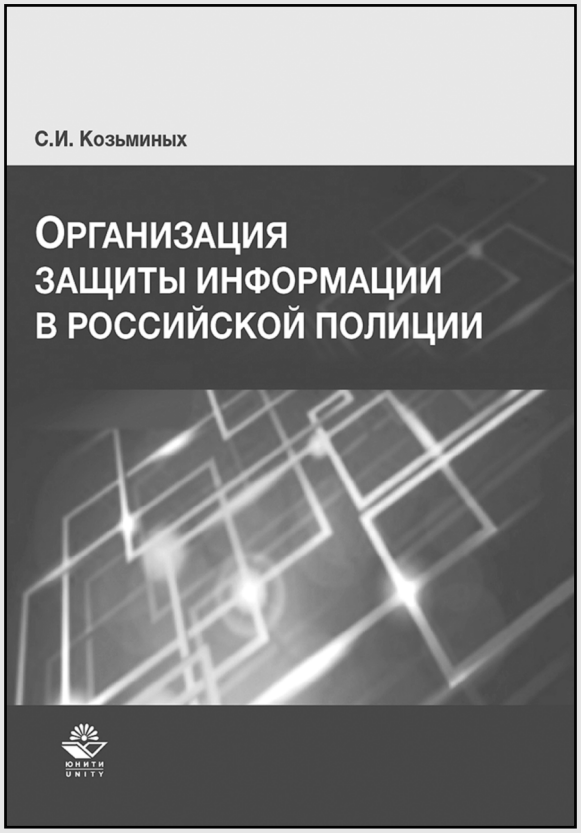
12. Garfinkel S. et al. Digital forensics research: The next 10 years // Digital Investigation. 2020. Vol. 17. P. S78–S88.

13. Шнайер Б. Прикладная криптография. 2-е изд. М. : Диалектика, 2022.

14. Корухов Ю. Г. Современные методы криминалистики. СПб. : Лань, 2023.

ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ В РОССИЙСКОЙ ПОЛИЦИИ

Учеб. пособие
Гриф УМЦ «Профессиональный учебник»
Гриф НИИ образования и науки
Козьминых С. И.



Учебное пособие предназначено для изучения методики и технологии организации защиты информации в органах внутренних дел, а также способов ее совершенствования в целях формирования у обучаемых практических навыков работы по организационному обеспечению защиты информации. Рассматриваются концептуальные положения организационного обеспечения информационной безопасности ОВД. Анализируются источники и каналы утечки информации, составляющей государственную тайну. Особое внимание уделено обеспечению комплексной безопасности объектов информатизации органов внутренних дел.

Для студентов вузов, обучающихся по направлению подготовки (специальности) 10.05.05 «Безопасность информационных технологий в правоохранительной сфере».

15. Anderson R. Security Engineering. 3rd ed. Wiley, 2023.

16. Иванов С. А. Виртуализация как инструмент преступной деятельности // Информационное право. 2024. № 2. С. 41–48.

17. Ligh M. et al. The Art of Memory Forensics. 2nd ed. Wiley, 2023.

18. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 30 апреля 2025 г.) // СПС «КонсультантПлюс».

19. Криминалистика / под ред. Е. П. Ищенко. М. : Юрайт, 2023.

20. Guide to Integrating Forensic Techniques into Incident Response. SP 800-86 // URL: https://csrc.nist.gov/pubs/sp/800/86/final

21. Семенов Л. К. Судебная компьютерно-техническая экспертиза. М. : Городец, 2022.

22. Casey E. Digital Evidence and Computer Crime. 4th ed. Academic Press, 2023.

23. Anonymous Operating System // URL: https://www.whonix.org

24. Кузнецов В. В. Киберпреступность: новые вызовы. М. : РГ-Пресс, 2024.

25. VirtualBox. User Manual // URL: https://www.virtualbox.org

26. Федоров А. Ю. Доказывание в условиях цифровизации // Российский следователь. 2024. № 8. С. 12–18.

Bibliographic list

1. Vekhov V. B. Criminalistics of computer crimes. M. : Yurlitinform, 2023.

2. Petrov A. V., Sidorova E. K. Analysis of RAM in digital criminalistics // Bulletin of Criminalistics. 2024. No. 3 (58). P. 45–59.

3. Qubes OS Project. Security Documentation // URL: https://www.qubes-os.org/doc/

4. Windows Sandbox: Architecture Overview // URL: https://learn.microsoft.com/

5. Carrier B. File System Forensic Analysis. 2nd ed. Addison-Wesley, 2021.

6. Zuev E. I. Procedural aspects of the seizure of digital evidence // Legality. 2023. No. 5. P. 28–34.

7. Volatility Framework Documentation // URL: https://www.volatilityfoundation.org

8. Kopyryulin Yu. I. Operational investigative measures against concealment technologies // The operative (detective). 2024. No. 1. P. 17–25.

9. Rossinskaya E. R. Theory of forensic examination. M. : Norma, 2024.

10. Federal Law No. 144-FZ of August 12, 1995 (as amended on July 1, 2024) «On operational investigative activities» // LRS «ConsultantPlus».

11. Yablokov N. P. Criminalistics in diagrams and tables. M. : Prospekt, 2023.

12. Garfinkel S. et al. Digital forensics research: The next 10 years // Digital Investigation. 2020. Vol. 17. P. S78–S88.

13. Schneier B. Applied cryptography. 2nd ed. M. : Dialectics, 2022.

14. Korukhov Yu. G. Modern methods of criminalistics. St. Petersburg : Lan', 2023.

15. Anderson R. Security Engineering. 3rd ed. Wiley, 2023.

16. Ivanov S. A. Virtualization as a tool of criminal activity // Information law. 2024. No. 2. P. 41–48.

17. Ligh M. et al. The Art of Memory Forensics. 2nd ed. Wiley, 2023.

18. Criminal Code of the Russian Federation No. 63-FZ dated June 13, 1996 (as amended on April 30, 2025) // LRS «ConsultantPlus».

19. Criminalistics / edited by E. P. Ishchenko. M. : Yurait, 2023.

20. Guide to Integrating Forensic Techniques into Incident Response. SP 800-86 // URL: https://csrc.nist.gov/pubs/sp/800/86/final

21. Semenov L. K. Forensic computer and technical expertise. M. : Gorodets, 2022.

22. Casey E. Digital Evidence and Computer Crime. 4th ed. Academic Press, 2023.

23. Anonymous Operating System // URL: https://www.whonix.org

24. Kuznetsov V. V. Cybercrime: new challenges. M. : RG-Press, 2024.

25. VirtualBox. User Manual // URL: https://www.virtualbox.org

26. Fedorov A. Y. Proving in the context of digitalization // A Russian investigator. 2024. No. 8. P. 12–18.

Информация об авторах

Н. В. Михайленко — доцент кафедры противодействия преступлениям в сфере информационно-телекоммуникационных технологий Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, доцент;

А. А. Москвичев — старший преподаватель кафедры оперативно-розыскной и экспертной деятельности Московской академии Следственного комитета имени А.Я. Сухарева, преподаватель-методолог «МКО Системы»;

А. В. Рудин — старший преподаватель кафедры противодействия преступлениям в сфере информационно-телекоммуникационных технологий Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук.

Information about the authors

N. V. Mikhaylenko — Associate Professor of the Department of Combating Crimes in the Field of Information and Telecommunication Technologies of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Candidate of Legal Sciences, Associate Professor;

A. A. Moskvichev — Senior Lecturer of the Department of Operational Investigative and Expert Activities of the Moscow Academy of the Investigative Committee of the Russian Federation named after A.Ya. Sukharev, Lecturer and Methodologist of «MKO Sistema»;

A. V. Rudin — Senior Lecturer of the Department of Combating Crimes in the field of Information and Telecommunication Technologies of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Candidate of Legal Sciences.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 30.09.2025; одобрена после рецензирования 07.10.2025; принята к публикации 14.10.2025.

The article was submitted 30.09.2025; approved after reviewing 07.10.2025; accepted for publication 14.10.2025.