Дата поступления рукописи в редакцию: 04.03.2026 г.
Дата принятия рукописи в печать: 03.04.2026 г.
DOI: 10.24412/2076-1503-2026-3-623-627

ГОНЧАР Владимир Владимирович,
кандидат юридических наук, доцент кафедры информационных технологий и организации расследования киберпреступлений, Московская академия Следственного комитета Российской Федерации имени А.Я. Сухарева, e-mail: vg78@list.ru

ОСОБЕННОСТИ ОСМОТРА И ИЗЪЯТИЯ СЕРВЕРНОГО ОБОРУДОВАНИЯ

Аннотация. *В рамках настоящей статьи рассматриваются особенности обнаружения, осмотра, описания и изъятия серверного оборудования, некоторые аспекты изучения данных, хранящихся в составе RAID массивов, уделено внимание получению информации из облачных сервисов.*

Ключевые слова: *электронный носитель информации, серверное оборудования, информационные технологии, следственные действия, осмотр предметов, обыск, осмотр места происшествия, компьютерная криминалистика, RAID массив, облачные хранилища информации, облачные сервисы.*

GONCHAR Vladimir Vladimirovich,
PhD in Law, Associate Professor, Department of Information Technology and Cybercrime Investigation, Moscow Academy of the Investigative Committee of the Russian Federation named after A. Ya. Sukharev

INSPECTION AND REMOVAL OF SERVER EQUIPMENT

Annotation. *This article examines the detection, inspection, description, and seizure of server equipment, some aspects of studying data stored in RAID arrays, and focuses on obtaining information from cloud services.*

Key words: *electronic storage media, server equipment, information technology, investigative actions, inspection of objects, search, crime scene inspection, computer forensics, RAID array, cloud storage, cloud services.*

Как отмечают в экспертном сообществе, «Ежегодно количество успешных кибератак стремительно растет, а их сложность и агрессивность продолжают увеличиваться. Суммарное количество киберинцидентов за рассматриваемый период в 2025 году на 6% превосходит количество инцидентов за 2024 год, на 11% и 37% — за 2023 и 2022 год соответственно. По оценкам экспертов, глобальный ущерб от действий киберпреступников в 2026 году достигнет 11,9 триллионов долларов США, что составляет около 11% от мирового ВВП на 2024 год.» [1].

Разработчики ВПО уделяли много внимания методам сокрытия деструктивного воздействия и совершенствовали способы доставки, переключились на использование уязвимостей на сетевом периметре. Частных лиц в основном атаковали с помощью шпионского ВПО и банковских троянов, а организации чаще становились жертвами программ-вымогателей.

Трендом нескольких последних лет продолжает оставаться применение шифровальщиков, их доля среди ВПО составила около 50%. [1] Операторы программ-вымогателей перешли от массовых атак к целенаправленному выбору жертв, увеличили суммы выкупа, открыли новые сайты по продаже украденной информации и начали использовать DDoS-атаки для шантажа жертв.

Успешное раскрытие и расследование подобных преступлений невозможно без участия специалистов и экспертов, обладающих знаниями по особенностям работы с серверным оборудованием.

В данной статье авторы рассматривают отдельные аспекты данной деятельности.

Следует отметить, что при проведении следственных действий, связанных с исследованием серверного оборудования, можно выделить две основные следственные ситуации:

- изъятие серверного оборудования при поддержке владельца (сотрудник, занимающийся эксплуатацией и администрированием данного оборудования, добровольно предоставляет учетные данные и рассказывает о способах подключения);
- изъятие серверного оборудования, при котором администратор (собственник) не желает оказывать содействие, либо активно противодействует проводимому следственному действию.

И если при первой ситуации методики работы с оборудованием понятны, то в отсутствии средств взаимодействия и хоть какой-то первичной информации осмотр значительно осложняется.

Даже обнаружение сервера может вызвать затруднения, т.к. роль сервера может выполнять абсолютно любой компьютер. В рамках проведения следственного действия особое внимание стоит уделять исследованию сетевого взаимодействия устройств. Факт обнаружения сетевого хранилища, с которым взаимодействуют локальные компьютеры задаст необходимый вектор проведения следственного действия и в дальнейшем установление его местоположения станет лишь вопросом времени.

Обнаружив соответствующее устройство, его необходимо описать и упаковать (либо создать копию для дальнейшего исследования). В данном случае необходимо обратить внимание на особенности эксплуатации накопителей в серверном оборудовании. Зачастую привычные экспертам и специалистам накопители на жестких магнитных дисках используются в составе RAID-массивов, и изъятие отдельно накопителей, а уж тем более без должного их описания, последовательности установки и конфигурации RAID-массива приводит к серьезным затруднениям при проведении дальнейшего исследования (экспертизы).

Связано это, прежде всего, с недостаточной компетенцией привлеченного к производству следственного действия специалиста, который, например, не усмотрел необходимости в изъятии целиком аппаратного контроллера RAID-массива, ограничившись копиями жестких дисков, либо при схожих обстоятельствах не изъял из ноутбука один из жестких дисков, объединенных в массив, в виду того, что компоновка современных компьютеров затрудняет осмотр его элементов без полной разборки.

Не редко, следователи даже не подозревают, что в ходе осмотра и изъятия ноутбука или системного блока они также сталкиваются с хранением данных в RAID-массивах, поскольку жесткие диски, из которых он собран, не утрачены, настройки не нарушены. При этом высокий уровень компетенций судебного компьютерно-технического эксперта позволяет впоследствии качественно произвести исследование хранящихся в массиве данных, собрав в массив копии жестких дисков.

Таким образом, значимость указанной проблемы представляется надуманной. Допуская, что она может быть усугублена применением различных средств и способов шифрования данных, которые затрудняют доступ к значимой информации, необходимо отметить, что это не является чем-то особенным, поскольку зашифрованы и на аппаратном, и на программном уровне могут быть также жесткие диски, не собранные в RAID.

Проблемные следственные ситуации возникают, например, когда следователь привлекает к следственному действию специалиста в информационных технологиях, но не имеющего достаточной квалификации для изъятия серверного оборудования. Во избежание этого еще на подготовительном этапе необходимо убедиться, что специализация привлекаемого специалиста соответствует целям и задачам планируемого следственного действия.

При подготовке к проведению следственного действия следует предпринять все возможные меры к выявлению обстоятельств и обстановки, связанных с эксплуатацией серверного оборудования, подлежащего изучению и изъятию.

Важную информацию можно получить из показаний знакомых заподозренных лиц; посредством изучения статистических данных сетевых подключений и образцов сетевого трафика, предоставленных провайдером, оказывающим услугу доступа в сеть Интернет; а также сведений, истребованных из центров обработки данных и у провайдеров хостинговых услуг, предоставляющих дисковое пространство и вычислительные мощности.

Следователю целесообразно поручить привлеченным к расследованию преступления оперативным сотрудникам проведение оперативно-розыскных мероприятий по сбору таких сведений [3].

Результаты подготовительных мероприятий, проведенных совместно с заранее привлеченным квалифицированным специалистом, позволяют минимизировать ошибки, вызванные неправильным установлением места проведения следственного действия, например, когда серверы размещены не в офисном здании, а в дата-центре сторонней организации, или с объединением серверов в кластеры и их виртуализацией, либо активным противодействием подозреваемых.

Учитывая высокую изменчивость цифровых данных, обрабатываемых серверным оборудованием, легкость их уничтожения с целью сокрытия следов преступления, повышенные меры конспирации преступной деятельности, в том числе в виде систематической миграции данных с одного сервера на другой, возможность длительной подготовки к производству следственных действий, связанных с изъятием серверного оборудования, зачастую отсутствует. При таких обстоятельствах еще более тщательно следует отнестись к привлечению специалиста соответствующей квалификации и проверке его компетенции, поскольку ему придется действовать в сложной обстановке на протяжении длительного времени, возможно, в состоянии значительного психического напряжения, вызванном активным противодействием заподозренных лиц.

Следующей проблемой, с которой сталкиваются следователи и специалисты, является невозможность изъятия серверного оборудования целиком, например, при его внушительных размерах либо вследствие необходимости поддержания непрерывного информационного технологического процесса. В современных центрах, предоставляющих вычислительные мощности, широко используется технология виртуализации серверов, то есть разделения физического сервера с помощью специализированного программного обеспечения на несколько изолированных виртуальных серверов. От уровня изолированности виртуализация может быть полной либо частичной. В этом случае виртуальные серверы находятся под управлением специального программного обеспечения - гипервизора, но операционную систему и настройки пользователь выбирает и устанавливает самостоятельно. В другом варианте виртуализация реализуется на уровне операционной системы.

В подобном случае изъятие виртуального сервера особых трудностей не вызывает, поскольку данные и настройки сервера содержатся в директории в единой файловой системе физического сервера, специалисту необходимо скопировать содержимое директории на электронный носитель информации, предварительно поместив его в архив и рассчитав хеш-сумму архива с использованием криптостойких алгоритмов (например, SHA-256), которую следует внести в протокол следственного действия. Складывающаяся правоприменительная практика допускает самостоятельное копирование виртуального сервера сотрудниками компаний - провайдеров хостинговых услуг на электронный носитель информации с последующим его изъятием в ходе выемки.

Изъятие виртуального сервера, находящегося под управлением гипервизора, становится более сложной задачей, если его владельцем применяются средства шифрования, например, сервис BitLocker в случае использования ОС Windows. При таких обстоятельствах изъятие копии сервера (например, с помощью стандартных средств создания резервной копии) не позволит получить доступ к данным. Для преодоления создавшейся проблемной ситуации следует, помимо копии виртуальной машины, получить дамп процесса виртуализации из оперативной памяти физического сервера и сохранить его на электронный носитель информации. В процессе экспертного исследования из дампа процесса с помощью специальных программных средств возможно извлечь пароль для расшифровки данных, содержащихся в копии виртуальной машины.

Противодействие со стороны заподозренных лиц при изъятии серверного оборудования создает значительные проблемы для следственной группы. Ситуация усугубляется в случае использования серверов, объединенных в одну группу с образованием единого ресурса (кластера серверов), либо ультракомпактных серверов (блейд-серверов) в единой корзине (шасси) с созданием RAID-массивов. Несмотря на то, что кластеры находятся, как правило, в одной локальной сети, как и блейд-серверы, задача по их изъятию значительно усложняется при нежелании их владельцев сотрудничать со следствием.

Для пресечения возможного активного противодействия проводимым следственным действиям после проникновения в исследуемое с целью изъятия серверного оборудования помещение следует отстранить от техники и силовых кабелей находящихся там лиц и, используя фактор внезапности, немедленно приступить к исследованию системы. Если заподозренные лица отказываются от содействия следователю, необходимо самостоятельно, совместно со специалистом обнаружить серверное оборудование, подлежащее изъятию. Для этого следует вручную последовательно отключать сегменты локальной сети, одновременно непрерывно посылая тестовые сетевые пакеты на требуемый ресурс. Когда сервер становится недоступным, необходимо сужать круг поиска, продолжая отключать серверы из этого сегмента сети.

Получив таким образом доступ к серверу, на котором установлен гипервизор, управляющий виртуальными машинами, физически расположенными на других серверах, можно контролировать дальнейшие отключения, чтобы не допустить неполноты следственного действия. Кроме того, в поисковых мероприятиях можно использовать

программу Traceroute, которая при определенных обстоятельствах возвращает, в том числе, IP-адрес гипервизора. Значительно упростит исследование локальной сети компании - провайдера хостинговых услуг доступ к интерфейсу биллинговой системы, которая может содержать сведения о гипервизорах и таблицы соответствия IP-адресов виртуальных машин и гипервизоров. Действия специалиста по выявлению оборудования должны быть подробным образом описаны в протоколе соответствующего следственного действия. Выявленное таким образом оборудование подлежит изъятию целиком, в том числе блейд-серверы. Такая возможная избыточность в изъятии средств вычислительной техники вполне оправдана, поскольку в ином случае доказательства могут быть безвозвратно утрачены, а перспективы успешного расследования преступления уменьшаются.

Следует отметить, что в последние годы все более активно применяются так называемые RAID-массивы в серверном оборудовании. Массивы могут быть реализованы на аппаратном, интегрированном аппаратном и программном уровнях, следование следующим методикам при осмотре и изъятии компьютерной техники позволит избежать проблемных ситуаций, связанных с дальнейшей ее исследованием [2].

Программный RAID-массив создается средствами операционной системы, данные обрабатываются непосредственно центральным процессором.

При проведении следственных действий, обнаружив сервер, установить наличие RAID можно с помощью штатных средств операционных систем. На работающей системе под управлением ОС LINUX-подобных операционных системах информация о RAID-массиве может быть собрана с помощью команд.

В ОС Windows диспетчер дисков отображает информацию о жестких дисках, собранных в массив. Сведения о конфигурации массива хранятся в реестре Windows. В данном случае, с учетом полученных сведений о настройках RAID-массива и используемых жестких дисках, создание их побитовых (посектроных) копий (образов) достаточно для восстановления массива данных.

В то же время необходимо иметь в виду, что в случае интегрированного аппаратного подхода для реализации RAID обработка данных осуществляется совместно центральным процессором и отдельным интегрированным в материнскую плату контроллером. Операционная система в этом случае определяет массив как физический диск и, соответственно, средствами операционной системы получить информацию о конфигурации и настройках RAID-массива не представляется возможным.

Для проверки наличия RAID необходимо зайти в меню BIOS, которое отображает информацию о подключенных жестких дисках, конфигурации и настройках RAID. Такая проверка позволит исключить ситуацию, когда один из дисков, собранных в RAID, не будет оставлен в компьютере, если принято решение не изымать системный блок либо ноутбук целиком.

Изъятые жесткие диски либо их побитовые (посекторные) копии в случае с интегрированной реализацией RAID также без особых проблем могут быть собраны в массив, например, с использованием специализированного ПО R-studio либо подобного ему (PC-3000 Data Extractor UDMA RAID Edition, UFS Explorer Professional Recovery). Иначе может обстоять дело с осмотром аппаратного RAID-массива, который реализован как отдельный контроллер со своим процессором и памятью для хранения кэша, обрабатывающий данные, хранящиеся на подключенных к нему жестких дисках.

В этом случае целесообразным является изъятие контроллера целиком, поскольку конфигурация и настройка массива дисков могут быть отличными от стандартных вариантов. Иначе восстановление RAID-массива придется производить в ручном режиме с большими временными затратами.

В то же время необходимо отметить, что в случае утраты части жестких дисков ранее упомянутое специализированное ПО, как например R-studio, при определенных обстоятельствах может восстановить пользовательские данные, хранящиеся на оставшихся дисках либо файловую структуру. Объем и вид восстановленной информации зависит от многих факторов (уровня RAID, размера страйпа, очередностью диска в последовательности записи данных и т.п.).

Рекомендации по методике осмотра компьютерной техники, использующей такой способ хранения данных как RAID-массив, когда имеются основания полагать, что данные могут быть защищены аппаратным либо программным шифрованием, не отличаются от общих рекомендаций.

Особое же внимание необходимо уделить серверному оборудованию, доступ к которому осуществляется посредством взаимодействия через специализированную аппаратную консоль (например, серверные решения от IBM). В таком случае роль средства взаимодействия отводится отдельному компьютеру\консоли, внешне аппаратная реализация консоли Hardware Management

Console – HMC мало чем отличается от любого другого серверного оборудования. При этом исследовать отдельно накопители информации вне аппаратного контроллера RAID, как уже было сказано ранее, нецелесообразно. В связи с этим имеет смысл при производстве следственных действий помимо сервера хранения данных установить, где находится консоль управления и изъять объекты в составе как сервера хранения данных, так и консоли управления.

Далее, скопировав всю необходимую информацию, можно исследовать полученную информацию согласно имеющимся методикам.

Стоит также отметить, что наилучшим вариантом получения данных с серверного оборудования является копирование непосредственно на месте осмотра изъятия данной техники. Это обусловлено тем, что на имеющихся на месте устройствах могут быть активные сессии, которые позволят получить доступ к хранимой информации без каких-либо препятствий. На рабочей системе необходимо произвести поиск криминалистически значимой либо оперативно ориентирующей информации и скопировать ее на внешний носитель. В протоколе следственного действия должны быть в полной мере описаны действия специалиста по поиску и копированию информации и основания необходимости проведения таких действий.

В следственной практике не редко встречаются ситуации, при которых необходимо наряду с RAID массивами осматривать «облачные» хранилища информации, данные, имеющие доказательственное значение, и реализованные как публичные либо приватные сервисы в сети Интернет. Считаем, что такие действия целесообразно осуществлять в рамках оперативного мероприятия «получение компьютерной информации», так как уголовно-процессуальным законодательством не предусмотрено соответствующего следственного действия.

Сложившаяся следственная практика изучения электронных страниц веб-сайтов в ходе осмотре электронного документа в данном случае неприменима, т.к. доступ к аккаунту облачного хранилища, в большинстве случаев, осуществляется по URL-адресу под аутентификационными данными владельца хранящейся в нем информации. Таким образом, при осмотре информации, содержащейся в «облачном» хранилище, производится копирование данных с удаленных серверов на электронный носитель информации, который приобщается к протоколу и в дальнейшем направляется на исследование или экспертизу. Действия, направленные на копирование информации, не должны нарушать целостность и конфиденциальность иных данных, не относящихся к исследуемому аккаунту.

Список литературы:

[1] Ландшафт киберугроз в 2025-м в России и мире // Хабр. URL: https://habr.com/ru/companies/pt/articles/988872/ (дата обращения: 17.01.2026).

[2] Гончар В.В., Галиев Д.В. Особенности осмотра и изъятия электронных носителей информации с учётом требований ст. 164.1 УПК РФ // Вестник Московского университета МВД России. 2020. № 2. С. 134-134.

[3] Тисен О.Н. Субъекты досудебного соглашения о сотрудничестве// // Судебная власть и уголовный процесс. 2013. № 2. С. 91-95.

References:

[1] The Cyber Threat Landscape in 2025 in Russia and the World // Habr. URL: https://habr.com/ru/companies/pt/articles/988872/ (accessed: 17.01.2026).

[2] Gonchar V.V., Galiev D.V. Features of Inspection and Seizure of Electronic Storage Media Taking into Account the Requirements of Art. 164.1 of the Criminal Procedure Code of the Russian Federation // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2020. No. 2. pp. 134-134.

[3] Tisen O.N. Parties to a Pre-Trial Cooperation Agreement // Judicial Authority and Criminal Procedure. 2013. No. 2. pp. 91-95.