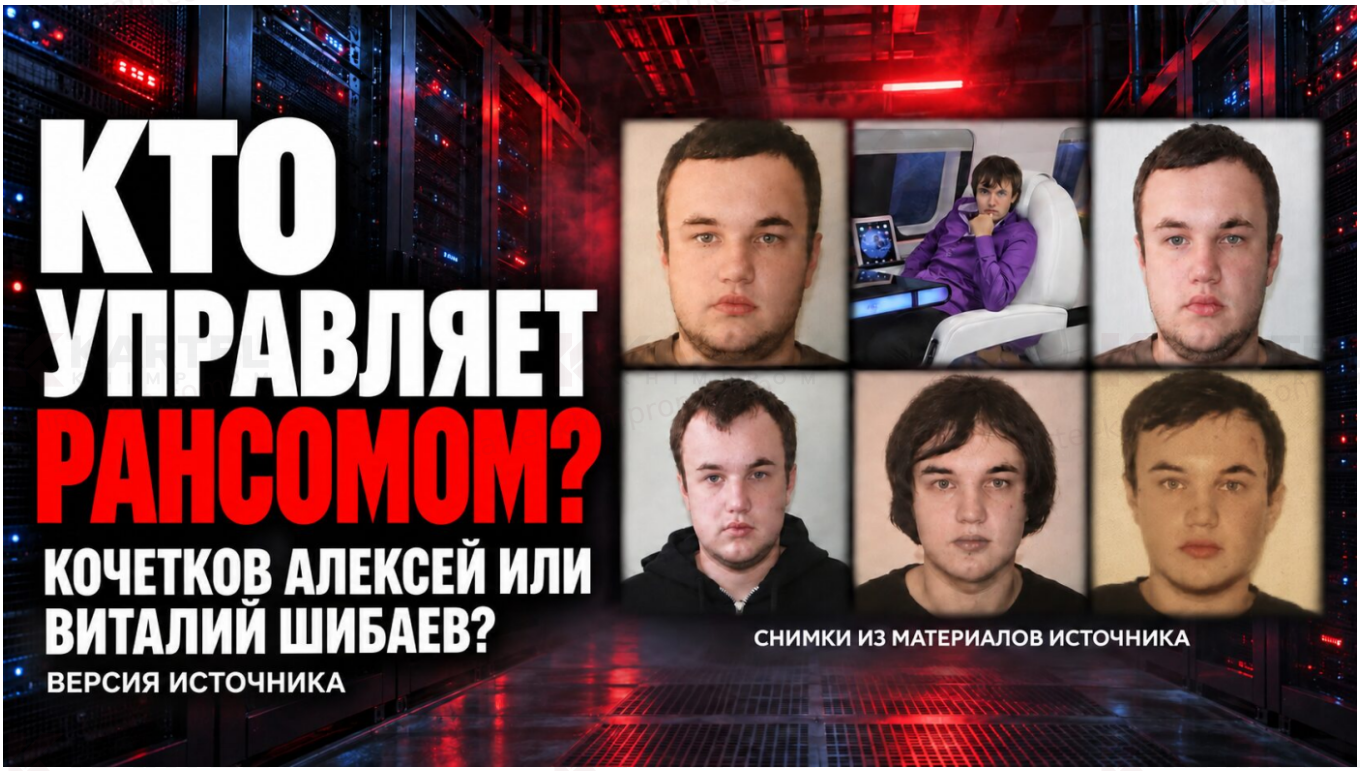
ПУБЛИКАЦИЯ / RU

Кочетков Алексей или Виталий Шибаев? Кто управляет рансомом

Опубликовано 18.11.2026 · Обновлено 18.11.2026

Как устроено кибервымогательство, кто стоял за LockBit и REvil, что содержится в материалах о розыске Алексея Кочеткова и на чём основана версия о Виталии Шибаеве.



Фотоколлаж с ИИ из шести предоставленных снимков. Связь между именами Алексея Кочеткова и Виталия Шибаева остаётся версией источника.

При использовании обязательна ссылка на оригинал
kartel-khimprom.com / RU

В материалах, полученных редакцией, рядом с именем Алексея Кочеткова стоит отметка *High Tech Crime*. В том же документе указан запрос на розыск и арест по каналам Интерпола от 19 марта 2015 года. Источник KARTEL KHIMPROM выдвигает более серьёзную версию: говорит, что Кочетков стал одним из руководителей группировки, которую собеседник относит к крупнейшим на рынке ransomware, а в Украине получил документы на имя Виталия Шибаева. Мы сверили даты и номера в полученных материалах и проверили, какую часть этой истории можно подтвердить.

Публичные дела LockBit, REvil и других сетей показывают, на чём строится доказательство руководящей роли. В расследованиях появились конкретные псевдонимы, серверы, переписки и операции с выкупом. В материалах о Кочеткове есть другая отправная точка — реквизиты московского дела и фотокопии отчёта о розыске. До названия рансом-группы и доказанной связи с ней нужно пройти ещё несколько шагов.

Что такое рансом и за что требуют выкуп

Ransomware — вредоносное ПО, с помощью которого преступники блокируют доступ к данным, обычно шифруя файлы, и требуют выкуп за восстановление. В разговорах о киберпреступности «рансомом» часто называют всю схему вымогательства. Жертве могут угрожать и публикацией похищенных данных. Когда преступники одновременно шифруют системы и шантажируют утечкой, это называют **двойным вымогательством**. Бывают и случаи, когда давление строится исключительно на угрозе публикации. Руководство CISA по ransomware и вымогательству данных.

Размер требования — лишь часть ущерба. Компания теряет доступ к рабочим системам и платит за их восстановление. Если в сеть утекли сведения о клиентах, риск сохраняется и после восстановления файлов. У больницы, например, простой затрагивает приём пациентов и доступ сотрудников к медицинским записям. В обзоре ENISA за 2026 год ransomware выделен как тип инцидента с наиболее тяжёлыми краткосрочными последствиями. Обзор киберугроз ENISA за 2026 год.

Почему у одной группировки может быть много исполнителей

При **Ransomware-as-a-Service (RaaS)** одни участники поддерживают вредоносную программу и сервис для партнёров, а другие проводят атаки. Администраторы могут отвечать за панель со списком жертв и площадку для публикации похищенных данных. Партнёр, или аффилиат, использует инфраструктуру и делится частью выкупа. Именно такую модель американское обвинение описывает в деле LockBit. В материалах о Дмитрии Хорошеве прокуратура утверждает, что администратор обычно получал около 20% от каждого платежа. Обвинение Минюста США по делу Хорошева и LockBit.

Этот расклад помогает понять, почему выражение «лидер группировки» требует расшифровки. Тот, кто отвечает за разработку, может контролировать код, а тот, кто ведёт переговоры, — знать жертв и суммы. Управление всей платформой предполагает доступ к её инфраструктуре, правилам работы партнёров или расчётам между ними. Чтобы установить такую роль, следствию нужно связать конкретного человека с конкретными действиями.

У расследователей здесь три разных вопроса. Кто контролировал аккаунт, с которого общались с жертвой? Кто мог изменить правила работы сервиса или отключить партнёра? Кто получил долю после перевода денег? Переписка помогает ответить на первый вопрос, журналы работы сервиса и материалы изъятой инфраструктуры — на второй, а документы о платеже — на третий. Одна и та же подпись в записке о выкупе может называть бренд, которым пользовались разные исполнители.

Кого называют «королями рансома» и что известно об их делах

Дмитрий Хорошев, LockBit. В мае 2024 года Минюст США назвал его предполагаемым разработчиком и администратором. Ведомство оценивает масштаб работы LockBit более чем в 2,5 тысячи жертв как минимум в 120 странах и не менее чем в $500 млн полученных выкупов. Это оценка всей операции, которую приводит обвинение. В феврале 2024 года в ходе операции Cronos правоохранители получили контроль над частью инфраструктуры LockBit. Europol об операции Cronos.

Ярослав Васинский, REvil. В мае 2024 года суд в США приговорил его к 13 годам и 7 месяцам заключения. Минюст США сообщил о более чем 2,5 тысячи атак и требованиях выкупа на сумму свыше $700 млн. Здесь речь о сумме требований. Суд также обязал Васинского выплатить более $16 млн компенсации. В материалах дела он фигурирует как аффилиат REvil. Сообщение Минюста США о приговоре Васинскому.

Михаил Матвеев, LockBit, Babuk и Hive. В 2023 году американская прокуратура обнародовала обвинения, связывающие его с применением трёх видов программ-вымогателей. В публичных материалах среди его предполагаемых псевдонимов назван Wazawaka. Этот пример показывает, что одного участника могут связывать с несколькими программами. При сравнении групп полезно смотреть, что именно подтверждают материалы дела — разработку, администрирование платформы или участие в отдельных атаках. Обвинения Минюста США в отношении Матвеева.

Цифры из этих дел измеряют разное. Количество атак описывает активность, сумма требований — масштаб давления на потерпевших, а подтверждённые платежи помогают оценить доход. Для сравнения двух групп нужны один и тот же период и одна и та же мера. В случае Кочеткова источник не назвал ни группу, ни показатель, по которому относит её к крупнейшим.

Алексей Кочетков. Что можно прочитать в материалах о розыске

В двух полученных редакцией учётных записях совпадают ФИО Алексея Алексеевича Кочеткова, дата рождения **21 сентября 1988 года** и номер уголовного дела **369631**. В одной строке указано, что 17 февраля 2014 года его поставили на розыск по инициативе УВД по Центральному административному округу ГУ МВД России по Москве. В качестве основания указана ч. 4 ст. 159 УК РФ. В другой записи при том же номере дела перечислены неправомерный доступ к компьютерной информации, вредоносные программы и мошенничество. Там же встречаются ссылки на ст. 272, 273 и 159 УК РФ, а отдельная строка упоминает ч. 1 ст. 210. Привязку этой отдельной строки к делу № 369631 установить не удалось.

В переданной редакции фотокопии *Individual Report* указаны **Alexey Kochetkov**, та же дата рождения и ссылка **2015/18570-1**. В графе вида международного сообщения стоит **Diffusion**, дата — **19 марта 2015 года**. Указаны бюро *NCB Moscow*, статус *Wanted*, цель *Arrest* и

категория *High Tech Crime*. В качестве судебного основания названо решение **Тверского районного суда Москвы от 22 ноября 2013 года**. В видимой части фотокопии номер российского уголовного дела отсутствует. Имя и дата рождения дают основание сопоставить записи. Связь между номерами предстоит проверить по судебному акту.

Интерпол поясняет, что *diffusion* может направляться национальным бюро напрямую другим странам. Поиск публичных красных уведомлений поэтому не отвечает на вопрос, рассылался ли такой запрос. Подлинность полученной фотокопии и актуальный статус сообщения редакция независимо не подтвердила. В проверенных открытых источниках мы также не нашли самого постановления, обвинительного приговора или сведений об экстрадиции Кочеткова по этому делу. Интерпол о механизме diffusion. Портал Тверского районного суда.

Кочетков Алексей или Виталий Шибаев? Что утверждает источник

По словам источника KARTEL KHIMPROM, Кочетков занял руководящую роль в одной из группировок, которые собеседник относит к крупнейшим в ransomware. Полученные учётные материалы относятся к делу о компьютерных преступлениях. В них нет названия рансом-группировки, периодов управления, названий атакованных организаций или подтверждённых эпизодов получения выкупа. Пока редакция не может независимо установить, о какой группе говорит источник и в чём выражалась предполагаемая руководящая роль.

Тот же источник утверждает, что в Украине Кочетков получил паспорт на имя **Виталия Викторовича Шибаева** с датой рождения **3 декабря 1986 года**, и называет этот документ паспортом прикрытия. Это утверждение требует отдельной проверки. В доступных редакции материалах нет записи уполномоченного органа о выдаче такого документа Кочеткову или судебного акта, связывающего два имени. Сопоставлять их по присланным портретам недостаточно. Дату рождения в этой версии приводим со слов источника как данные предполагаемого документа.

Что мы ищем и за какие сведения готовы обсудить вознаграждение

Для проверки важны постановление Тверского районного суда от 22 ноября 2013 года, материалы с привязкой дела № 369631 к конкретному компьютерному эпизоду, а также документы, позволяющие проверить связь Кочеткова с конкретной группой или сведения о выдаче документа на имя Шибаева. Если у вас есть проверяемые материалы, **напишите в редакцию. Мы готовы обсудить вознаграждение за сведения, которые удастся подтвердить.** Для первого сообщения достаточно указать вид документа, его дату и то, что он подтверждает. Редакция открыта для комментариев упомянутых лиц и ведомств. Контакты редакции KARTEL KHIMPROM.

Источники

1. Руководство CISA по ransomware и вымогательству данных
   https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf
2. Обзор киберугроз ENISA за 2026 год
   https://www.enisa.europa.eu/publications/enisa-threat-landscape-2026
3. Обвинение Минюста США по делу Хорошева и LockBit
   https://www.justice.gov/usao-nj/pr/us-charges-russian-national-developing-and-operating-lockbit-ransomware
4. Europol об операции Cronos
   https://www.europol.europa.eu/node/5666
5. Сообщение Минюста США о приговоре Васинскому
   https://www.justice.gov/archives/opa/pr/sodinokibirevil-affiliate-sentenced-role-700m-ransomware-scheme
6. Обвинения Минюста США в отношении Матвеева
   https://www.justice.gov/archives/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure
7. Интерпол о механизме diffusion
   https://www.interpol.int/en/How-we-work/Notices/About-Notices
8. Портал Тверского районного суда
   https://mos-gorsud.ru/rs/tverskoj/services/cases/criminal-materials

Использование материалов

При использовании материалов обязательна активная ссылка на исходную публикацию.

Оригинал материала

https://kartel-khimprom.com/ru/article/kochetkov-aleksej-ili-vitalij-shibaev-kto-upravlyaet-ransomom/

При использовании обязательна ссылка на оригинал