УДК 343.9 **DOI: 10.34670/AR.2026.81.57.070**

Современные формы организованной киберпреступности: уголовно-правовые проблемы квалификации, соучастия и доказывания

Салманов Элнур Ризванович

Аспирант,
Всероссийский государственный университет юстиции (РПА Минюста России),
117638, Российская Федерация, Москва, ул. Азовская, 2, корп. 1;
e-mail: elnur.s.00@mail.ru

Аннотация

Организованная киберпреступность в последние годы трансформировалась из совокупности разрозненных эпизодов неправомерного доступа, хищений и мошеннических действий в устойчивый сегмент преступной деятельности, основанный на цифровой инфраструктуре, функциональном разделении ролей и трансграничном характере взаимодействия участников. Российская статистика 2021–2026 гг. фиксирует не только значительный рост числа зарегистрированных ИТ-преступлений, но и усложнение их способов, вовлечение легальных платформ, платежных сервисов, криптоактивов, а также расширение практик социальной инженерии. В настоящей статье сформулирован вывод о необходимости доказывания как факта технологического взаимодействия, так и криминальной интеграции функций, проявляющейся через регулярность коммуникации, распределение денежных потоков, общий пул ресурсов, правил конспирации, централизованное управление, повторяемость сценариев и сознательное участие лиц в создании либо поддержании преступной инфраструктуры. Таким образом, доказывание по делам об организованной киберпреступности должно строиться по модели «цепочки цифрового события».

Для цитирования в научных исследованиях

Салманов Э.Р. Современные формы организованной киберпреступности: уголовно-правовые проблемы квалификации, соучастия и доказывания // Вопросы российского и международного права. 2026. Том 16. № 4А. С. 574-583. DOI: 10.34670/AR.2026.81.57.070

Ключевые слова

Организованная киберпреступность, киберпреступления, соучастие, организованная группа, преступное сообщество, цифровые доказательства, вредоносное программное обеспечение, криптоактивы, трансграничная преступность, уголовный процесс.

Введение

Киберпреступность в России давно перестала быть периферийным явлением. По официальным данным, число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, выросло с 517 722 в 2021 г. до 765,4 тыс. в 2024 г. В 2025 г. МВД России зафиксировало 663 тыс. таких преступлений, а за первые четыре месяца 2026 г. сообщалось об их снижении, в том числе по тяжким составам и преступлениям в сфере компьютерной информации [Состояние преступности, 2026]. Однако даже на фоне отдельных положительных тенденций проблема не утрачивает актуальности: скорее, киберпреступность становится более сложной, скрытой и организованной.

Криминологическая значимость темы определяется не только масштабом причиняемого ущерба, но и изменением самой структуры преступной деятельности. Цифровая среда облегчила формирование устойчивых преступных сетей, в которых функции организаторов, разработчиков вредоносных средств, операторов call-центров, вербовщиков «дропов» и посредников по выводу похищенных средств распределяются между разными участниками и юрисдикциями. Рост целевых атак и преступлений, основанных на социальной инженерии, показывает, что современные киберпосягательства все чаще строятся на заранее спланированных и многоэтапных схемах [Данилова, 2026].

Основная часть

Динамика 2021-2024 гг. показывает, что киберпреступность росла не только количественно, но и структурно. Если на ранних этапах доминировало представление о «компьютерных преступлениях» как о неправомерном доступе или создании вредоносных программ, то фактически основная масса посягательств переместилась в сферу дистанционных хищений, мошенничества, несанкционированных операций с денежными средствами, подмены учетных записей, использования SIM-карт, реквизитов электронных средств платежа, а также манипулирования поведением потерпевшего через социальную инженерию. Преступный результат все чаще достигается не отдельным техническим действием, а серией взаимосвязанных операций: сбором персональных данных, компрометацией аккаунта, созданием поддельного интерфейса, вовлечением потерпевшего в коммуникацию, переводом средств на промежуточные счета, дроблением транзакций, дальнейшим обналичиванием или конвертацией в криптоактивы.

Эта трансформация означает, что организованность в цифровой среде проявляется иначе, чем в классических имущественных преступлениях. Устойчивость группы здесь нередко обеспечивается не личными контактами участников, а общей инфраструктурой: набором доменов, ботов, IP-узлов, панелей управления, кошельков, серверов хранения, баз данных, шаблонов скриптов общения с жертвами и каналов распределения ролей. Для таких схем характерны заменяемость исполнителей нижнего уровня и, напротив, высокая централизация на уровне администрирования. Иначе говоря, «ядро» организованной киберпреступной структуры может быть компактным, а периферия – широкой и легко обновляемой. Это особенно заметно в схемах с «дропами», фальшивыми инвестиционными платформами, кол-центрами, фишинговыми экосистемами и бот-сетями.

Статистика 2025–2026 гг. требует более осторожной интерпретации. Снижение общего числа зарегистрированных ИТ-преступлений, жертв и материального ущерба не обязательно

указывает на ослабление организованных цифровых групп [Семенцова, Малявина, 2025]. Во-первых, повышение защищенности банковского сектора и улучшение фильтрации сомнительных транзакций прежде всего бьет по массовым, но не всегда наиболее профессиональным схемам. Во-вторых, часть преступной активности смещается в сегменты с меньшей вероятностью регистрации: атаки на корпоративные сети, вымогательство, хищения криптоактивов, компрометация бизнес-переписки, нелегальный оборот данных и инфраструктуры доступа. В-третьих, организованные группы способны быстро адаптировать тактику, переключаясь с массовых обзвонов на гибридные схемы, где сочетаются взлом учетной записи, социальная инженерия и финансовое посредничество. Наконец, отдельного внимания заслуживает криминализация детской и подростковой аудитории: в 2025 г. ущерб от кибермошенничества в отношении несовершеннолетних оценивался примерно в 1 млрд руб., а число инцидентов, по данным отраслевой аналитики, превысило 7 тыс [Более 7 тыс. детей, 2025]. Это показывает, что преступные группы стали точечно выбирать уязвимые категории потерпевших и создавать под них отдельные сценарии воздействия.

Таким образом, основная тенденция состоит не просто в росте количества киберпреступлений, а в переходе к устойчивым преступным моделям платформенного типа. Для уголовного права это принципиально: квалифицировать приходится не единичное действие пользователя за клавиатурой, а сложную цепочку ролей, эпизодов и инструментов, часть из которых может иметь формально нейтральный характер.

С точки зрения Общей части уголовного права исходными остаются положения о соучастии, организованной группе и преступном сообществе, закрепленные в УК РФ. Однако цифровая среда обнажает ограниченность слишком буквального понимания признаков устойчивости, сплоченности и согласованности. В традиционной практике доказательствами организованной группы служили длительность совместной деятельности, распределение ролей, предварительная договоренность, конспирация, единая цель. В киберпространстве все эти признаки сохраняют значение, но приобретают иные внешние формы.

Во-первых, устойчивость группы может выражаться в устойчивости инфраструктуры, а не только персонального состава. Если преступная схема функционирует через один и тот же набор администрируемых аккаунтов, криптокошельков, фишинговых шаблонов, сервисов удаленного доступа и каналов вывода средств, то замена отдельных «операторов» не разрушает ее организованный характер. Во-вторых, распределение ролей получает техническое измерение: один участник пишет и адаптирует вредоносное ПО, другой обеспечивает хостинг и домены, третий ведет коммуникацию с жертвами, четвертый осуществляет «обнал» через цепочку карт и электронных кошельков, пятый вербует номинальных держателей счетов. В-третьих, предварительная согласованность нередко подтверждается не только перепиской или личными встречами, но и логами доступа, иерархией прав в панели администрирования, правилами распределения средств, автоматизированным учетом «планов» и выплат.

Поэтому применительно к цифровой среде следует исходить из функционального критерия организованности: если преступный результат обеспечивается заранее выстроенной системой взаимодополняющих ролей, объединенных единым преступным планом и общей инфраструктурой, то отсутствие территориальной совместности либо минимальный уровень личного знакомства между участниками не исключают признания группы организованной [Ахатова, 2026]. Более того, в ряде случаев именно удаленный формат и модульность выступают признаками более высокой, а не более низкой степени организованности.

Вместе с тем важно избегать чрезмерного расширения понятия организованной

киберпреступности. Не всякое использование нескольких лиц в интернет-среде образует организованную группу, и не всякий «маркетплейс» криминальных услуг автоматически свидетельствует о преступном сообществе. Наличие на теневой площадке продавца фишинговых наборов, покупателя доступа и независимого посредника еще не означает существования единой устойчивой структуры. Для квалификации по признакам организованной группы требуется установление именно совместного умысла на совершение конкретных преступлений либо серии однородных преступлений в рамках согласованной схемы. Если же лицо предоставляет универсальный цифровой сервис без доказанной осведомленности о конкретном преступном плане пользователя, основания для вменения соучастия оказываются существенно слабее.

Отсюда вытекает важный практический вывод: в делах об организованной киберпреступности нужно доказывать не только факт технического взаимодействия, но и криминальную интеграцию функций. Она проявляется через регулярность коммуникации, распределение доходов, общий пул ресурсов, правила конспирации, централизованное управление, повторяемость сценариев и сознательное участие лица в создании либо поддержании преступной инфраструктуры.

Квалификация организованной киберпреступности осложняется тем, что одно фактическое поведение часто затрагивает несколько уголовно-правовых запретов. Уже на базовом уровне возникает вопрос о соотношении преступлений против собственности и преступлений в сфере компьютерной информации. Если неправомерный доступ к системе используется лишь как способ последующего хищения денежных средств, возможны конкуренция либо совокупность норм об имущественном посягательстве и деяниях, предусмотренных гл. 28 УК РФ. Автоматическое поглощение одного состава другим неправильно. Необходимо выяснять, имел ли неправомерный доступ самостоятельное уголовно-правовое значение, причинял ли он дополнительный вред охраняемым отношениям в сфере конфиденциальности, целостности и доступности компьютерной информации либо выступал исключительно технической стадией хищения.

На практике наиболее проблемными являются три блока.

Первый связан с разграничением кражи, мошенничества и специальных мошеннических составов. В цифровой среде потерпевший нередко сам совершает перевод под воздействием обмана, но содержание обмана может быть опосредовано взломом аккаунта, подменой номера, использованием поддельного интерфейса банка или мессенджера. В таких ситуациях принципиально установить, кто совершил распоряжение имуществом: сам потерпевший вследствие обмана либо виновный через несанкционированный доступ к счету, устройству или средству платежа. Если денежные средства списываются без реального волеизъявления потерпевшего, квалификация по правилам хищения путем кражи оказывается более обоснованной. Если же перевод произведен самим потерпевшим под воздействием обмана, в том числе посредством социальной инженерии, речь идет о мошенничестве, а при использовании электронных средств платежа следует учитывать разъяснения судебной практики по соответствующим специальным составам [Вольдимарова, 2018].

Второй блок касается соотношения мошенничества в сфере компьютерной информации и «традиционного» мошенничества. Ошибка правоприменения часто состоит в том, что любой эпизод, где фигурирует интернет, автоматически квалифицируется по ст. 159.6 УК РФ. Между тем ключевое значение имеет механизм причинения ущерба. Если обман адресован прежде всего человеку и именно его заблуждение порождает перевод денежных средств, то цифровая

среда выступает каналом коммуникации, но не самостоятельным способом вмешательства в обработку компьютерной информации. Если же хищение достигается путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи данных, основания для применения ст. 159.6 УК РФ существенно усиливаются.

Третий блок связан с многоэпизодностью и трансграничностью. Организованные кибергруппы нередко строят деятельность как непрерывный поток однотипных действий: создают набор фишинговых страниц, закупают трафик, обзванивают потерпевших, используют сотни банковских карт и аккаунтов, а затем распределяют доход. Возникает вопрос: следует ли квалифицировать такое поведение как продолжаемое преступление, совокупность преступлений либо серию эпизодов, объединенных деятельностью организованной группы. Универсального решения здесь нет. Если каждый эпизод имеет самостоятельного потерпевшего, отдельный предмет посягательства и самостоятельный момент окончания, основания для совокупности сохраняются. Но при этом сама устойчивость схемы, общность инфраструктуры и единство организующего центра должны учитываться при квалификации по признакам совершения деяния организованной группой, а в исключительных случаях – при решении вопроса о преступном сообществе.

Отдельную сложность вызывает обращение с вредоносным ПО, бот-сетями и средствами удаленного доступа. Создание, приобретение и распространение такого инструментария могут образовывать самостоятельные составы преступлений в сфере компьютерной информации, но в рамках организованной схемы они нередко выступают стадией подготовки к хищениям, вымогательству, неправомерному доступу либо нарушению работы информационных систем. Поэтому квалификация должна учитывать не только факт использования программы, но и ее функциональную роль в общем преступном плане. Если вредоносный инструмент создается специально под атаку на конкретную категорию потерпевших и встроен в устойчивую схему распределения ролей, его нельзя рассматривать как нейтральный технический ресурс.

Не менее дискуссионен вопрос о «дропах». Формально их участие часто сводится к предоставлению банковской карты, счета, SIM-карты или учетной записи [Сорокин, 2024] Однако уголовно-правовая оценка зависит от доказанности умысла. Лицо, сознательно вовлекаемое в схему вывода похищенных средств, может выступать пособником, а при устойчивом участии и осознании общего плана – осоисполнителем в функциональном смысле либо членом организованной группы. Напротив, номинальный держатель счета, введенный в заблуждение относительно характера операций, не должен автоматически криминализироваться как участник хищения. В этой части практике недостает единых критериев оценки осведомленности и степени вовлеченности.

Именно институт соучастия наиболее остро испытывает воздействие цифровой среды. Классическая модель, в которой исполнитель непосредственно совершает объективную сторону, а остальные лица лишь содействуют, в ряде киберпреступлений оказывается недостаточной. Преступный результат здесь нередко достигается совокупностью технических, коммуникативных и финансовых действий, ни одно из которых по отдельности не исчерпывает всей объективной стороны [Ващенко, 2022]. Поэтому при квалификации целесообразно исходить из функционального понимания совместного исполнения.

Исполнителем в распределенной цифровой схеме может быть не только лицо, непосредственно нажимающее кнопку перевода или отправляющее команду на заражение системы, но и участник, без действий которого реализация общего плана в конкретном эпизоде была бы невозможна. Например, оператор, который в режиме реального времени убеждает

потерпевшего назвать код подтверждения либо перевести денежные средства, фактически реализует ключевую часть механизма хищения. Администратор панели, распределяющий доступы и лимиты, в ряде случаев не менее значим для наступления результата, чем «линейный» обзвонщик. Соответственно, разграничение исполнителя и пособника должно строиться не формально-технически, а с учетом вклада лица в причинение преступного результата.

Организатор в киберсреде, как правило, характеризуется не физическим руководством на месте совершения преступления, а контролем над инфраструктурой и денежными потоками. Признаками такой роли могут служить создание устойчивой схемы, подбор участников, распределение функций, определение целевых категорий жертв, установление правил конспирации, централизованное распоряжение базами данных, ботами, кошельками, доменами и доходом от преступной деятельности [Мосечкин, 2022]. Для цифровых дел это особенно важно, поскольку организатор нередко максимально дистанцирован от непосредственного контакта с потерпевшими и потому ошибочно воспринимается как второстепенный участник.

Пособничество также приобретает новые формы. Оно может выражаться в предоставлении вредоносного кода, арендованной инфраструктуры, услуг анонимизации, готовых фишинговых шаблонов, баз номеров телефонов, поддельных аккаунтов, каналов вывода средств. Однако вменение пособничества допустимо только при наличии доказательств, что лицо осознавало преступное назначение предоставляемого ресурса и желало либо сознательно допускало его использование для совершения конкретного преступления или серии преступлений. Именно здесь проходит граница между уголовно наказуемым содействием и формально нейтральным предоставлением сервиса.

Подстрекательство в цифровых схемах встречается реже в «чистом» виде, но не исчезает. Вербовка несовершеннолетних в качестве «дропов», склонение лиц к регистрации счетов и аккаунтов, предложение «легкого заработка» через прием и дальнейший перевод денежных средств, обучение сценариям общения с потерпевшими – все это может рассматриваться как склонение к участию в преступной деятельности. При этом цифровая форма коммуникации не снижает общественную опасность, а часто, напротив, облегчает массовую и анонимную вербовку.

Участники одной схемы нередко знают не весь план, а только свой сегмент. Но это не исключает соучастия, если доказано, что лицо осознавало преступный характер общей деятельности и понимало, что действует в составе координируемой цепочки. Для организованных кибергрупп типично именно частичное знание общей картины: один участник может не знать личность организатора, но понимать, что обеспечивает вывод средств, похищаемых у потерпевших через кол-центр; другой может не знать конкретных жертв, но осознавать, что предоставляет доступ к инфраструктуре для совершения хищений. Следовательно, критически важно доказывать не полноту знаний о каждой детали, а осведомленность о преступной направленности общего механизма.

УПК РФ не закрепляет электронные доказательства в качестве самостоятельного вида доказательств; цифровые данные в практике распределяются между вещественными доказательствами, иными документами, заключениями экспертов, протоколами следственных действий и приложениями к ним Такая конструкция формально работоспособна, но в делах об организованной киберпреступности создает значительные трудности. Цифровой след изменяем, копируем, удаляем, может храниться одновременно в нескольких юрисдикциях и в нескольких версиях, а потому вопрос о его происхождении, целостности и неизменности становится центральным.

Нормы УПК РФ позволяют производить осмотр устройств, изымать электронные носители,

получать сведения о соединениях и иных данных, однако в реальной практике качество фиксации существенно колеблется. Нередко в протоколах описывается лишь внешний вид устройства без надлежащего отражения версии программного обеспечения, состояния сессий, сетевых подключений, временных меток, хэш-значений копий, последовательности действий следователя и специалиста. Между тем именно такие детали позволяют в дальнейшем исключить сомнения в достоверности и неизменности цифрового материала.

Также следует отметить, что совпадение IP-адреса, номера телефона, аккаунта мессенджера, электронной почты, устройства и банковского счета не тождественно безусловному установлению личности виновного. Организованные группы сознательно строят схемы маскировки: используют VPN, удаленные рабочие столы, «одноразовые» аккаунты, чужие SIM-карты, арендованные устройства, цепочки «дропов» и криптовалютные миксеры [Марсаков, 2025] Поэтому доказательственное значение отдельного цифрового следа почти всегда ограничено; необходима конвергенция данных из разных источников – ологов, переписки, банковских транзакций, геолокации, сведений о доступе к аккаунтам, видеофиксации банкоматов, данных операторов связи, результатов компьютерно-технических и финансово-аналитических исследований.

Для дел об организованной киберпреступности недостаточно доказать, что конкретное лицо имело доступ к тому или иному устройству либо аккаунту. Необходимо показать, что оно понимало преступную направленность деятельности и выполняло в ней определенную функцию. Здесь особую ценность приобретают внутренние переписки участников, инструкции по работе с жертвами, таблицы учета, распределение процентов, данные о тестировании фишинговых страниц, правила вывода средств, обучающие материалы для «операторов» и «дропов». Именно они позволяют перейти от технической связки к доказанности совместного умысла.

Отдельная проблема связана с допустимостью цифровых доказательств, полученных от частных субъектов: банков, операторов связи, владельцев платформ, служб информационной безопасности, коммерческих центров мониторинга. С одной стороны, без этих данных расследование зачастую невозможно. С другой – необходимо соблюдать процессуальные формы их получения и проверки, исключая подмену следственного доказывания частной аналитикой. Частные отчеты могут служить ориентиром для следствия, но доказательственную силу в уголовном деле приобретают лишь после надлежащего процессуального оформления и проверки.

Из этого следует, что доказывание по делам об организованной киберпреступности должно строиться по модели «цепочки цифрового события». Она включает: происхождение данных; способ их извлечения и копирования; подтверждение неизменности; связь с конкретным устройством, аккаунтом и лицом; место цифрового следа в общей структуре преступной схемы; сопоставление с финансовыми и коммуникативными данными; объяснение роли участника в достижении преступного результата. Без такой цепочки даже большой массив электронных сведений легко распадается на набор вероятностных предположений.

Заключение

Сложившаяся ситуация не требует радикального отказа от действующих уголовно-правовых конструкций, но настоятельно требует их уточняющего толкования и более современной процессуальной инфраструктуры.

Применительно к организованной киберпреступности следует развивать функциональный

подход к признакам организованной группы и преступного сообщества. Для судебной практики целесообразно прямо разъяснить, что устойчивость и согласованность могут подтверждаться постоянством цифровой инфраструктуры, централизованным администрированием, устойчивым распределением ролей, едиными каналами финансирования и конспирации, даже если участники территориально разобщены и не знакомы лично. Такое разъяснение сократило бы число ситуаций, когда высокоорганизованная цифровая схема искусственно редуцируется до «группы лиц по предварительному сговору» лишь потому, что следствие не может показать очное взаимодействие участников.

Также необходимы более четкие ориентиры для разграничения исполнителя, соисполнителя и пособника в распределенных цифровых схемах. Представляется обоснованным исходить из следующего критерия: лицо должно признаваться соисполнителем, если его действия образуют функционально необходимый сегмент объективной стороны конкретного преступления, а не только создают условия для него. Предоставление же инфраструктуры, данных или финансового канала без участия в реализации конкретного эпизода при наличии осознания преступной цели должно оцениваться как пособничество.

Необходимы более точные подходы к оценке осведомленности «дропов» и иных периферийных участников. Простая фиксация поступления и перевода денежных средств еще не доказывает умысла на участие в хищении. Однако устойчивое участие, аномальный характер транзакций, использование нескольких карт и счетов, заранее согласованное вознаграждение, конспиративные инструкции, ложные объяснения источника средств и наличие связи с иными участниками могут образовывать совокупность признаков сознательного пособничества. Правоприменение должно опираться именно на совокупную оценку, а не на одну формальную деталь.

Библиография

1. Ахатова А. М. Уголовно-правовые признаки организованной группы в преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей // Образование. Наука. Научные кадры. 2026. № 1. С. 117–122.
2. Более 7 тыс. детей вовлекли в мошеннические схемы в 2025 году // Коммерсантъ. – URL: https://www.kommersant.ru/doc/8535164 .
3. Ващенко Т. В. Введение в международный финансовый менеджмент. М.: Проспект, 2022. 128 с.
4. Вольдимарова Н. Г. Уголовно-правовые средства противодействия экономическим угрозам в сфере кредитования // Право и образование. 2018. № 8. С. 102–107.
5. Данилова М. А. Digital-CPTED: теоретико-криминологические основы предупреждения преступности в цифровой среде // Современная наука: актуальные проблемы теории и практики. 2026. № 03. С. 90–94.
6. Марсаков И. С. Оперативно-розыскное противодействие обнальным площадкам XXI века // Вестник Казанского юридического института МВД России. 2025. Т. 16, № 2(60). С. 123–132.
7. Мосечкин И. Н. Уголовная ответственность за организацию устойчивой группы лиц, созданной для совершения преступлений в сфере компьютерной информации // Вестник Санкт-Петербургского университета. Право. 2022. Т. 13, № 1. С. 28–45.
8. Семенцова И. А., Малявина А. Б. Цифровая преступность как угроза национальной безопасности в Российской Федерации // Искусственный и естественный интеллект: алгоритмы, мышление и образовательные технологии : Материалы XXI международного конгресса с элементами научной школы для молодых ученых, Москва, 27–28 марта 2025 года. М.: Московский университет им. С. Ю. Витте, 2025. С. 1294–1302.
9. Сорокин М. Б. Дропперы как новый вид финансовых мошенников // Виттевские чтения – 2024 : Материалы XXIV международного Конгресса молодой науки, Москва, 26 апреля 2024 года. М.: Московский университет им. С. Ю. Витте, 2024. С. 1475–1478.
10. Состояние преступности // МВД РФ. – URL: https://xn--b1aew.xn--p1ai/reports/ .

Modern Forms of Organized Cybercrime: Criminal-Legal Problems of Qualification, Complicity, and Proving

Elnur R. Salmanov

Postgraduate Student,
All-Russian State University of Justice
(RPA of the Ministry of Justice of Russia),
117638, 2, bld. 1, Azovskaya str., Moscow, Russian Federation;
e-mail: elnur.s.00@mail.ru

Abstract

Organized cybercrime in recent years has transformed from a set of disparate episodes of unlawful access, theft, and fraudulent actions into a stable segment of criminal activity based on digital infrastructure, functional division of roles, and the cross-border nature of participant interaction. Russian statistics for 2021–2026 record not only a significant increase in the number of registered IT crimes but also the complication of their methods, the involvement of legal platforms, payment services, crypto-assets, as well as the expansion of social engineering practices. This article formulates a conclusion on the need to prove both the fact of technological interaction and the criminal integration of functions, manifested through the regularity of communication, the distribution of financial flows, a common pool of resources, rules of conspiracy, centralized management, the repeatability of scenarios, and the conscious participation of persons in the creation or maintenance of criminal infrastructure. Thus, proving in cases of organized cybercrime should be built according to the "digital event chain" model.

For citation

Salmanov E.R. (2026) Sovremennye formy organizovannoy kiberprestupnosti: ugolovno-pravovye problemy kvalifikatsii, souchastiya i dokazyvaniya [Modern Forms of Organized Cybercrime: Criminal-Legal Problems of Qualification, Complicity, and Proving]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (4A), pp. 574-583. DOI: 10.34670/AR.2026.81.57.070

Keywords

Organized cybercrime, cybercrimes, complicity, organized group, criminal community, digital evidence, malicious software, crypto-assets, cross-border crime, criminal procedure.

References

1. Akhatova, A. M. (2026). Ugolovno-pravovye priznaki organizovannoy gruppy v prestupleniyakh, sovershaemykh s ispolzovaniem informatsionno-telekommunikatsionnykh setey [Criminal-legal signs of an organized group in crimes committed using information and telecommunication networks]. *Obrazovanie. Nauka. Nauchnye kadry*, 1, 117-122.
2. Bolee 7 tys. detey vovlekli v moshennicheskie skhemy v 2025 godu [More than 7 thousand children were involved in fraudulent schemes in 2025]. (2025). *Kommersant*. Retrieved from https://www.kommersant.ru/doc/8535164
3. Danilova, M. A. (2026). Digital-CPTED: teoretiko-kriminologicheskie osnovy preduprezhdeniya prestupnosti v tsifrovoy srede [Digital-CPTED: theoretical and criminological foundations of crime prevention in the digital environment]. *Sovremennaya nauka: aktualnye problemy teorii i praktiki*, 03, 90-94.
4. Marsakov, I. S. (2025). Operativno-rozysknoe protivodeystvie obnalnym ploshchadkam XXI veka [Operational-search

counteraction to cash-out platforms of the 21st century]. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii*, 16(2), 123-132.

5. Mosechkin, I. N. (2022). Ugolovnaya otvetstvennost za organizatsiyu ustoychivoy gruppy lits, sozdannoy dlya soversheniya prestupleniy v sfere kompyuternoy informatsii [Criminal liability for organizing a stable group of persons created to commit crimes in the sphere of computer information]. *Vestnik Sankt-Peterburgskogo universiteta. Pravo*, 13(1), 28-45.
6. Sementsova, I. A., & Malyavina, A. B. (2025). Tsifrovaya prestupnost kak ugroza natsionalnoy bezopasnosti v Rossiyskoy Federatsii [Digital crime as a threat to national security in the Russian Federation]. In *Iskusstvennyy i estestvennyy intellekt: algoritmy, myshlenie i obrazovatelnye tekhnologii* (pp. 1294-1302). Moscow: Moscow University named after S. Yu. Witte.
7. Sorokin, M. B. (2024). Droppery kak novyy vid finansovykh moshennikov [Droppers as a new type of financial fraudsters]. In *Vittevskie chteniya - 2024* (pp. 1475-1478). Moscow: Moscow University named after S. Yu. Witte.
8. Sostoyanie prestupnosti [The state of crime]. (2026). *Ministry of Internal Affairs of the Russian Federation*. Retrieved from https://xn--b1aew.xn--p1ai/reports/
9. Vashchenko, T. V. (2022). *Vvedenie v mezhdunarodnyy finansovyy menedzhment* [Introduction to international financial management]. Moscow: Prospekt.
10. Voldimarova, N. G. (2018). Ugolovno-pravovye sredstva protivodeystviya ekonomicheskim ugrozam v sfere kreditovaniya [Criminal-legal means of countering economic threats in the field of lending]. *Pravo i obrazovanie*, 8, 102-107.