Рекомендации по противодействию использованию цифровых коммуникационных платформ организованной преступностью: задачи силовых ведомств, органов государственной безопасности и международного сотрудничества

Автор: Василий К.Исаул

Дата: 01.06.2026

Содержание

Кому адресована статья

Статья адресована **научному сообществу и практикам, работающим на стыке криминологии, уголовного права, информационного права, теории государства и права, цифровой криминалистики и государственного управления**, а также **сотрудникам правоохранительных органов, органов государственной безопасности, подразделений финансовой разведки, следствия, прокуратуры и международного полицейского сотрудничества**. Кроме того, она может быть полезна **разработчикам государственной политики, экспертам в сфере национальной безопасности, преподавателям и исследователям**, изучающим трансформацию организованной преступности в условиях цифровой платформенной среды.

Аннотация

В статье исследуется **организованная преступность в цифровых коммуникационных средах как сложное социально-правовое, инфраструктурное и управленческое явление**. Обосновывается, что цифровые платформы перестали быть нейтральными каналами передачи информации и превратились в **устойчивую среду существования, координации, маскировки и воспроизводства преступных сетей**. Показано, что современная преступность использует платформенную логику для вербовки, распределения ролей, сокрытия следов, финансового сопровождения, переноса аудитории между каналами и быстрого восстановления после блокировок. Особое внимание уделено **стратегической постановке проблемы для силовых ведомств**, необходимости перехода от реактивного реагирования к **проактивному выявлению криминальных экосистем**, а также развитию межведомственных центров цифрового противодействия, цифровой разведки, криминального анализа, стандартизации цифровой доказательственной фиксации и риск-ориентированной модели приоритизации. Рассматриваются **подходы к использованию финансовой разведки, задачи органов государственной безопасности, вопросы международного сотрудничества, включая роль Интерпола, Европола, Управлением Организации Объединённых Наций по наркотикам и преступности и иных международных структур**, а также меры профилактики и информационно-правового воздействия. Делается вывод о том, что эффективное противодействие возможно только при условии **комплексного соединения правовых, организационных, аналитических, технических, профилактических и международных механизмов**, направленных не только на пресечение отдельных эпизодов, но и на разрушение самой инфраструктуры цифровой организованной преступности.

1. ВВЕДЕНИЕ

В начале XXI века стало окончательно очевидно: цифровые коммуникационные платформы более не могут рассматриваться как простые и нейтральные каналы передачи сообщений. Их общественная роль качественно изменилась. Они превратились в многоуровневые социально-технические среды, где одновременно сосуществуют повседневное общение, распространение общественно значимой информации, деловая координация, институциональное взаимодействие, неформальные горизонтальные связи и разнообразные формы противоправной деятельности. Тем самым складывается новая реальность, в которой преступность не просто использует технические средства для совершения отдельных деяний, а встраивается в саму ткань цифрового общения, адаптируется к логике платформенной организации и извлекает выгоду из архитектуры современной информационной среды. **Именно здесь проходит одна из важнейших линий современного противостояния между публичной властью, правопорядком и организованной преступностью**.

Проблема, таким образом, заключается не в самом факте присутствия противоправного контента или преступных коммуникаций в цифровой среде, а в гораздо более глубоком явлении: цифровые платформы становятся устойчивой инфраструктурой криминальной деятельности. Организованные преступные сообщества используют их не случайно, не вспомогательно и не в режиме разовых контактов, а как долговременную, гибкую и постоянно воспроизводимую среду для поиска исполнителей, распределения ролей, маскировки намерений, поддержания дисциплины, расширения клиентской базы, легитимации незаконного предложения в глазах массовой аудитории и оперативного восстановления нарушенных каналов взаимодействия. **Платформа в этих условиях выступает уже не как внешний инструмент, а как среда существования преступной сети**. Это обстоятельство требует принципиального пересмотра как научных представлений о цифровой преступности, так и практических подходов государства к ее предупреждению, выявлению и пресечению.

Следует подчеркнуть, что современная организованная преступность все чаще отказывается от прежней логики пространственной изоляции, конспиративной замкнутости и опоры исключительно на труднодоступные участки сети. Напротив, значительная часть преступной активности перемещается в те цифровые пространства, которые встроены в повседневную жизнь миллионов граждан. Такая трансформация имеет далеко идущие последствия. Во-первых, исчезает прежняя символическая дистанция между «обычным» пользователем и криминальной средой: противоправное предложение начинает восприниматься как одно из многочисленных сообщений в общем информационном потоке. Во-вторых, снижается психологический барьер вхождения в незаконные практики, поскольку коммуникация с потенциальным вербовщиком, посредником

или распространителем приобретает форму привычного и технологически упрощенного взаимодействия. В-третьих, создаются условия для постепенной нормализации преступных моделей поведения, когда незаконное действие теряет в общественном восприятии ореол исключительности и начинает маскироваться под разновидность «обычной» цифровой активности. **Опасность состоит не только в сокрытии преступности, но и в ее повседневизации**.

Существенным фактором роста данной угрозы является сочетание нескольких свойств современных цифровых платформ. К их числу относятся высокая скорость распространения сведений, низкие издержки создания и тиражирования информационных материалов, относительная простота доступа к широкой аудитории, техническая возможность использования закрытых сообществ и псевдонимных учетных записей, а также слабая прозрачность внутренних процедур управления информационными потоками. В результате преступные структуры получают уникальное преимущество: они могут быстро перестраивать маршруты связи, масштабировать свое присутствие, тестировать способы воздействия на различные аудитории и с минимальными затратами воспроизводить разрушенные правоохранительными органами каналы. Удаление отдельных учетных записей, сообществ или информационных материалов в подобных условиях само по себе еще не означает разрушения преступной сети. Напротив, нередко оно лишь побуждает ее к более сложной адаптации, рассредоточению и переходу к новым формам маскировки. **Цифровая среда предоставляет организованной преступности не только средство связи, но и режим постоянной адаптивной устойчивости**.

Научная значимость рассматриваемой проблемы определяется тем, что она находится на пересечении нескольких крупных исследовательских направлений: криминологии, уголовного права, теории государства и права, информационного права, социологии коммуникаций, теории управления, судебной экспертизы цифровых следов и практики обеспечения национальной безопасности. Организованная преступность в цифровой среде не укладывается в традиционные схемы изучения, поскольку соединяет в себе черты сетевой структуры, высокой распределенности, функциональной гибкости и трансграничности. Ее участники могут находиться в различных государствах, пользоваться разными правовыми режимами, разделять между собой этапы противоправной деятельности и при этом сохранять организационное единство через устойчивые цифровые каналы. В этих условиях классические модели расследования, построенные вокруг локализованного места совершения деяния, ограниченного круга участников и материально фиксируемых следов, сталкиваются с серьезными пределами применимости. **Перед наукой стоит задача описать не отдельный цифровой**

эпизод, а целостную инфраструктурную логику современной преступности.

Особое внимание необходимо обратить на то обстоятельство, что цифровые платформы создают благоприятную среду для совмещения различных этапов преступной деятельности в едином коммуникационном контуре. Там, где ранее подготовка, реклама, поиск исполнителей, передача инструкций, распределение прибыли, психологическое давление и контроль исполнения могли быть разведены по времени, пространству и каналам связи, теперь они нередко объединяются в одном цифровом пространстве. Это обеспечивает беспрецедентную скорость управленческого цикла внутри преступной сети. Решения принимаются быстрее, связи между организаторами и исполнителями становятся плотнее, а управленческая дистанция между центром и периферией сокращается. Более того, сама цифровая среда способствует формированию новых типов преступной дисциплины: участник сообщества может находиться под постоянным информационным воздействием, получать регулярные указания, отчитываться о выполнении задач, подвергаться внутреннему контролю и санкциям. **Организованная преступность в цифровой среде все в большей степени приобретает черты непрерывно действующей управляемой системы**.

Не менее важен и социальный аспект проблемы. Цифровые платформы, будучи пространствами массового пребывания граждан, становятся ареной борьбы не только за информацию, но и за нормы, представления, допустимость тех или иных практик. Преступные сообщества стремятся не просто скрыться, а встроиться в окружающую среду, мимикрировать под законную активность, использовать язык повседневности, приемы визуального и смыслового упрощения, доверительные формы обращения и механизмы групповой идентификации. Это делает противоправное воздействие особенно опасным для молодежи, социально уязвимых групп, лиц с низким уровнем правовой культуры и граждан, находящихся в состоянии экономической или психологической нестабильности. Вовлечение в преступную деятельность в таких условиях может осуществляться постепенно, через последовательную деформацию восприятия: от простого наблюдения за незаконным предложением - к его допущению, от допущения - к пробному участию, от участия - к устойчивой криминальной включенности. **Цифровая среда превращает вербовку из исключительного акта в растянутый и технологически сопровождаемый процесс социального переформатирования личности**.

Именно поэтому противодействие организованной преступности в цифровых коммуникационных средах не может ограничиваться уголовно-правовым реагированием на уже совершенные деяния. Репрессивный механизм остается необходимым, но его явно недостаточно. Если государство ограничивается только расследованием отдельных эпизодов и

наказанием установленных исполнителей, оно неизбежно действует с опозданием, реагируя на последствия, а не на механизмы воспроизводства угрозы. Между тем сама природа цифровой преступной среды требует иного подхода - системного, опережающего, межведомственного, научно обоснованного и технологически оснащенного. Такой подход должен включать профилактику, криминологическое прогнозирование, постоянное аналитическое сопровождение, развитие цифровой разведки, совершенствование правового регулирования, укрепление международного сотрудничества, формирование единых стандартов обмена сведениями и создание механизмов быстрого межгосударственного реагирования. **Только соединение правовых, организационных, технических и профилактических мер способно нарушить инфраструктурную устойчивость преступных сетей.**

При этом особую сложность представляет соотношение задач обеспечения безопасности и соблюдения прав и свобод человека. Цифровые платформы являются пространством реализации свободы общения, распространения информации, участия в общественной жизни и профессиональной деятельности. Следовательно, государственное вмешательство в эту сферу неизбежно затрагивает фундаментальные правовые ценности. Отсюда вытекает необходимость предельно точного, соразмерного и правомерного регулирования, способного одновременно защищать общество от криминального использования платформ и не превращать борьбу с преступностью в основание для произвольного ограничения законной коммуникации. Научный анализ должен, таким образом, учитывать не только эффективность правоохранительных механизмов, но и пределы допустимого вмешательства, гарантии судебного и ведомственного контроля, требования доказуемости, проверяемости и правовой определенности. **Сильное государство в цифровую эпоху - это не государство бесконтрольного наблюдения, а государство точного, законного и ответственного действия**.

Актуальность заявленной темы усиливается и международным измерением проблемы. Организованная преступность, действующая через цифровые платформы, почти всегда обладает трансграничным характером. Данные могут храниться в одной юрисдикции, организаторы находиться в другой, исполнители - в третьей, а потерпевшие - одновременно в десятках государств. Такое расслоение криминальной деятельности разрушает традиционные представления о территориальной привязке преступления и требует новых форм международного правового и институционального взаимодействия. Без согласованных процедур запроса, обмена сведениями, сохранения цифровых следов, идентификации участников, совместных расследований и признания электронных доказательств борьба с транснациональными преступными сетями неизбежно оказывается

фрагментарной. **Преступность давно научилась действовать поверх границ; право и государственное управление не вправе отставать**.

Следовательно, предметом научного анализа должно стать не только выявление отдельных форм использования цифровых платформ в преступных целях, но и исследование тех структурных условий, которые делают такое использование устойчивым, выгодным и трудно пресекаемым. Речь идет о необходимости рассмотреть цифровую платформу как особую институциональную среду, где пересекаются интересы пользователей, владельцев инфраструктуры, государственных органов, правоохранительных структур, международных институтов и преступных сообществ. В этой среде действуют собственные правила видимости, распространения сведений, группообразования, рейтингового усиления внимания, сегментации аудитории и воспроизводства доверия. Игнорирование этих закономерностей делает борьбу с организованной преступностью заведомо реактивной и недостаточно результативной. **Нельзя эффективно противостоять преступной сети, не понимая устройства той среды, которая обеспечивает ее жизнеспособность**.

Настоящее исследование исходит из того, что организованная преступность в цифровых коммуникационных средах должна рассматриваться как сложное социально-правовое и управленческое явление, требующее комплексного анализа. Необходимо установить, каким образом платформенная логика усиливает устойчивость преступных структур; какие именно функции цифровые среды выполняют в механизме криминальной организации; почему традиционные правоохранительные инструменты оказываются ограниченными; какие правовые, технологические и организационные изменения необходимы для адекватного ответа государства; каким образом должны сочетаться превентивные и репрессивные меры; и, наконец, как выстроить такую модель противодействия, которая будет одновременно эффективной, законной и соразмерной масштабу угрозы. **Вопрос стоит предельно ясно: либо государство научится действовать в логике цифровой эпохи, либо организованная преступность продолжит использовать ее преимущества быстрее и изощреннее публичной власти**.

Целью данного введения является обоснование необходимости перехода от фрагментарного восприятия отдельных цифровых преступных эпизодов к пониманию организованной преступности как сетевой, адаптивной и инфраструктурно укорененной формы криминальной деятельности. Исходя из этого, последующее изложение должно быть направлено на раскрытие механизмов функционирования преступных сообществ на цифровых платформах, анализ уязвимостей существующего правового и организационного реагирования, а также формулирование предложений по совершенствованию государственной политики в рассматриваемой сфере.

Научная и практическая задача состоит не просто в описании угрозы, а в выработке целостной модели ее сдерживания и разрушения.

2. СТРАТЕГИЧЕСКАЯ ПОСТАНОВКА ПРОБЛЕМЫ ДЛЯ СИЛОВЫХ ВЕДОМСТВ

Для правоохранительных органов и структур, обеспечивающих государственную безопасность, в настоящее время приобретает первостепенное значение **радикальный пересмотр самого предмета противодействия цифровой преступности**. Наиболее опасной методологической ошибкой остается представление о ней как о совокупности отдельных, слабо связанных между собой эпизодов: незаконного сбыта, мошеннического хищения, распространения запрещенных сведений, вербовки, легализации преступных доходов, координации насильственных действий или оборота поддельных документов. Подобный взгляд, при всей своей внешней удобности для ведомственного учета, уже не соответствует реальной картине происходящего. Он порождает ложное ощущение, будто каждое цифровое преступление существует изолированно, как автономный случай, требующий лишь частной правовой оценки и частного следственного реагирования. Между тем современная преступная среда в цифровом пространстве развивается не как сумма эпизодов, а как **устойчивая, самовоспроизводящаяся, приспосабливающаяся криминальная среда**, обладающая собственными правилами, внутренним разделением ролей, механизмами самозащиты и способностью к быстрому обновлению.

Именно поэтому стратегическая постановка проблемы должна исходить из признания того факта, что сегодня перед государством находятся не отдельные правонарушители, действующие случайно и бессистемно, а **цифровые криминальные экосистемы**. Это понятие требует особого внимания, поскольку оно отражает не метафору, а подлинную организационную природу современной преступности. Речь идет о таких совокупностях лиц, средств связи, способов сокрытия, каналов расчетов, методов воздействия на аудиторию и схем распределения функций, которые образуют целостную среду преступного существования. В этой среде одни участники производят незаконный продукт, другие обеспечивают его распространение, третьи поддерживают доверие к площадке, четвертые разрешают споры, пятые занимаются привлечением новых исполнителей, шестые отвечают за сокрытие следов, седьмые перераспределяют денежные потоки, а восьмые восстанавливают нарушенную инфраструктуру после внешнего воздействия. Следовательно, перед силовыми ведомствами находится не просто правонарушение как юридический факт, а **сложный социально-технический организм**, в котором отдельный преступный акт является лишь видимой частью значительно более глубокого процесса.

Принципиальное значение имеет то обстоятельство, что такие экосистемы обладают **распределенной структурой**. Это означает отсутствие единого центра, уничтожение которого автоматически повлекло бы разрушение всей противоправной сети. Организационная устойчивость достигается за счет рассредоточения ролей, дублирования каналов связи, использования множества учетных записей, распределения функций между администраторами, посредниками, техническими исполнителями, перевозчиками, вербовщиками, хранителями денежных средств и лицами, обеспечивающими информационное прикрытие. В условиях подобной структуры ликвидация одного участника или одного узла не разрушает систему в целом: на его место быстро встраивается другой элемент, а сама сеть продолжает функционировать, изменяя лишь форму внешнего проявления. Для силовых ведомств это означает, что **поиск формального организатора перестает быть достаточным условием успеха**, поскольку преступная среда способна существовать и после утраты отдельных координаторов.

Не менее существенным признаком является **высокая скорость восстановления после блокировок и пресечений**. Цифровая преступная среда давно освоила практику множественного резервирования. Удаление канала связи, закрытие одной площадки, ограничение доступа к определенному ресурсу или выявление отдельной группы участников не прекращает противоправную деятельность, а чаще всего переводит ее в иное пространство, на иную площадку, под иным обозначением и с новыми техническими параметрами. Такая среда заранее готовится к вмешательству государства: создаются запасные каналы оповещения, зеркальные ресурсы, скрытые способы уведомления аудитории, условные сигналы перехода, заранее распределенные перечни новых точек доступа. Отсюда вытекает важнейший практический вывод: **разовое ограничительное воздействие без последующего системного сопровождения нередко лишь фиксирует момент миграции, но не прекращает преступный процесс**. Более того, в ряде случаев блокировка одного видимого звена даже способствует дополнительной консолидации сообщества, которое начинает воспринимать себя как осажденную, но жизнеспособную среду, требующую еще большей закрытости и дисциплины.

Особую сложность создает **международный характер коммуникаций**, который разрушает привычные территориальные представления о преступлении. В цифровой среде организатор может находиться в одной стране, технический посредник - в другой, исполнитель - в третьей, пострадавший - в четвертой, а денежный след проходить через цепочку площадок и расчетных средств, находящихся вне юрисдикции каждого из названных государств. При этом коммуникация между участниками осуществляется непрерывно, быстро и нередко в рамках распределенных сообществ, участники которых никогда не встречались лично. Для

правоохранительных структур это означает, что **пространственная локализация преступления утрачивает прежнюю определенность**, а потому традиционные механизмы ведомственной и межгосударственной координации, построенные на сравнительно медленных процедурах запросов и согласований, оказываются запаздывающими по отношению к темпам преступной деятельности. Если государственная машина сохраняет инерционный ритм, а криминальная среда действует в ритме мгновенного перемещения и непрерывной перестройки, то преимущество неизбежно смещается в пользу преступника.

К числу важнейших опор устойчивости цифровой преступной среды относится и **использование псевдоанонимности**. Следует подчеркнуть, что речь идет не о полной неуязвимости правонарушителя, а о многослойном сокрытии его подлинного положения, которое затрудняет атрибуцию действий, усложняет связывание цифровых следов с конкретным лицом и увеличивает издержки расследования. Преступник последовательно дробит сведения о себе, меняет учетные обозначения, использует промежуточные средства связи, скрывает местоположение, прибегает к посредникам, техническим подменам и одноразовым средствам доступа. Тем самым он не исчезает для расследования окончательно, но стремится повысить цену своего обнаружения, сделать его трудоемким, длительным и заведомо менее эффективным. В стратегическом отношении это означает, что **государство сталкивается не просто с фактом сокрытия личности, а с индустрией управляемой неразличимости**, которая поставлена на поток и используется как стандартная мера преступной безопасности.

Серьезную роль играют и **репутационные механизмы**, которым долгое время уделялось недостаточное внимание. Ошибочно полагать, будто преступная среда держится только на страхе или прямой выгоде. Напротив, в цифровых криминальных сообществах активно формируются собственные системы доверия: отзывы, рейтинги, свидетельства надежности, подтверждения исполнения обязательств, санкции за обман, процедуры арбитража, правила допуска и символические признаки принадлежности к «проверенному» кругу. Эти механизмы имеют глубоко прагматический смысл. Они снижают внутреннюю неопределенность, уменьшают риск взаимного мошенничества внутри преступной среды, укрепляют лояльность участников и создают у новых лиц ложное ощущение упорядоченности и безопасности. Следовательно, для силовых ведомств **репутация в преступной среде должна рассматриваться как функциональный ресурс противоправной экономики**, а не как побочный социальный фон. Там, где поддерживается доверие между незнакомыми участниками, там создаются условия для масштабирования преступной деятельности.

Особого анализа заслуживает **сочетание открытых и закрытых контуров взаимодействия**. Современные преступные экосистемы редко существуют

только в полностью скрытом виде. Напротив, они используют открытую видимость как оболочку для сокрытия глубинных уровней организации. Наружный контур может маскироваться под новостное обсуждение, бытовое общение, консультационную деятельность, коммерческое посредничество, культурные интересы, развлекательное общение или взаимопомощь. Через этот внешний слой осуществляется первичное привлечение внимания, отбор заинтересованных лиц, формирование доверия и постепенное вовлечение в более закрытые формы коммуникации. Уже затем участник переводится в специальные каналы, закрытые группы, личные контакты, технически изолированные пространства или временные цепочки связи. В результате **открытое и скрытое здесь не противопоставлены, а функционально соединены**: открытость служит входом, закрытость - механизмом защиты, а переход между ними становится частью преступной технологии.

Не менее опасной чертой является **быстрый перенос аудитории между каналами, чатами, ботами и зеркальными ресурсами**. Для современной цифровой преступности аудитория - это не случайная совокупность наблюдателей, а стратегический актив. Именно поэтому преступные группы заблаговременно выстраивают способы ее удержания и мгновенного перемещения. Пользователю внушается необходимость следить за запасными точками доступа, сохранять резервные обозначения, пользоваться альтернативными маршрутами входа, доверять определенным оповещениям и в случае блокировки немедленно переходить в новую среду. С точки зрения силовых ведомств здесь имеет значение не только техническая сторона вопроса, но и **социальная управляемость аудитории**, ее дисциплина, привычка к подчинению внутренним сигналам и готовность следовать за координаторами независимо от смены площадки. Там, где аудитория переносима, сама блокировка информационного носителя теряет решающее значение. Уничтожается оболочка, но сохраняется сообщество, а следовательно, сохраняется и возможность воспроизводства преступной активности.

К числу наиболее тревожных признаков относится **способность маскировать криминальную активность под обычную информационную, коммерческую или социальную коммуникацию**. Это обстоятельство имеет не только тактическое, но и глубокое стратегическое значение. Преступная среда сознательно растворяет противоправные сигналы в массиве внешне законной повседневности. Незаконные предложения могут выглядеть как частные объявления, вербовочные действия - как приглашение к заработку, координация преступления - как бытовое обсуждение, передача указаний - как нейтральная переписка, а распределение ролей - как обычное деловое взаимодействие. Подобная мимикрия преследует сразу несколько целей: снизить вероятность автоматического выявления, усложнить правовую оценку содержания сообщения, затруднить доказательство умысла, а также

обеспечить психологическое привыкание аудитории к присутствию криминального элемента. Отсюда вытекает важнейший для правоохранительной практики вывод: **современная цифровая преступность стремится не только скрываться, но и нормализовать свое присутствие**, вписывая себя в ткань повседневной коммуникации так, чтобы противоправное воспринималось как привычное, технически нейтральное и социально терпимое.

Все перечисленное приводит к фундаментальному выводу: **объектом противодействия должен становиться не только отдельный противоправный материал, не только единичный исполнитель и не только конкретный эпизод, но вся инфраструктура производства, распространения, сопровождения и воспроизводства преступной деятельности**. Иначе говоря, если государство ограничивается удалением отдельных сообщений, задержанием отдельных курьеров, блокировкой отдельных страниц или пресечением отдельных финансовых операций, не разрушая при этом механизмы кадрового пополнения, доверительного обмена, координации, маршрутизации денежных потоков, распределения заданий и восстановления нарушенных связей, то оно наносит удар по поверхности, а не по основанию. Такое реагирование может быть необходимым, но само по себе оно недостаточно. В стратегическом плане борьба с цифровой преступностью должна быть направлена на **разрыв воспроизводящего цикла**, в котором преступная деятельность не просто осуществляется, а вновь и вновь порождает условия для собственного продолжения.

Отсюда непосредственно вытекает требование **перехода от реактивной модели к проактивной**. Реактивная модель строится на логике последующего ответа: преступление совершено, следствие начато, доказательства собираются, лица устанавливаются, процессуальные меры применяются. Эта логика сохраняет свое значение и не может быть отменена, однако в условиях цифровой криминальной среды она оказывается стратегически запаздывающей. Государство, которое неизменно приходит после завершения преступного акта, фактически уступает инициативу противнику. Напротив, проактивная модель предполагает смещение внимания на ранние признаки формирования угрозы: появление устойчивых криминогенных узоров поведения, повторяющихся способов вовлечения, признаков скрытой координации, необычных миграций аудитории, связок между информационной активностью и денежными перемещениями, а также повторяемости определенных ролевых схем. Это означает, что силовые ведомства должны быть способны **видеть не только уже совершенное, но и еще складывающееся**.

В практическом смысле такая постановка вопроса требует, прежде всего, выявления **криминогенных паттернов**, то есть устойчиво повторяющихся

конфигураций действий, сообщений, переходов и связей, указывающих на формирование противоправного процесса. Речь идет не о произвольном подозрении и не о расширительном толковании повседневного поведения граждан, а о научно обоснованном выделении типовых признаков преступной организации цифровой среды. Для одних видов преступности определяющим может быть повторение вербовочных формул и последовательности перевода лица из открытого общения в закрытый контур; для других - сочетание информационного предложения с быстрым финансовым сопровождением; для третьих - регулярное появление одних и тех же посредников, обслуживающих разные внешне несвязанные эпизоды. Значение имеет именно повторяемость, структурная сходность и функциональная связанность признаков. **Там, где повторяется схема, нередко уже действует не случайность, а система**.

Наряду с этим необходим поиск **узлов координации**, то есть тех точек, где пересекаются потоки указаний, распределения ролей, разрешения внутренних споров, обновления правил доступа, подтверждения надежности участников и перераспределения ресурсов. Следует подчеркнуть, что такие узлы не всегда совпадают с формальным организатором. Нередко центральная фигура скрыта или вообще рассредоточена, тогда как реальное управление осуществляется через совокупность посреднических центров: технических, финансовых, информационных, кадровых. В одном случае ключевым оказывается лицо, которое не совершает основного преступного действия, но обеспечивает допуск новых участников. В другом - посредник, поддерживающий доверие и расчеты. В третьем - администратор, который не прикасается к незаконному продукту, но связывает производителей, распространителей и исполнителей. Следовательно, **узел координации - это не обязательно вершина иерархии; это точка, потеря которой болезненна для всей сети**.

Столь же важным направлением становится выявление **механизмов вербовки**, поскольку именно через них цифровая преступная среда превращает случайного наблюдателя в участника, затем в исполнителя, а иногда и в убежденного носителя преступной нормы. Вербовка в цифровом пространстве редко имеет грубый и прямолинейный характер. Гораздо чаще она строится на постепенном втягивании: сначала человеку предлагают безобидное взаимодействие, затем демонстрируют легкость заработка, затем нормализуют риск, затем подменяют правовую оценку бытовыми оправданиями, затем включают его в малую группу, где срабатывает психологическое давление принадлежности. В дальнейшем следуют испытательные поручения, частичные обязательства, накопление взаимных компрометирующих сведений и превращение исполнителя в зависимое звено. Для государства понимание этих стадий чрезвычайно важно, поскольку **эффективное предупреждение начинается не на этапе**

завершенного вовлечения, а на этапе первых признаков преступного подбора и психологической обработки.

Особое место занимает анализ **цифровых маршрутов движения незаконных услуг, денежных средств, сведений и исполнителей**. Современная преступность существует как движение: от предложения к контакту, от контакта к соглашению, от соглашения к расчету, от расчета к исполнению, от исполнения к сокрытию следов, от сокрытия к восстановлению канала. Каждый из этих переходов оставляет следы не обязательно в форме прямого признания, но в форме последовательности действий, повторяющихся связей, временных совпадений, аномальных перемещений и функционально сопряженных событий. Задача силовых ведомств состоит не только в фиксации конечного результата, но и в реконструкции цепи движения. **Маршрут преступления нередко важнее его отдельной точки**, потому что именно в маршруте проявляются посредники, резервные звенья, уязвимые места и скрытые центры обслуживания.

Все сказанное подводит к необходимости нового институционального взгляда. Силовые ведомства должны рассматривать цифровую преступность не как периферийное приложение к традиционным формам противоправной деятельности, а как **среду, в которой заново организуются старые и рождаются новые формы криминального поведения**. В этой среде изменяется не только способ совершения преступления, но и логика преступной устойчивости, масштабирования и самосохранения. Именно поэтому успешное противодействие невозможно без соединения правового анализа, криминологии, теории организации, социальной психологии, лингвистического исследования коммуникации, изучения сетевых связей и постоянного межведомственного взаимодействия. Требуется не частичное приспособление старых методов к новым условиям, а **формирование полноценной стратегии опережающего государственного присутствия в цифровом пространстве**.

Итак, стратегическая постановка проблемы для силовых ведомств должна исходить из нескольких непреложных положений. **Во-первых**, цифровая преступность - это не совокупность отдельных инцидентов, а сложная экосистема, обладающая способностью к самоорганизации, миграции и воспроизводству. **Во-вторых**, ее устойчивость обеспечивается распределенностью, скоростью восстановления, международностью связей, псевдоанонимностью, внутренними механизмами доверия, соединением открытых и закрытых контуров, переносимостью аудитории и мимикрией под законную коммуникацию. **В-третьих**, подлинным объектом противодействия должна быть вся инфраструктура преступного существования, а не только отдельные проявления. **В-четвертых**, стратегический успех возможен лишь при переходе к проактивному выявлению криминогенных узоров, узлов координации, механизмов вербовки и маршрутов движения незаконных ресурсов. В этом и состоит

главная задача современного государства: **не догонять преступную среду после очередного эпизода, а лишать ее способности к организации, расширению и повторному рождению**.

3. РЕКОМЕНДАЦИИ ДЛЯ СИЛОВЫХ ВЕДОМСТВ

3.1. Создание специализированных межведомственных центров цифрового противодействия

В современных условиях преступность окончательно вышла за пределы привычного вещественного пространства и прочно закрепилась в цифровой среде, где скорость передачи сведений, анонимизация участников, разветвлённость каналов связи и трансграничный характер взаимодействий многократно усиливают устойчивость криминальных образований. Именно здесь сегодня формируются преступные замыслы, осуществляется вербовка, координируются противоправные действия, распределяются роли, легализуются преступные доходы, уничтожаются следы и ведётся постоянная работа по уклонению от государственного контроля. При этом особую опасность представляет не только сама техническая оснащённость преступных сетей, но и их организационная гибкость: они действуют быстро, децентрализованно, скрытно и способны молниеносно адаптироваться к изменениям правоохранительной практики. В этой ситуации ведомственная разобщённость перестаёт быть просто административным недостатком - она превращается в прямой фактор уязвимости государства.

Поэтому создание постоянно действующих специализированных межведомственных центров цифрового противодействия должно рассматриваться не как факультативная организационная мера, а как необходимое условие обеспечения эффективности борьбы с современной преступностью. Подобные центры призваны соединить в единой институциональной конструкции те силы и средства, которые в разобщённом состоянии неизбежно теряют значительную часть своего потенциала. Речь идёт об объединении оперативных подразделений, подразделений по борьбе с преступностью в цифровой среде, структур, специализирующихся на противодействии организованной преступности, подразделений финансовой разведки, специалистов в области цифровой криминалистики, аналитиков открытых источников и социальных сред, экспертов по лингвистическому и поведенческому анализу, а также представителей прокуратуры и следственных органов. Только такое объединение позволяет преодолеть опасный разрыв между обнаружением признаков преступной активности, её аналитическим осмыслением, процессуальным закреплением доказательств и последующим судебным преследованием виновных лиц.

Смысл создания этих центров заключается не в механическом сосредоточении представителей различных ведомств в одном помещении и не в формальном учреждении очередной координационной структуры. **Их фундаментальная задача состоит в формировании единой системы быстрого реагирования, в которой оперативные, аналитические, технические и процессуальные ресурсы действуют как части одного государственного механизма.** Если такой механизм не создан, сведения, добытые одним подразделением, остаются недоступными для другого; следы преступной деятельности утрачиваются из-за промедления; цифровые доказательства не получают надлежащего закрепления; финансовые потоки выявляются с опозданием; международные запросы направляются тогда, когда преступные субъекты уже сменили используемые каналы связи, расчётные средства и идентификационные признаки. В результате государственная машина, обладая значительным набором сил и средств, действует медленнее и разрозненнее, чем преступные сети, для которых скорость давно стала главным ресурсом выживания.

Необходимо особо подчеркнуть, что специализированный межведомственный центр цифрового противодействия должен строиться на принципах постоянного, а не эпизодического взаимодействия. Практика показывает, что временные рабочие группы, создаваемые под конкретное дело или в ответ на уже развившийся кризис, не способны обеспечить устойчивое накопление компетенций, формирование единых методик, воспроизводимость аналитических решений и надёжность межведомственных информационных связей. **Только постоянно действующая структура способна превратить разрозненные профессиональные навыки в целостную систему государственного противодействия.** Постоянный режим работы позволяет не просто реагировать на уже совершённые преступления, но и вести упреждающее выявление угроз, наблюдать за трансформацией преступных моделей, отслеживать технологические новации в среде криминальных сообществ и заблаговременно подготавливать правовые, организационные и тактические ответы.

Состав такого центра должен определяться логикой самой цифровой преступности, которая носит сложный, многослойный и междисциплинарный характер. Оперативные подразделения необходимы для получения первичных сведений, документирования деятельности подозреваемых, проведения негласных мероприятий и практической реализации разрабатываемых материалов. Подразделения, специализирующиеся на противодействии преступности в цифровой среде, обеспечивают понимание технической архитектуры противоправной деятельности, способов сокрытия цифровых следов, механизмов анонимизации и особенностей функционирования распределённых

коммуникационных площадок. Подразделения по борьбе с организованной преступностью привносят в работу центра опыт выявления и пресечения устойчивых преступных сообществ, знания в области криминальной иерархии, распределения ролей, внутренних дисциплинарных механизмов и способов внешнего прикрытия незаконной деятельности. Финансовая разведка позволяет вскрывать движение преступных доходов, устанавливать схемы их рассеивания и маскировки, выявлять связь между цифровой активностью и материальной базой преступного сообщества.

Исключительно важна роль специалистов в области цифровой криминалистики. Именно они обеспечивают правильное обнаружение, изъятие, сохранение, исследование и интерпретацию цифровых следов, без чего даже наиболее ценные сведения рискуют утратить доказательственное значение. В условиях, когда преступники активно используют удалённые хранилища сведений, зашифрованные каналы связи, многослойные системы идентификации и способы автоматического уничтожения содержимого, ошибки на стадии технической фиксации могут оказаться необратимыми. **Цифровое доказательство хрупко: его легко утратить, исказить, оспорить, а потому профессионализм в этой области должен быть не вспомогательным, а системообразующим элементом всей межведомственной работы.**

Не меньшую значимость имеют аналитики открытых источников и социальных сред, а также специалисты по лингвистическому и поведенческому анализу. Их участие позволяет выходить за пределы чисто технического наблюдения и видеть в цифровом пространстве не набор разрозненных сообщений, а сложную среду коммуникативных сигналов, смысловых кодов, символических маркеров и поведенческих шаблонов. Преступные сообщества редко говорят о своих намерениях прямо; они используют жаргон, иносказания, намёки, устойчивые риторические формулы, групповые меметические конструкции, замещающие обозначения товаров, услуг и действий. Анализ таких элементов даёт возможность устанавливать истинное содержание коммуникации, выявлять степень вовлечённости участников, распознавать стадии подготовки преступления, отличать случайного наблюдателя от активного координатора. Более того, поведенческий анализ позволяет выявлять типичные сценарии цифровой конспирации, определять моменты смены тактики, фиксировать признаки внутригруппового напряжения, подготовки к перемещению активов или попытки срочно свернуть коммуникационную инфраструктуру.

Присутствие представителей прокуратуры и следственных органов в составе центра имеет принципиальное значение. Долгое время в правоохранительной практике сохранялась разрушительная модель, при которой оперативный материал и следственная перспектива существуют как бы в разных мирах: одни собирают сведения, не всегда соотнося их с

будущими требованиями доказывания, другие получают эти сведения поздно и в форме, не позволяющей полноценно ввести их в уголовное судопроизводство. **Между тем в борьбе с преступностью цифровой эпохи процессуальная безупречность должна сопровождать работу с самого начала, а не появляться постфактум в качестве запоздалого юридического оформления.** Участие следственных и надзорных представителей позволяет уже на ранней стадии определять допустимые пределы использования материалов, своевременно формулировать следственные версии, обеспечивать надлежащее оформление доказательств, вырабатывать стратегию их дальнейшего предъявления и минимизировать риск признания собранных данных недопустимыми.

Если говорить о функциональном предназначении подобных центров, то в первую очередь они должны осуществлять постоянный мониторинг цифровых площадок высокого риска. Под такими площадками следует понимать не только общеизвестные сетевые ресурсы, на которых выявляется противоправный контент, но и замкнутые коммуникационные среды, анонимные каналы взаимодействия, тематические сообщества, полулегальные торговые сегменты, распределённые площадки обмена сведениями, а также быстро возникающие и столь же быстро исчезающие цифровые пространства, предназначенные для рекрутирования участников, сбыта запрещённых предметов, организации мошеннических схем, распространения экстремистских материалов, координации насильственных акций и иных форм преступной деятельности. Мониторинг не должен сводиться к механическому наблюдению за содержанием сообщений. Он должен включать выявление динамики активности, установление ключевых коммуникаторов, отслеживание смены лексических кодов, определение пиков координации и переходов от пропагандистской риторики к практическим указаниям.

Вторым важнейшим направлением работы должно стать картирование криминальных сетей и связей. Здесь речь идёт о системном выявлении не только отдельных лиц, но и всей структуры отношений между ними: каналов связи, устойчивых ролей, узлов координации, посреднических фигур, связей между цифровыми идентификаторами и реальными субъектами, маршрутов движения средств, контактных контуров, используемых для вербовки, снабжения, оплаты и сокрытия преступной деятельности. **Современная организованная преступность сильна не отдельными участниками, а архитектурой связей.** Следовательно, и противодействие ей должно быть нацелено не столько на изолированное выявление отдельных исполнителей, сколько на вскрытие всей конфигурации сообщества, его функциональных центров, резервных каналов, опорных финансовых точек и международных сопряжений. Картирование преступных сетей даёт возможность перейти от

эпизодического реагирования к системному разрушению криминальной инфраструктуры.

Особого внимания заслуживает задача выявления типовых моделей цифровой конспирации. Преступность в цифровой среде давно выработала стандартные и вместе с тем постоянно обновляющиеся способы сокрытия своей деятельности. К ним относятся фрагментация общения между различными площадками, разделение ролей между носителями сведений, использование временных учётных записей, переход на кодовую лексику, маскировка преступных обсуждений под повседневное общение, применение удалённого управления, подмена географических и технических признаков присутствия, использование посредников для передачи указаний и средств, резкое изменение интенсивности коммуникации перед совершением преступления или после него, а также создание ложных информационных следов, направленных на дезориентацию правоохранительных органов. Задача центра заключается в том, чтобы не просто фиксировать такие приёмы постфактум, а создавать их классификации, выделять повторяющиеся закономерности, формировать признаки раннего распознавания и превращать их в практические ориентиры для оперативных и следственных подразделений. **Кто научится видеть конспирацию как систему, тот лишит преступную среду её главного преимущества - невидимости.**

Следующей ключевой функцией межведомственного центра должно быть сопровождение оперативных разработок. В отличие от разрозненной модели, при которой каждое подразделение ведёт лишь свой фрагмент работы, центр обеспечивает непрерывное аналитическое, техническое и процессуальное сопровождение разработки от момента первичного сигнала до стадии возбуждения дела, предъявления обвинения и, при необходимости, международного взаимодействия. Это означает, что любой поступающий материал должен немедленно включаться в межведомственный оборот, сопоставляться с уже имеющимися сведениями, проверяться по цифровым, финансовым и поведенческим индикаторам, оцениваться с точки зрения доказательственных перспектив и рисков утраты следов. Такая организация работы не позволяет преступным субъектам использовать межведомственные разрывы в качестве защитного пространства. Напротив, она создаёт эффект непрерывного преследования, при котором каждое новое проявление преступной активности мгновенно встраивается в общую картину.

Не менее важно накопление и стандартизация цифровых доказательств. Сегодня одной из наиболее болезненных проблем остаётся отсутствие единообразия в подходах к сбору, описанию, хранению, исследованию и представлению цифровых следов. В одних подразделениях применяются одни требования к фиксации содержимого, в других - иные; где-то ведётся тщательная регистрация последовательности действий с носителем, а где-

то подобные процедуры выполняются формально; одни специалисты подробно описывают среду обнаружения данных, другие ограничиваются общими формулировками. Подобная неоднородность подрывает доверие к доказательственной базе, усложняет межведомственный обмен, создаёт почву для процессуальных споров и судебного оспаривания. **Специализированный центр должен стать местом выработки единых стандартов обращения с цифровыми доказательствами, обязательных для всех вовлечённых структур.** Это касается порядка фиксации экранного содержимого, правил описания сетевой активности, способов документирования метаданных, процедур изъятия устройств, требований к обеспечению неизменности данных, условий хранения копий, регламента работы с удалёнными ресурсами и порядка экспертной интерпретации результатов исследования.

Существенное место в деятельности центра должна занимать подготовка материалов для международных запросов. Цифровая преступность не признаёт государственных границ, и это не метафора, а практическая реальность, ежедневно подтверждаемая расследованиями: серверные мощности могут находиться в одной стране, оператор преступной схемы - в другой, посредник по переводу средств - в третьей, а потерпевшие - в десятках государств одновременно. При такой конфигурации любое промедление в международном взаимодействии означает фактическую утрату шанса на эффективное расследование. Вместе с тем подготовка материалов для зарубежных партнёров требует высокой точности, полноты и правовой грамотности: необходимо ясно формулировать обстоятельства дела, конкретизировать искомые сведения, указывать их значение для расследования, соблюдать процедурные требования, учитывать различия правовых систем и особенности иностранной практики обращения с цифровыми данными. Центр, аккумулирующий оперативную, аналитическую и процессуальную компетентность, способен существенно повысить качество таких запросов и сократить время их подготовки. В условиях стремительной миграции цифровых следов именно скорость международного обращения становится решающим фактором.

Наконец, одной из наиболее значимых функций межведомственных центров должна стать выработка типовых методик расследования. Здесь открывается особое поле государственной ответственности. Пока каждое новое дело воспринимается как почти уникальное, правоохранительная система обречена вновь и вновь тратить силы на изобретение того, что давно должно быть переведено в форму устойчивых алгоритмов. Между тем типизация не означает огрубления реальности; напротив, она позволяет выделить устойчивые механизмы преступной деятельности, определить оптимальную последовательность действий, установить приоритеты изъятия данных, сформировать перечни первичных вопросов к специалистам, закрепить модели межведомственного взаимодействия,

выработать стандартные признаки угрозы и тем самым резко повысить качество и скорость расследования. **Методика в сфере цифрового противодействия - это не бюрократический документ, а концентрированное выражение накопленного профессионального опыта, превращённого в инструмент практической эффективности.**

Следует также отметить, что деятельность межведомственных центров не может быть полноценной без единой внутренней системы учёта, сопоставления и оценки сведений. Речь идёт не только о хранении материалов, но и о формировании интегрированного аналитического пространства, где цифровые следы, финансовые транзакции, данные о коммуникациях, поведенческие признаки, сведения открытых источников и процессуальные документы связываются в единую доказательственную и разведывательную картину. Такая система должна обеспечивать выявление скрытых связей, автоматизированное предупреждение о совпадении значимых признаков, быстрый доступ к ранее накопленным материалам, фиксацию хода межведомственной работы и возможность ретроспективного анализа уже завершённых дел с целью совершенствования практики. **Без памяти система слепа; без сопоставления сведений она беспомощна; без аналитического единства она проигрывает преступной сети, которая давно научилась действовать как целое.**

Организационная модель центра должна предусматривать чёткое распределение полномочий, регламентированный обмен сведениями, режимы допуска к материалам различной степени чувствительности, систему персональной ответственности за полноту и своевременность внесения данных, а также процедуры срочного созыва межведомственных групп в случае обнаружения признаков неминуемой угрозы. Необходим и постоянный учебно-методический контур, поскольку преступная среда обновляет свои средства и приёмы гораздо быстрее, чем традиционная ведомственная система успевает перерабатывать полученный опыт. Поэтому центр должен выполнять не только оперативно-аналитическую, но и образовательную функцию: проводить разборы завершённых дел, формировать базы типовых ошибок, распространять методические рекомендации, организовывать подготовку сотрудников к работе с новыми формами цифровой преступности.

В более широком смысле создание специализированных межведомственных центров цифрового противодействия означает смену самой философии правоохранительной деятельности. Государство должно отказаться от устаревшей иллюзии, будто преступление можно понять, расследовать и пресечь внутри узких ведомственных рамок, когда каждый участник видит лишь свою часть картины и ревностно охраняет её от других. Такой подход был недостаточен уже вчера; сегодня он становится просто опасным. **Преступные сети побеждаются не количеством разрозненных структур, а единством воли, скоростью обмена сведениями, глубиной анализа и**

процессуальной безупречностью совместных действий. Именно поэтому межведомственный центр цифрового противодействия следует рассматривать как необходимый опорный институт современной системы безопасности, как инструмент не локального ведомственного удобства, а стратегического государственного самообеспечения перед лицом быстро эволюционирующей преступности.

Таким образом, создание постоянно действующих специализированных межведомственных центров цифрового противодействия отвечает сразу нескольким фундаментальным задачам: обеспечивает преодоление ведомственной разобщённости, ускоряет выявление и пресечение преступной активности, повышает качество доказательственной базы, усиливает международное взаимодействие, способствует выработке единых методических подходов и создаёт условия для упреждающего, а не запаздывающего реагирования на угрозы. И если государство действительно намерено не догонять преступность, а опережать её, то подобные центры должны стать не периферийным элементом правоохранительного механизма, а его нервным узлом, его аналитическим сердцем, его решающим средством в борьбе за контроль над цифровым пространством, где сегодня всё чаще определяется безопасность общества, правопорядок и суверенитет.

3.2. Развитие цифровой разведки и криминального анализа

Современная организованная преступность давно перестала быть лишь совокупностью разрозненных эпизодов насилия, вымогательства, незаконного оборота запрещённых веществ, оружия, людей и капитала. Сегодня она всё в большей степени существует как сложная, распределённая, технологически опосредованная среда, где преступная деятельность опирается не только на физическое принуждение, но и на управление потоками сведений, на сокрытие цифровых следов, на постоянное воспроизводство каналов связи, доверительных контуров, расчётных механизмов и способов конспирации. В этих условиях перед силовыми ведомствами встаёт не частная, а **стратегическая задача**: перейти от преимущественно реактивного пресечения отдельных эпизодов к системному выявлению архитектуры преступной деятельности, её повторяющихся функций, её внутренних зависимостей и точек уязвимости.

Именно поэтому развитие цифровой разведки и криминального анализа должно рассматриваться не как вспомогательное направление, а как **одно из центральных оснований современной правоохранительной политики**. Речь идёт о формировании такой аналитической способности государства, которая позволяет видеть преступную среду не в виде набора разрозненных сообщений, а как целостную структуру: с её иерархией, распределением ролей, логистикой, механизмами вербовки, каналами финансирования, схемами информационного прикрытия и воспроизводимыми моделями

поведения. В противном случае силовые ведомства обречены бесконечно бороться с внешними проявлениями криминальной активности, не затрагивая её организационного ядра.

Принципиальное значение здесь имеет анализ открытых данных. Под ним следует понимать не механический сбор общедоступных сведений, а **систематическое извлечение оперативно значимой информации** из множества разнородных источников: страниц в сетевых сообществах, каналов распространения сообщений, видеоматериалов, объявлений, форумов, торговых площадок, архивов доменных записей, реестров юридических лиц, судебных актов, публикаций в средствах массовой информации, сервисов размещения вакансий, открытых картографических сведений, записей о перемещении товаров, изображений объектов, следов цифровой рекламы и иных массивов, которые по отдельности могут казаться нейтральными, но в совокупности раскрывают скрытые формы преступной координации. **Сила открытых данных** заключается в том, что преступные структуры, как бы тщательно они ни маскировались, вынуждены оставлять следы своей деятельности в пространстве публичной коммуникации. Им необходимо объявлять набор исполнителей, поддерживать узнаваемость незаконных площадок, перемещать аудиторию между каналами, реагировать на действия конкурентов и правоохранительных органов, подтверждать «надёжность» своих посредников, удерживать доверие в преступной среде. Всё это создаёт массив признаков, подлежащих выявлению, сопоставлению и правовой оценке.

Не менее важным направлением становится разведка по социальным медиаплощадкам и платформенным коммуникациям. Это направление требует от силовых структур глубокого понимания того, что преступные сообщества сегодня строят своё влияние не только через прямой контакт, но и через **управление вниманием, эмоциями, лояльностью и привычками аудитории**. В сетевой среде преступность действует как особая система воздействия: она распространяет символику, формирует речевые клише, культивирует ритуалы «доверия», навязывает легенды о собственной неуязвимости, создаёт ложную картину массовости и устойчивости, нормализует криминальное поведение через повседневный язык общения. Изучение этой среды должно включать не только отслеживание конкретных сообщений, но и анализ динамики сообществ, миграции пользователей между каналами, ритма публикационной активности, смены способов маскировки, способов вовлечения несовершеннолетних и социально уязвимых лиц, а также особенностей цифрового самоописания преступных посредников и координаторов. **Ключевой научно-практический вывод** состоит в том, что преступная коммуникация почти никогда не бывает хаотичной: даже при внешней фрагментарности она подчиняется

устойчивым правилам сигнализации, допуска, подтверждения, распределения ролей и контроля исполнения.

Особое место должен занимать анализ связей между субъектами, каналами связи, автоматизированными учётными записями, электронными кошельками, доменными именами, техническими устройствами и иными цифровыми сущностями. Именно такой подход позволяет перейти от исследования отдельного объекта к пониманию **преступной сети как функциональной системы**. Для правоохранительной практики это означает необходимость выявлять не только прямые, но и косвенные связи: совпадения по времени активности, пересечения в используемых шаблонах речи, повторяющиеся реквизиты для расчётов, общие технические признаки инфраструктуры, типовые маршруты перехода пользователей, сходные цепочки переадресации, совпадающие интервалы публикаций, единый стиль оформления объявлений, синхронность действий в ответ на внешнее давление. Анализ связей особенно важен потому, что организованная преступность сознательно дробит свою структуру, стремясь сделать каждое звено на первый взгляд автономным. Однако между этими звеньями сохраняются функциональные зависимости, и задача аналитика состоит в том, чтобы не поддаться иллюзии разрозненности, а восстановить скрытую систему координации. **Там, где преступники видят конспирацию через расщепление ролей, государство должно видеть целостность через реконструкцию связей**.

Необходимым элементом современной аналитической работы является выявление повторяющихся криминальных сценариев. Организованная преступность уязвима не в тех точках, где она громче всего заявляет о себе, а там, где она вынуждена постоянно воспроизводить одни и те же организационные действия. Ей необходимо переводить аудиторию из одного канала в другой после блокировок, публиковать сигналы о доступности товара или услуги, собирать оплату через цепочки посредников, координировать курьеров или закладчиков, проверять лояльность и дисциплину исполнителей, разрешать конфликты, поддерживать репутацию, наращивать клиентскую базу, реагировать на нештатные ситуации, скрывать следы сбоев и утрат. Всё это образует **повторяемые преступные циклы**, которые могут быть описаны, классифицированы и положены в основу прогностических моделей. Когда силовые ведомства выявляют такие циклы, они получают возможность действовать не только после совершения преступления, но и на предшествующих стадиях - в момент подготовки инфраструктуры, вербовки исполнителей, тестирования новых каналов, смены расчётных механизмов, перестройки маршрутов коммуникации. Иными словами, анализ повторяющихся сценариев переводит правоохранительную деятельность из режима запоздалой фиксации в режим опережающего вмешательства.

С этим напрямую связано установление совпадений между различными цифровыми идентичностями. В условиях сетевой преступности один и тот же субъект может действовать под множеством имён, использовать разные площадки, менять способы самопрезентации, применять отдельные каналы для связи с покупателями, другие - для связи с посредниками, третьи - для расчётов, четвёртые - для вербовки новых участников. Преступник стремится разорвать единство собственного образа, превратить свою деятельность в совокупность несвязанных масок. Поэтому для силовых ведомств критически важно развивать методы, позволяющие устанавливать, что за несколькими на первый взгляд независимыми цифровыми профилями может стоять **одно и то же лицо, одна и та же группа или единый центр управления**. Основанием для такого вывода могут служить не только технические признаки, но и особенности речевого поведения, повторяющиеся шаблоны общения, типичные ошибки в написании, устойчивые временные интервалы активности, привычные способы оформления сообщений, повторяющиеся модели финансового поведения, сходство реквизитов, единый набор используемых изображений, пересечения в контактных цепочках. Значение такой работы трудно переоценить: пока преступная сеть успешно множит фиктивные личности, она сохраняет мобильность, устойчивость и возможность быстро восстанавливаться после локальных потерь. Когда же эти маски аналитически сводятся к реальным субъектам и центрам координации, преступная среда теряет главное преимущество - анонимизированную многоликость.

Исключительно важным направлением выступает восстановление хронологии преступной активности. Для раскрытия организованных форм преступности недостаточно знать, кто, где и каким образом действовал. Необходимо понимать, **когда и в какой последовательности** разворачивались события, какие действия были подготовительными, какие - маскирующими, какие - координационными, какие - расчётными, какие - реакцией на внешнее воздействие. Хронологическая реконструкция позволяет увидеть логику преступной операции: от появления первичных сигналов и пробной активности до развертывания устойчивой схемы, её расширения, кризиса, трансформации и возможного распада. В практическом отношении такая реконструкция даёт возможность устанавливать причинно-следственные связи между эпизодами, выявлять инициаторов, отличать центр принятия решений от рядовых исполнителей, определять фазы наибольшей уязвимости сети, а также доказывать согласованность действий участников в рамках единого преступного замысла. **Временное измерение** здесь не является второстепенным: именно оно превращает набор разрозненных цифровых следов в доказуемую историю преступной деятельности.

Не менее значим анализ дезорганизации преступной сети, то есть определение таких ключевых узлов, устранение которых максимально ослабляет её жизнеспособность. Ошибка многих правоохранительных подходов состоит в том, что усилия сосредоточиваются на наиболее заметных участниках или на наиболее шумных каналах распространения информации. Однако наиболее заметное далеко не всегда является наиболее важным. Преступная сеть может легко пожертвовать внешним распространителем, второстепенным посредником, публичным каналом или заменяемым исполнителем, если при этом сохранены её расчётные механизмы, доверительные контуры, маршруты координации и технические администраторы. Следовательно, задача силовых ведомств заключается в том, чтобы выявлять не просто участников сети, а её **структурно критические элементы**: те узлы, через которые проходят потоки доверия, денег, команд, допуска, подтверждения, перенаправления аудитории, восстановления после блокировок. Воздействие именно на такие узлы способно не просто сократить видимую активность, но вызвать системный сбой, увеличить внутренние издержки преступной организации, подорвать её способность к самовоспроизводству, посеять недоверие между участниками и сделать дальнейшее функционирование рискованным и дорогостоящим.

Из этого вытекает более широкий методологический вывод: современная борьба с организованной преступностью должна быть ориентирована не только на обнаружение запрещённого содержания или отдельных исполнителей, но и на исследование **повторяемых организационных функций преступной среды**. Преступная сеть живёт не одними лишь преступлениями как таковыми; она живёт процедурами, без которых преступления невозможно постоянно воспроизводить. Ей необходимо привлекать новых участников, проверять старых, обеспечивать расчёты, поддерживать каналы связи, компенсировать потери, формировать репутационные гарантии, управлять страхом разоблачения, распределять роли, документировать внутренние обязательства в неформальных формах, переводить аудиторию на резервные ресурсы, стирать следы ошибок и утечек. Именно эти обязательные функции, повторяясь снова и снова, создают **аналитически уязвимый контур**. Там, где есть повтор, там есть закономерность. Там, где есть закономерность, там возможны выявление, измерение, прогнозирование и прицельное пресечение.

Для достижения обозначенных целей силовым ведомствам необходима не эпизодическая модернизация, а глубокая институциональная перестройка аналитической работы. Прежде всего требуется создание устойчивых межведомственных механизмов объединения сведений, поскольку цифровые следы преступной деятельности почти всегда распределены между различными органами, уровнями управления и предметными направлениями. Если одна служба видит финансовые признаки, другая -

сетевую инфраструктуру, третья - миграцию каналов связи, четвёртая - перемещение исполнителей, но эти сведения не сводятся в общую картину, государство само воспроизводит ту фрагментацию, на которой паразитирует преступная сеть. Следовательно, **межведомственная аналитическая сшивка данных** должна стать обязательным принципом, а не исключением. При этом речь идёт не о механическом накоплении массивов сведений, а о выработке единых правил описания объектов, событий, связей и временных меток, чтобы разнородная информация могла быть сопоставлена в единой доказательной и оперативной логике.

Необходим также качественно иной уровень подготовки кадров. Цифровая разведка и криминальный анализ требуют специалистов, которые способны мыслить одновременно юридически, оперативно, технически и социологически. Недостаточно владеть отдельными приёмами поиска сведений; необходимо уметь различать подлинный сигнал и шум, понимать способы самоорганизации сетевых сообществ, распознавать маскировочные приёмы, работать с неполными и противоречивыми данными, строить проверяемые гипотезы, отделять вероятностный вывод от доказанного факта, учитывать пределы допустимого вмешательства в сферу прав граждан. **Профессионализм нового типа** в правоохранительной сфере - это способность соединять строгую доказательность с аналитической дальновидностью. Без этого цифровая среда будет продолжать давать преступникам преимущество в скорости, пластичности и скрытности.

Особого внимания заслуживает вопрос о правовой и этической рамке такой деятельности. Усиление цифровой разведки не должно превращаться в произвольное вторжение в частную жизнь, в неразборчивое накопление сведений или в подмену доказательства предположением. Напротив, чем мощнее аналитический инструментарий государства, тем строже должны быть **правовые гарантии его применения**. Научно обоснованная и общественно легитимная модель цифрового криминального анализа предполагает чёткое разграничение между открытыми сведениями, оперативно значимой информацией, допустимыми процедурами проверки, процессуально значимыми доказательствами и мерами ограничения прав. Только в этом случае аналитическое усиление силовых ведомств будет работать не против правопорядка, а в его защиту. Государство, борющееся с сетевой преступностью, не должно уподобляться ей в стремлении к непрозрачности и произволу; его преимущество должно состоять в законности, точности и ответственности.

Наконец, принципиально важно осознать: в борьбе с организованной преступностью цифровая аналитика не может быть сведена к роли обслуживающего инструмента. Она должна стать **ядром упреждающего государственного действия**. Там, где преступная среда использует цифровые площадки для рассеивания следов, государство обязано научиться собирать их в единую доказательную ткань. Там, где преступные

сообщества дробят идентичности, государство должно восстанавливать субъекта за множеством масок. Там, где преступность полагается на повторение скрытых организационных процедур, правоохранительная система должна превращать это повторение в карту уязвимости. Там, где криминальная сеть надеется пережить блокировку одного канала за счёт резервной инфраструктуры, государство должно бить не по поверхности, а по механизму самовосстановления.

В конечном счёте именно здесь проходит одна из важнейших линий современного противостояния между государством и организованной преступностью. Побеждает не тот, кто фиксирует больше отдельных эпизодов, а тот, кто глубже понимает устройство преступной среды, быстрее выявляет её закономерности и точнее определяет точки решающего воздействия. **Организованную преступность необходимо поражать не только силой пресечения, но и силой понимания**. И чем раньше силовые ведомства превратят цифровую разведку и криминальный анализ в приоритет государственной безопасности, тем меньше пространства останется у преступных сетей для маскировки, воспроизводства и экспансии.

3.3. Стандартизация цифровой доказательственной фиксации

Одной из наиболее острых и в то же время наиболее недооцененных проблем современной правоохранительной деятельности остается не столько обнаружение цифровых следов преступления, сколько их надлежащее, юридически безупречное и технически достоверное закрепление. В условиях, когда значительная часть противоправной активности переместилась в электронную среду, вопрос о судьбе доказательства решается уже не только в момент его выявления, но прежде всего в момент его фиксации. Там, где отсутствует единообразие действий, где не выработаны обязательные правила обращения с цифровыми объектами, где сотрудники действуют по собственному усмотрению, неизбежно возникает разрушительный для правосудия разрыв между фактическим обнаружением следа и возможностью его судебного использования. Иными словами, цифровой след, который не был правильно зафиксирован, в процессуальном смысле перестает существовать. Эта истина должна быть положена в основу всей ведомственной политики в рассматриваемой сфере.

Цифровая доказательственная фиксация требует не частных усовершенствований, а построения целостной, общегосударственной, нормативно и методически выверенной системы. Такая система должна исходить из природы самой электронной среды, для которой характерны изменчивость, многослойность, распределенность хранения, зависимость содержания от времени обращения, различие между отображаемым и фактически существующим содержанием, а также постоянная угроза автоматического удаления, перезаписи, скрытого изменения или утраты

данных. Любое сообщение, любая переписка, любой размещенный файл, любая запись о времени входа, любой переход по ссылке, любой перечень участников беседы, любой след взаимодействия пользователя с информационной площадкой - все это способно иметь доказательственное значение. Однако в отсутствие стандартизированных правил фиксации один и тот же объект может быть в одном случае признан допустимым доказательством, а в другом - отвергнут судом как ненадлежащим образом закрепленный, непроверяемый или допускающий сомнения в подлинности. Подобная ситуация несовместима с принципами законности, равенства правоприменения и эффективности уголовного преследования.

Прежде всего необходимо **разработать единые протоколы фиксации сообщений, каналов, бесед, файлов, служебных сведений о данных и ссылочных переходов**. Речь должна идти не о ведомственных памятках общего характера, а о строго формализованных правилах, обязательных для оперативных подразделений, следственных органов, экспертных учреждений и иных участников процессуального доказывания. В этих правилах необходимо определить, какие именно сведения подлежат обязательному закреплению при обнаружении цифрового объекта: наименование площадки или службы обмена сообщениями; сведения об учетной записи; точное название канала, беседы или группы; идентификационные обозначения участников; дата и время обнаружения; дата и время, отображаемые в самой среде; полный адрес сетевого перехода; описание последовательности действий сотрудника; перечень технических средств, использованных при фиксации; сведения о сетевом соединении; признаки доступности или ограниченности содержания; наличие удаления, редактирования, самоуничтожения сообщений либо иных признаков нестабильности данных.

Особое значение имеет **различение содержания и его цифрового контекста**. Недостаточно закрепить лишь текст сообщения или изображение на экране. Необходимо зафиксировать, где именно этот объект находился, каким образом он был получен, в какой среде отображался, какие сведения сопровождали его появление, каково было положение объекта в общей структуре беседы, имелись ли указания на время отправки, пересылки, редактирования, удаления, ответного сообщения, прикрепления файлов, реакций участников, статуса прочтения. Для суда важно не только то, что сказано, но и кем, когда, где, в какой последовательности и при каких обстоятельствах это было сделано. Следовательно, протокол фиксации должен охватывать не только само содержание, но и весь доказательственный каркас, делающий это содержание юридически значимым.

Необходимость единых правил особенно очевидна применительно к ссылочным переходам и связанным с ними объектам. В современной электронной среде содержание нередко размещается не непосредственно в

беседе, а через внешние переходы, временные страницы, распределенные хранилища, скрытые приглашения, одноразовые адреса доступа. Если сотрудник ограничивается лишь сохранением внешнего вида сообщения, не закрепляя точный адрес перехода, время обращения по нему, последовательность перенаправлений, признаки доступности содержимого и его состояние на конкретный момент времени, доказательство теряет значительную часть своей удостоверительной силы. Поэтому в национальных протоколах следует предусмотреть обязательную фиксацию полного адреса ресурса, всех последующих перенаправлений, параметров доступа, времени открытия, отображаемых заголовочных сведений, данных о владельце или размещающей стороне, если они доступны законным способом, а также результатов повторного обращения к тому же адресу в разумный промежуток времени. Только так можно показать суду, что обнаруженное содержание не является случайной, искусственно созданной или неидентифицируемой информацией.

Не менее важной задачей является **обеспечение юридически устойчивого документирования временных данных**. Время в цифровой криминалистике - это не вспомогательная деталь, а один из центральных элементов доказательственной конструкции. Именно временная привязка позволяет установить последовательность действий, координацию участников, момент формирования умысла, связь между сообщением и совершенным деянием, наличие предварительного сговора, длительность участия в преступной деятельности, факт сокрытия следов, удаления материалов или смены учетных записей. Между тем временные сведения в электронной среде нередко уязвимы: они зависят от настроек устройства, часового пояса, особенностей отображения в самой площадке, различий между локальным временем и временем сервера, запаздывания синхронизации, ручной корректировки системных часов, а также от того, что часть площадок отображает время приблизительно, сокращенно или изменяет способ его показа по мере устаревания записи.

Из этого следует необходимость создания строгих правил документирования времени, при которых каждое зафиксированное значение должно сопровождаться указанием источника времени, часового пояса, технической среды, в которой оно отображено, и способа его сверки с эталонным временем. Для правоприменения принципиально важно, чтобы сотрудник не просто переписывал увиденное обозначение времени, а удостоверял, какое именно время он фиксирует: системное время устройства, время, отображаемое площадкой, время из журнала соединений, время из служебных записей, время получения ответа от удаленного ресурса. В каждом случае требуется отдельное отражение способа установления временного значения и степени его надежности. Целесообразно закрепить обязательное сопоставление времени устройства с государственными эталонными источниками времени непосредственно до

и после проведения действий по фиксации, а также обязательное документирование любых расхождений. Если такая процедура не будет стандартизирована, защита неизбежно поставит под сомнение всю временную линию событий, а вместе с ней - и достоверность выводов следствия.

Особого рассмотрения требует **немедленное сохранение быстро исчезающих данных**. Электронная среда живет по законам текучести: сведения, существующие в один момент, уже через несколько минут могут быть безвозвратно утрачены. К этой категории относятся не только так называемые самоуничтожающиеся сообщения, но и отображаемые в течение ограниченного срока истории просмотра, сведения о присутствии пользователя, записи о подключениях, временные ключи доступа, промежуточные буферы, временные копии файлов, содержимое оперативной памяти устройств, сведения о текущих сеансах связи, быстро изменяющиеся страницы и иные неустойчивые цифровые объекты. В условиях, когда такие данные могут исчезнуть автоматически, правоохранительные органы не вправе действовать так, будто перед ними обычный вещественный предмет, способный месяцами лежать в камере хранения без изменений. Здесь промедление означает утрату истины.

В связи с этим должна быть введена **обязательная процедура незамедлительного реагирования на выявление быстро исчезающих данных**. Такая процедура должна определять, какие действия подлежат первоочередному выполнению, какие сотрудники уполномочены их осуществлять, в какой последовательности должна вестись фиксация, какие сведения необходимо сохранить прежде всего, каким образом обеспечивается неизменность исходной среды, как отражаются все произведенные манипуляции и каким образом минимизируется риск изменения данных самим фактом их обнаружения. Для одних ситуаций первоочередным будет сохранение текущего состояния экрана, для других - выгрузка журнала сообщений, для третьих - изъятие сведений из оперативной памяти, для четвертых - фиксация действующего сеанса связи и сетевого окружения. Но во всех случаях принцип должен быть единым: сначала - сохранение наиболее хрупкого, затем - более устойчивого; сначала - предотвращение утраты, затем - углубленный анализ. Любая иная логика неизбежно приведет к тому, что ценные сведения будут уничтожены в промежутке между их обнаружением и началом процессуального оформления.

Следующий краеугольный камень - **использование сертифицированных средств вычисления контрольных сумм, удостоверения времени и протоколирования цепи хранения доказательств**. В цифровой сфере нельзя ограничиться ссылкой на добросовестность сотрудника. Необходима техническая подтверждаемость того, что объект после изъятия, копирования или выгрузки не подвергался изменению, что время его

закрепления удостоверено, что каждый этап обращения с ним отражен в непрерывной и проверяемой последовательности. Контрольная сумма цифрового объекта должна рассчитываться по утвержденным правилам сразу после его получения и, при необходимости, повторно на последующих этапах. Результаты должны вноситься в протоколы, сопроводительные документы и хранилища доказательственной информации. Это не формальность, а фундамент доверия к цифровому доказательству.

Не менее значимо удостоверение времени фиксации. В условиях, когда защита может заявить, что файл был создан позднее, выгрузка произведена в иной момент, а изображение экрана изготовлено задним числом, простого указания сотрудника о дате и времени составления протокола уже недостаточно. Требуется юридически значимое закрепление самого факта существования конкретного цифрового объекта в определенный момент. Поэтому ведомственные стандарты должны предусматривать обязательное использование средств удостоверения времени, признаваемых государством и допускающих последующую проверку. Такая практика позволит укрепить доказательственную силу материалов, исключить споры о времени их происхождения и существенно повысить устойчивость обвинения в суде.

Особое внимание должно быть уделено **цепи хранения доказательства**, то есть непрерывному документированию всех действий с цифровым объектом с момента его обнаружения до представления в суде. Для обычного вещественного доказательства эта проблема давно осознана, однако в отношении цифровых объектов она приобретает многократно большую сложность. Один и тот же файл может существовать в нескольких копиях; рабочая копия может отличаться от исходной; при открытии файла могут автоматически изменяться служебные сведения; при переносе на другой носитель возможна порча данных; при исследовании без соблюдения правил - непреднамеренное изменение содержимого. Поэтому национальные стандарты должны требовать обязательного разграничения исходного объекта, его побитовой копии, рабочей копии для исследования и копии для судебного обозрения. Должно быть ясно и проверяемо, кто, когда, на каком основании и с какой целью получил доступ к каждому экземпляру, какие действия с ним производил, какими средствами пользовался, где объект хранился, при каких условиях обеспечивалась его сохранность и кем подтверждена неизменность на каждом этапе. Если эта цепь разорвана, доказательство оказывается под угрозой исключения, а вместе с ним может разрушиться и вся доказательственная система по делу.

Отсюда вытекает необходимость **формирования национальных стандартов получения изображений с экрана, выгрузки и проверки цифровых объектов**. На первый взгляд может показаться, что изображение с экрана - простейший способ закрепления информации. Но именно здесь правоприменение особенно часто сталкивается с процессуальной беспомощностью.

Изображение с экрана нередко выполняется без указания устройства, без фиксации адресной строки, без отображения системного времени, без видимой структуры источника, без подтверждения того, что изображение относится именно к исследуемой учетной записи, а не к искусственно созданной имитации. Подобная практика должна быть признана недопустимо примитивной. Национальный стандарт должен строго определить, что именно должно содержаться в изображении с экрана и в сопроводительном протоколе: полное отображение интерфейса; наименование приложения или страницы; реквизиты учетной записи; системные дата и время; элементы навигации; видимые признаки подлинности источника; последовательность переходов, предшествовавших получению изображения; сведения о средстве, которым выполнено сохранение; контрольная сумма созданного файла изображения; сведения о дальнейшем хранении.

Однако и этого недостаточно. В научно и процессуально зрелой системе изображение с экрана не должно рассматриваться как самодостаточное средство фиксации там, где возможно получение более полного цифрового следа. При наличии технической и правовой возможности приоритет следует отдавать выгрузке исходных данных, журнальных записей, файловых копий, служебных сведений о данных и иным формам фиксации, позволяющим проверить происхождение, целостность и внутреннюю структуру объекта. Изображение с экрана должно использоваться либо как первичная срочная мера при угрозе утраты, либо как дополнительное средство наглядной демонстрации обнаруженного содержания, но не как единственная опора обвинения в сложных делах о деятельности преступных сообществ, координации противоправных действий, вовлечении новых участников, незаконном обороте запрещенных предметов, экстремистской и террористической пропаганде, шантаже, вымогательстве, мошенничестве и иных деяниях, где электронная переписка образует сам нерв преступного механизма.

Стандартизация выгрузки цифровых объектов также требует глубокой регламентации. Следует нормативно определить, в каких форматах допустимо сохранять переписку, файлы и сопровождающие сведения; как обеспечивается полнота выгрузки; каким образом фиксируются сведения о невыгруженных или недоступных элементах; как документируются ошибки, пропуски, ограничения доступа, автоматические сокращения содержимого; каким образом удостоверяется, что выгруженный массив соответствует отображавшемуся в исходной среде содержанию. Критически важно предусмотреть процедуры повторной проверки выгрузки и сопоставления ее с визуально наблюдаемым содержанием. Только так можно избежать ситуации, когда в деле имеется лишь фрагментарная или частично искаженная копия цифрового взаимодействия, а ключевые

сообщения, даты или вложения оказываются утраченными либо оспариваемыми.

Принципиальной составляющей стандартизации является **верификация цифровых объектов**, то есть установление их подлинности, целостности, относимости и воспроизводимости. Верификация не может сводиться к субъективному убеждению сотрудника, что «он видел это своими глазами». Нужна совокупность проверочных действий: сопоставление нескольких источников сведений; установление логической связи между содержанием и учетной записью; анализ признаков редактирования или монтажа; оценка соответствия временных отметок; проверка служебных сведений о данных; сопоставление с изъятыми устройствами, сведениями операторов связи, показаниями лиц, результатами осмотра и экспертного исследования. Государственный стандарт должен закрепить минимальный обязательный набор таких проверок для различных типов цифровых объектов. В противном случае в одном регионе и даже в одном подразделении подлинность будут считать установленной на основании поверхностного визуального осмотра, а в другом - требовать полноценного экспертного подтверждения. Такая разноречивость подрывает единство правоприменения и наносит прямой ущерб авторитету государства.

Наконец, вся эта система останется мертвой буквой без **целенаправленного обучения следователей и оперативных сотрудников правильной работе с исчезающим содержанием**. Электронная среда беспощадна к непрофессионализму. Одно неосторожное касание экрана, одно автоматическое открытие беседы, один вход в учетную запись без соблюдения процедур, одно неверно выполненное копирование - и доказательство либо исчезает, либо оказывается зараженным сомнением в своей чистоте. Следовательно, подготовка кадров должна перестать быть эпизодическим ознакомлением с техническими новинками и превратиться в системную профессиональную специализацию.

Такое обучение должно носить не отвлеченный, а прикладной характер. Сотрудники должны уметь различать типы цифровых объектов по степени их устойчивости; понимать, какие данные исчезают немедленно, какие - спустя ограниченное время, а какие сохраняются длительно; знать признаки редактируемых и самоуничтожающихся сообщений; владеть методикой первоначальной фиксации переписки, изображений, звуковых сообщений, видеозаписей, файлов, сведений о размещении, списков участников, временных отметок и сетевых переходов; уметь сохранять цифровую среду без ее разрушения; грамотно составлять процессуальные документы; взаимодействовать со специалистами и экспертами; понимать пределы допустимого воздействия на устройство и учетную запись. Кроме того, обучение должно включать моделирование типичных ошибок и их правовых последствий. Сотрудник обязан ясно осознавать: нарушение порядка фиксации - это не просто технический недочет, а потенциальная

гибель всего дела, результат многомесячной работы, перечеркнутый в судебном заседании одним обоснованным сомнением в достоверности доказательства.

Подготовка кадров должна сопровождаться созданием ведомственных учебно-методических центров, единых программ повышения квалификации, обязательной периодической аттестацией и формированием устойчивой практики совместной работы следователей, оперативных сотрудников, специалистов по компьютерной криминалистике и процессуалистов. Более того, необходимо преодолеть опасное заблуждение, будто цифровая фиксация - дело узких технических специалистов, к которому основной состав правоохранительных органов может обращаться лишь в исключительных случаях. Напротив, в современных условиях это должна быть одна из базовых компетенций каждого сотрудника, соприкасающегося с раскрытием и расследованием преступлений. Там, где цифровой след стал повседневной формой следа преступного, его грамотное закрепление должно стать повседневным навыком государства.

В более широком смысле стандартизация цифровой доказательственной фиксации - это вопрос не только процессуальной техники, но и правовой цивилизации государства. Правосудие не может зависеть от случая, личной осведомленности конкретного сотрудника или технической изобретательности отдельного подразделения. Оно должно опираться на единые, воспроизводимые, проверяемые и обязательные для всех правила обращения с цифровой реальностью. Лишь при таком подходе возможно обеспечить одновременно и эффективность уголовного преследования, и соблюдение прав личности, и устойчивость судебных решений.

Следует подчеркнуть, что цифровая криминалистика в современную эпоху перестала быть вспомогательной областью. Она стала одним из решающих рубежей борьбы за доказательство. Можно выявить преступную сеть, установить ее участников, проследить каналы координации, вскрыть механизмы финансирования и распространения противоправного содержания, но при отсутствии надежной системы цифровой фиксации вся эта работа способна рассыпаться в судебной стадии. Суд не выносит обвинительный вывод на основании догадок, профессиональной интуиции или оперативной убежденности; ему требуется доказательство, происхождение, целостность и допустимость которого не вызывают обоснованных сомнений. Именно поэтому стандартизация в рассматриваемой сфере должна рассматриваться не как частная техническая реформа, а как одна из первоочередных государственных задач в сфере обеспечения законности.

Итак, для силовых ведомств в качестве безусловного ориентира должно быть утверждено следующее: **единые протоколы фиксации цифровых объектов,**

юридически устойчивое документирование времени, **незамедлительное сохранение быстро исчезающих данных**, **обязательное применение сертифицированных средств контроля целостности, удостоверения времени и ведения цепи хранения**, **национальные стандарты получения изображений с экрана, выгрузки и проверки цифровых объектов**, а также **системная подготовка кадров**. Только соединение этих начал способно превратить разрозненную практику в подлинно государственную систему цифрового доказывания. И только такая система способна воспрепятствовать тому, чтобы обнаруженный след преступления исчезал не в бездне электронного пространства, а в пробелах правоприменительной беспомощности.

3.4. Внедрение риск-ориентированной модели приоритизации

Одной из наиболее существенных ошибок в деятельности силовых ведомств при противодействии преступности в цифровой среде остается стремление реагировать на все выявляемые проявления противоправной активности как на равноценные по степени общественной опасности. Подобный подход внешне может создавать впечатление высокой служебной активности, однако в действительности он ведет к распылению сил, перегрузке следственных и оперативных подразделений, утрате управляемости и, что особенно опасно, к стратегическому ослаблению государства перед лицом действительно крупных и системных угроз. **Не вся противоправная активность в цифровой среде обладает одинаковым уровнем опасности, одинаковыми последствиями и одинаковым потенциалом разрушительного воздействия на общество, экономику и государственные институты**. Именно поэтому современная практика противодействия цифровой преступности должна опираться не на механическое наращивание числа проверок, задержаний и возбужденных дел, а на выверенную, научно обоснованную, юридически устойчивую и организационно дисциплинированную модель приоритизации, основанную на оценке риска.

Сущность риск-ориентированного подхода состоит в том, что государство сознательно отказывается от иллюзии тотального и одинаково интенсивного контроля над всеми цифровыми правонарушениями и вместо этого сосредоточивает основные силы на тех сегментах преступной среды, которые несут наибольший ущерб, обладают высокой степенью воспроизводимости, связаны с организованными структурами, затрагивают критически важные интересы личности, общества и государства, а также способны быстро масштабироваться, уклоняясь от традиционных мер пресечения. **Приоритет должен определяться не заметностью преступления, не громкостью общественного резонанса и не простотой отчетного результата, а глубиной угрозы и тяжестью последствий**. Если ведомство направляет основные ресурсы на эпизодические, малозначительные или технически примитивные нарушения лишь потому,

что они легче документируются и быстрее доводятся до процессуального результата, оно тем самым оставляет в тени сложные, иерархически организованные, финансово обеспеченные преступные сети, которые в реальности формируют ядро современной цифровой преступности.

Выстраивание риск-ориентированной модели предполагает создание многоуровневой матрицы угроз, в которой каждый выявляемый объект оперативного интереса подлежит оценке по совокупности критериев. К числу таких критериев относятся масштаб причиняемого или потенциального вреда, количество возможных потерпевших, степень организованности группы, наличие трансграничных связей, устойчивость преступной инфраструктуры, объем незаконных доходов, связь с насильственными формами преступности, воздействие на несовершеннолетних, вовлеченность в коррупционные отношения, возможность быстрого восстановления после пресечения, использование средств сокрытия, а также вероятность дестабилизации общественной безопасности и подрыва государственных интересов. **Матрица угроз должна быть не формальным перечнем категорий, а рабочим инструментом распределения сил, полномочий, времени, технических средств и процессуального внимания**. Без этого любая декларация о приоритетах останется ведомственной риторикой, не способной изменить реальное положение дел.

В рамках такой модели первоочередное внимание должно уделяться транснациональным преступным сетям. Их опасность определяется не только географическим охватом, но и особым качеством преступной организации. Речь идет о структурах, которые используют различие правовых режимов, расхождения в национальных процедурах, территориальную рассредоточенность исполнителей и посредников, а также сложные цепочки финансового и технического сокрытия. Такие сети способны координировать незаконный оборот товаров, данных, финансовых средств и преступных услуг сразу в нескольких юрисдикциях, резко затрудняя выявление организаторов, изъятие активов и закрепление доказательств. **Транснациональная сеть опасна тем, что она атакует не отдельного гражданина и даже не отдельный регион - она испытывает на прочность саму способность государства защищать свой правопорядок в условиях цифровой взаимосвязанности мира**. Если силовые ведомства не выделяют подобные структуры в высшую категорию риска, они неизбежно оказываются в положении догоняющей стороны, реагирующей на последствия вместо того, чтобы разрушать центр координации преступной деятельности.

Особое место в системе приоритетов должны занимать каналы вербовки в насильственные и экстремистские структуры. Здесь речь идет не просто о распространении запрещенных материалов, а о преступном воздействии на сознание человека, о целенаправленном формировании готовности к

насилию, о вовлечении в деятельность, направленную против общественной безопасности, межнационального мира и конституционного порядка. В цифровой среде вербовка приобрела новые формы: она может маскироваться под общение по интересам, под идеологические дискуссии, под эмоциональную поддержку, под ложное чувство принадлежности к «избранному кругу», под риторику борьбы за справедливость. Особенно тревожным обстоятельством является то, что подобные каналы часто нацелены на молодежь, лиц с неустойчивой психикой, социально изолированных граждан и тех, кто переживает личный кризис. **Там, где государство не распознает вовремя цифровую вербовку, завтра оно сталкивается уже не с текстом на экране, а с насилием на улице, в учебном заведении, на объекте транспорта или в месте массового пребывания людей**. Следовательно, выявление, документирование и пресечение таких каналов должно рассматриваться как один из безусловных высших приоритетов.

К категории максимально опасных угроз обоснованно относятся и сегменты цифровой среды, обеспечивающие незаконный оборот оружия, наркотических средств и поддельных либо похищенных документов. Эти явления нельзя воспринимать изолированно как «отдельные рынки» преступной активности. В действительности они тесно переплетены между собой и образуют взаимно поддерживающую преступную экосистему, где один вид незаконной деятельности подпитывает другой. Незаконный оборот оружия повышает вероятность насильственных преступлений и террористических актов; сбыт наркотических средств разрушает здоровье нации, подпитывает организованную преступность и создает устойчивые коррупционные связи; теневой оборот документов облегчает легализацию иных преступлений, сокрытие личности, незаконное пересечение границ, мошенничество и проникновение в хозяйственные и государственные структуры. **Когда цифровая среда становится пространством обслуживания таких потоков, речь идет уже не о частных эпизодах, а о теневой логистике разрушения общественной безопасности**. Поэтому любые узлы, связывающие продавцов, посредников, перевозчиков, хранителей, изготовителей и финансовых операторов, должны получать повышенный приоритет в оперативной и следственной работе.

Не менее важным направлением приоритизации является борьба с мошенническими сетями, причиняющими массовый ущерб. Традиционное недооценивание подобных схем как якобы «ненасильственных» преступлений представляет собой серьезное заблуждение. Массовое мошенничество в цифровой среде способно поражать сотни тысяч граждан, лишать их сбережений, дестабилизировать доверие к финансовым учреждениям, подрывать уважение к праву и создавать атмосферу всеобщей уязвимости. За кажущейся множественностью «мелких» эпизодов зачастую скрываются высокоорганизованные структуры с жестким распределением ролей: разработчики легенд, операторы связи с потерпевшими, технические

исполнители, сборщики денежных средств, посредники по обналичиванию, координаторы и лица, обеспечивающие прикрытие. **Массовое мошенничество опасно не только похищенными суммами, но и разрушением общественного доверия как основы гражданского оборота**. Когда гражданин перестает верить звонку, сообщению, банковской операции, цифровому документу, страдает уже не только отдельная жертва - страдает сам механизм общественной коммуникации. Следовательно, приоритет должен отдаваться не отдельным исполнителям, а выявлению и разгрому всей сети, включая центры управления, финансовые каналы и схемы перераспределения похищенного.

К числу стратегически значимых угроз следует отнести торговлю персональными данными и сведениями ограниченного доступа. В современном обществе данные о человеке, его передвижениях, имущественном положении, профессиональной деятельности, семейных связях, привычках, биометрических признаках, контактах и цифровых следах становятся ценнейшим ресурсом преступного воздействия. Их незаконный оборот служит основой для последующего мошенничества, вымогательства, шантажа, кражи личности, давления на должностных лиц, проникновения в охраняемые системы и подготовки иных преступлений. Особая опасность заключается в том, что утечка и незаконная продажа таких сведений часто остаются недооцененными из-за отсутствия немедленно видимого ущерба. Однако именно из подобных, на первый взгляд «вспомогательных», массивов формируется инфраструктура будущих преступлений. **Торговля данными - это не вторичное сопровождение преступности, а ее питательная среда, ее сырьевая база, ее инструмент точечного удара по человеку, организации и государству**. Поэтому силовые ведомства обязаны рассматривать выявление каналов хищения, накопления, систематизации и сбыта данных как деятельность, непосредственно связанную с предупреждением более тяжких преступлений.

Особо жесткая и бескомпромиссная приоритизация необходима в отношении преступных схем, затрагивающих несовершеннолетних. Здесь государство не имеет нравственного права на половинчатость, процедурную расслабленность или ведомственную конкуренцию. Любая цифровая среда, в которой осуществляется вовлечение несовершеннолетних в преступную деятельность, сексуальная эксплуатация, распространение материалов, посягающих на половую неприкосновенность, склонение к саморазрушительному поведению, психологическое подавление, шантаж, вымогательство или манипулятивное управление, должна рассматриваться как пространство повышенной криминальной опасности. Уязвимость детей и подростков обусловлена не только возрастом, но и спецификой цифрового общения: высокой доверчивостью, стремлением к признанию, недостаточным жизненным опытом, неумением оценивать скрытые

мотивы собеседника, а также психологической зависимостью от мнения виртуального окружения. **Преступления против несовершеннолетних в цифровой среде особенно опасны тем, что они поражают личность в стадии формирования, оставляя след не на один день, а на годы, а порой и на всю жизнь**. В системе государственной приоритизации такие эпизоды должны автоматически переводиться в категорию высшей значимости с обязательным межведомственным взаимодействием, немедленным обеспечением защиты потерпевшего и ускоренным принятием процессуальных решений.

В особую группу приоритетного преследования необходимо выделить инфраструктуру финансового сопровождения организованной преступности. Организованная преступность живет не только силой intimidation, конспирацией и дисциплиной, но прежде всего движением денежных средств. Там, где сохраняется возможность быстро получать, перемещать, дробить, маскировать и извлекать преступные доходы, преступная сеть способна переживать задержание отдельных участников, утрату отдельных площадок и даже локальные оперативные удары. И напротив, разрушение финансовой основы нередко оказывается более действенным, чем пресечение отдельных исполнителей. Под инфраструктурой финансового сопровождения следует понимать совокупность лиц, схем, посреднических звеньев, расчетных каналов, фиктивных хозяйственных операций, подставных счетов, незаконных сервисов перевода средств и иных механизмов, обеспечивающих жизнеспособность преступной организации. **Следовать лишь за исполнителем - значит бороться с тенью; перекрыть финансирование - значит ударить в сердце преступной системы**. Именно поэтому риск-ориентированная модель должна неизменно поднимать в верхние строки приоритетов любые выявленные связи между цифровой преступностью и каналами отмывания, перераспределения и сохранения незаконных доходов.

Наивысший уровень внимания должны получать сети, связанные с коррупцией, диверсиями и подрывом национальной безопасности. Здесь цифровая преступность перестает быть сугубо уголовной проблемой в узком смысле и выходит на уровень прямой угрозы устойчивости государства. Коррупционные сети, использующие цифровую среду для координации действий, сокрытия связей, передачи сведений, распределения вознаграждений и уничтожения следов, подтачивают саму основу законности, поскольку лишают государственный аппарат внутренней целостности. Диверсионные формы активности - будь то посягательства на объекты жизнеобеспечения, транспорт, связь, управление, снабжение или информационные системы - способны вызвать панику, нарушить функционирование территорий и нанести ущерб, несоизмеримый с обычной уголовной статистикой. Подрыв национальной безопасности

может выражаться как в прямой координации враждебной деятельности, так и в скрытом содействии ей через каналы связи, финансирования, вербовки, сбора данных и дестабилизации общественных процессов. **Когда преступная сеть соприкасается с коррупцией и угрозами безопасности государства, вопрос приоритизации перестает быть вопросом служебной эффективности - он становится вопросом политической и исторической ответственности**.

Однако само по себе перечисление приоритетных категорий не решает проблему, если отсутствует ясный механизм их оценки. Ведомствам необходимо закрепить систему признаков, по которым объект оперативного интереса относится к той или иной ступени риска. В эту систему должны входить признаки организованности, устойчивости и воспроизводимости схемы; наличие распределения ролей; признаки профессиональной конспирации; использование подставных лиц; связь с насилием; вовлечение несовершеннолетних; ущерб критической инфраструктуре; объем похищенных или легализуемых средств; количество регионов или государств, охваченных деятельностью; наличие покровительства со стороны должностных лиц; использование похищенных данных; способность быстро воссоздавать каналы после блокировки; а также потенциал общественного резонанса, если он связан с массовым ущербом или дестабилизацией обстановки. **Приоритет должен присваиваться на основе измеримых и проверяемых признаков, а не по интуиции, личным предпочтениям руководителя или давлению текущей повестки**. Иначе система неминуемо скатится либо к субъективизму, либо к погоне за внешне эффектными, но стратегически второстепенными результатами.

Практическая ценность риск-ориентированной модели заключается и в том, что она позволяет выстраивать разумное распределение полномочий между подразделениями. Делам и материалам высокой степени риска должны соответствовать особый режим аналитического сопровождения, повышенные требования к оперативному проникновению, ускоренное межрегиональное взаимодействие, усиленная прокурорская и следственная координация, специальные меры защиты свидетелей и потерпевших, приоритетный доступ к техническим и экспертным ресурсам. Напротив, эпизоды низкой степени риска могут разрешаться в упрощенном порядке, без чрезмерного отвлечения кадров и средств. **Смысл приоритизации не в том, чтобы игнорировать малозначимые нарушения, а в том, чтобы не позволить им поглотить ресурс, предназначенный для борьбы с подлинно опасной преступностью**. Государство, которое тратит одинаковые усилия на второстепенное и на жизненно важное, в конечном счете проигрывает и там и там.

Принципиально важно, чтобы риск-ориентированная модель была встроена не только в оперативную деятельность, но и в процессуальное сопровождение дел. Если приоритетный объект выявлен, но его

документирование ведется поверхностно, без продуманной стратегии собирания, закрепления и проверки доказательств, итогом станет не победа государства, а развал дела в суде. По этой причине высокий приоритет должен означать не только ускорение действий, но и повышение их качества: тщательное установление всей структуры сети, роли каждого участника, каналов финансирования, способов связи, источников данных, фактов координации, трансграничных элементов, связи с иными преступлениями и конечных выгодоприобретателей. **Сильная приоритизация без сильного доказательственного основания опасна, поскольку она превращает громкое дело в громкое поражение**. Следовательно, ведомства должны соединять риск-ориентированный отбор объектов с безупречным соблюдением законности, процессуальной чистоты и стандарта доказанности.

Необходимо подчеркнуть и то обстоятельство, что риск-ориентированная модель не может быть раз и навсегда утвержденной схемой. Преступная среда изменчива, гибка и склонна быстро перестраиваться под действия государства. Появляются новые способы анонимизации, новые формы распределения ролей, новые финансовые механизмы, новые каналы психологического воздействия, новые формы маскировки под легальную деятельность. Поэтому матрица угроз должна постоянно уточняться на основе судебной практики, материалов расследований, сведений оперативного учета, результатов межведомственного обмена, криминологических исследований и анализа последствий уже пресеченных схем. **Приоритизация, не способная к обновлению, неизбежно превращается в архив вчерашних угроз и пропускает угрозы завтрашнего дня**. В этом вопросе государству требуется не разовая кампания, а устойчивая культура стратегического наблюдения, анализа и коррекции.

В конечном счете внедрение риск-ориентированной модели приоритизации есть не частная организационная мера, а выражение зрелости государственного мышления. Оно показывает, способно ли ведомство видеть не только отдельный эпизод, но и всю архитектуру угроз; умеет ли оно отличать симптом от источника болезни; готово ли оно действовать не ради формального показателя, а ради реального снижения преступного потенциала. **Ресурсы государства должны концентрироваться на наиболее опасных узлах, а не распыляться на второстепенные проявления**. Это не просто управленческий принцип - это требование здравого смысла, правовой ответственности и стратегического самосохранения. Там, где силы сосредоточены на главном, государство укрепляет суверенитет, защищает граждан и разрушает преступные системы в их ядре. Там же, где приоритеты размыты, неизбежно торжествуют имитация, ведомственная суета и запоздалое реагирование на уже созревшую угрозу.

3.5. Активное использование финансовой разведки

В борьбе с организованной преступностью, действующей в цифровой среде, **финансовая разведка** должна рассматриваться не как вспомогательное направление, а как один из центральных способов выявления, доказывания, пресечения и последующего разрушения преступной деятельности. Современные преступные сообщества могут тщательно скрывать средства связи, менять технические площадки, использовать многоступенчатые схемы конспирации, подменять личины участников и дробить организационную структуру на изолированные звенья. Однако при всей изощренности таких мер они почти неизбежно оставляют **денежный след**, поскольку любая устойчивая преступная деятельность требует поступления, распределения, накопления, сокрытия и легализации материальных ресурсов. Деньги питают преступную сеть, обеспечивают ее устойчивость, создают возможности для расширения, подкупа, вербовки, технического оснащения и ухода от ответственности. Именно поэтому поражение финансовой основы преступной структуры в ряде случаев оказывается более разрушительным для нее, чем точечное изъятие отдельных технических средств или задержание отдельных исполнителей.

Применительно к организованной преступности в цифровой среде финансовая разведка имеет особое значение еще и потому, что преступная деятельность здесь редко ограничивается одной территорией, одним видом дохода или одной схемой перевода средств. Напротив, наблюдается постоянное переплетение электронных расчетов, расчетов через виртуальные активы, использования подставных лиц, фиктивных договорных оснований, множественности расчетных каналов и дробления потоков на множество, на первый взгляд, не связанных между собой операций. За внешней хаотичностью такого движения средств скрывается вполне рациональная логика: усложнить восстановление цепочки, затруднить установление выгодоприобретателя, придать преступным доходам вид законного оборота. Отсюда вытекает принципиальный вывод: **финансовый анализ** должен быть не эпизодическим следственным действием, а непрерывным, системным и опережающим процессом, сопровождающим все стадии противодействия организованной преступности - от первичного выявления до исполнения судебного решения.

Прежде всего требуется **существенное усиление взаимодействия с подразделениями финансового мониторинга**, поскольку именно они аккумулируют сведения, позволяющие обнаружить неочевидные связи между лицами, счетами, платежными инструментами, хозяйственными образованиями и операциями, формально не связанными между собой в материалах первоначальной проверки. Речь должна идти не о формальном обмене отдельными запросами и ответами, а о выстраивании устойчивой межведомственной архитектуры, в которой сведения о подозрительных операциях, дроблении переводов, транзитном движении средств,

нетипичном поведении счетов, использовании номинальных участников и появлении признаков легализации преступных доходов немедленно включаются в общий массив доказательственно значимой информации. В условиях, когда преступные доходы могут перемещаться с исключительной быстротой, промедление в передаче сведений фактически играет на стороне преступников. Следовательно, **оперативность межведомственного взаимодействия** становится не организационной деталью, а условием реального успеха.

Такое взаимодействие должно опираться на единые подходы к финансово-аналитической работе. Важно не только фиксировать отдельные подозрительные операции, но и устанавливать закономерности: повторяемость контрагентов, аномальное время совершения платежей, использование однотипных реквизитов, совпадение устройств доступа, географическую несоразмерность операций, необычную скорость оборачиваемости средств, наличие искусственного дробления и признаки транзитности. В совокупности эти данные позволяют перейти от разрозненных фактов к **реконструкции преступной финансовой модели**, а затем - к раскрытию структуры самой преступной сети. Иными словами, финансовый мониторинг дает следствию и оперативным подразделениям не только сведения о деньгах, но и сведения о людях, ролях, зависимостях, дисциплине внутри группы, ее центрах управления и каналах обеспечения.

Особое место в современных условиях должен занимать **анализ операций с виртуальными активами, электронными кошельками и схемами обналичивания**. Распространенное заблуждение сводится к тому, будто расчеты в среде распределенного учета обеспечивают преступникам полную неуязвимость. На деле подобные операции, хотя и затрудняют установление личности владельца без дополнительных данных, оставляют след в виде неизменяемой последовательности переводов, позволяющей выявлять маршруты движения имущества, кластеры адресов, вероятные узлы концентрации средств и точки перехода из анонимизированной среды в традиционный денежный оборот. Главная задача правоохранительных органов здесь состоит в том, чтобы соединить технический анализ движения виртуальных активов с процессуально значимым установлением конкретных лиц, распоряжавшихся соответствующими средствами.

Для этого необходима последовательная работа по сопоставлению данных о времени переводов, используемых устройствах, сведений от площадок обмена, материалов оперативно-розыскной деятельности, следов деловой переписки, информации о приобретении оборудования, оплате услуг связи, аренде помещений, движении средств по банковским счетам и расходах на имущество. Только в таком объединении разнородных источников возможно преодолеть видимость безличности цифровых расчетов. **Финансовый след** в среде виртуальных активов не исчезает; он лишь меняет форму и требует более высокой аналитической культуры. Поэтому для

силовых ведомств принципиально важно формировать специализированые группы, способные понимать не только уголовно-правовую сторону вопроса, но и экономическую логику операций, особенности многоступенчатого перемещения цифровых имущественных ценностей, методы маскировки происхождения средств и способы вывода их в наличное или имущественное выражение.

Не менее значимым направлением является **выявление посредников, пунктов обмена, подставных держателей платежных средств и теневых расчетных узлов**, обеспечивающих преобразование преступного дохода в пригодный для дальнейшего использования ресурс. Любая организованная преступность живет не только за счет организаторов и исполнителей основных деяний, но и за счет многочисленного обслуживающего слоя. Этот слой включает тех, кто предоставляет реквизиты для переводов, открывает счета, регистрирует кошельки, снимает наличные, оформляет фиктивные договоры, проводит деньги через мнимую хозяйственную деятельность, создает видимость законных оснований для перемещения средств и помогает преступной среде соприкасаться с легальным финансовым оборотом. Именно эти фигуры часто становятся тем слабым звеном, через которое можно проникнуть в глубину преступной сети.

В правоприменительной практике недопустимо недооценивать роль подставных участников финансовых схем. За внешней второстепенностью их положения нередко скрывается колоссальная значимость: они обеспечивают разрыв между организатором и конечным денежным результатом, служат буфером между преступным источником дохода и его последующей легализацией, принимают на себя формальную видимость владения средствами и создают для следствия ложный горизонт расследования. Между тем грамотный финансовый анализ позволяет вскрыть их функцию. Он выявляет отсутствие у таких лиц реальной хозяйственной самостоятельности, несоразмерность операций их доходам и образу жизни, регулярность поступления и быстрого выбытия средств, синхронность действий с другими участниками схемы, повторяемость маршрутов движения денег. Следовательно, **обнаружение финансовых посредников** - это не периферийная задача, а путь к установлению скрытых центров управления преступным оборотом.

Финансовый профиль должен использоваться как **инструмент реконструкции преступной сети**, и в этом заключается одно из важнейших направлений современной правоохранительной деятельности. Под финансовым профилем целесообразно понимать систематизированное описание доходов, расходов, источников поступления имущества, способов его распределения, привычек расходования, характерных контрагентов, ритма операций, имущественного окружения, долговых обязательств, активов, находящихся под прямым и косвенным контролем лица, а также тех каналов, через которые оно осуществляет влияние на экономические

процессы внутри преступной группы. Такой профиль позволяет восстановить не только материальное положение фигуранта, но и его **реальную роль в иерархии сообщества**.

Организатор, куратор, казначей, вербовщик, технический исполнитель, держатель средств, легализатор доходов, подставной владелец имущества - все они оставляют разные финансовые рисунки поведения. У одних преобладает концентрация и распределение средств, у других - прием мелких переводов от множества источников, у третьих - маскировка денежных потоков под законную деятельность, у четвертых - приобретение имущества на третьих лиц. Если следствие ограничивается только содержанием переговоров или данными о совместном участии в эпизодах, оно может увидеть лишь внешнюю сторону организации. Но когда к делу подключается **финансовое профилирование**, структура преступной сети начинает проявляться в ее внутренней логике: кто получает основную выгоду, кто обеспечивает устойчивость схемы, кто выполняет функции распределителя, кто зависит от кого в денежном отношении, кто располагает резервными ресурсами, а кто используется как расходный материал.

Следует особо подчеркнуть, что **параллельные финансовые расследования** должны вестись одновременно с основным уголовным делом, а не после того, как установлены все фактические обстоятельства базового преступления. Отложенный финансовый анализ почти всегда означает потерю времени, а значит - потерю активов, утрату документов, сокрытие выгодоприобретателей, разрушение цепочек движения средств и создание новых прикрывающих конструкций. Преступная среда чрезвычайно быстро приспосабливается к угрозе изъятия имущества: средства дробятся, переводятся на доверенных лиц, выводятся в иные юрисдикционные пространства, обращаются в имущество, переписываются на родственников и аффилированные структуры, преобразуются в трудноотслеживаемые активы. Поэтому финансовое расследование должно разворачиваться с первых же стадий выявления преступной деятельности.

Параллельный характер такого расследования имеет и важное доказательственное значение. Во-первых, он позволяет своевременно зафиксировать происхождение и движение средств, пока следы еще не размыты. Во-вторых, дает возможность выявить дополнительные эпизоды преступной деятельности, не охваченные первоначальной квалификацией. В-третьих, способствует установлению иных участников сообщества, формально не присутствующих в непосредственном совершении основного деяния, но извлекающих из него систематическую выгоду. В-четвертых, позволяет раскрыть механизмы легализации преступных доходов, которые сами по себе образуют самостоятельную сферу общественной опасности. Наконец, в-пятых, финансовое расследование служит основой для принятия обеспечительных мер, без которых даже доказанное преступление рискует

завершиться лишь символическим наказанием при сохранении у преступников материальной базы для дальнейшей деятельности.

Именно поэтому требуется **более активное применение ареста активов и механизмов конфискационного воздействия**. Государство, ограничивающееся лишь обвинительным приговором без реального изъятия преступно нажитого, фактически оставляет преступной среде главный ресурс ее воспроизводства. Организованная преступность опасна не только совершенными деяниями, но и способностью вновь и вновь воссоздавать себя на основе ранее накопленного капитала. Пока этот капитал сохранен, сохраняется возможность оплачивать защиту, коррумпировать отдельных должностных лиц, вербовать новых участников, закупать технические средства, финансировать уклонение от следствия и суда, поддерживать семьи задержанных сообщников для сохранения их лояльности. **Лишение преступной среды имущественной базы** - это не дополнение к уголовному преследованию, а его стратегическое завершение.

При этом арест активов не должен пониматься узко, только как блокирование банковских счетов. В современных условиях активы могут быть распределены между денежными средствами, объектами недвижимости, транспортом, дорогостоящим оборудованием, имущественными правами, долями участия в хозяйственных обществах, предметами роскоши, средствами на электронных кошельках, цифровыми имущественными ценностями, дебиторской задолженностью, объектами, формально принадлежащими третьим лицам, но фактически находящимися под контролем фигурантов. Следовательно, правоохранительные органы должны исходить из расширенного понимания имущественной базы преступной сети. Необходимо своевременно устанавливать не только то, что принадлежит подозреваемому юридически, но и то, чем он распоряжается фактически, что приобретено на подконтрольных лиц, какие активы оплачены за счет преступного дохода и какие имущественные цепочки были созданы для сокрытия их истинного происхождения.

Особую трудность представляет доказывание связи между активом и преступной деятельностью в случаях, когда имущество оформлено на родственников, доверенных лиц или подконтрольные хозяйственные образования. Здесь решающее значение приобретает совокупность косвенных, но взаимно подтверждающих обстоятельств: отсутствие законных источников дохода, несоразмерность расходов официальным заработкам, участие одних и тех же лиц в движении средств, совпадение времени приобретения имущества с поступлением подозрительных денежных сумм, оплата содержания имущества за счет фигурантов, использование ими соответствующих объектов вопреки формальному титулу владения. **Финансовая реконструкция происхождения имущества** в

таких случаях становится центральным доказательственным мостом между основным преступлением и имущественным результатом, подлежащим аресту и последующему изъятию в доход государства.

Нельзя не отметить, что активное использование финансовой разведки имеет не только репрессивное, но и превентивное значение. Когда преступная среда сталкивается с устойчивой практикой быстрого выявления денежных потоков, блокирования счетов, вскрытия схем обналичивания, изъятия имущества, обращения в доход государства активов, скрытых за номинальными владельцами, и неотвратимого разрушения системы финансового обслуживания преступлений, она утрачивает важнейшее преимущество - уверенность в сохранности преступного дохода. А именно ожидание безнаказанного материального результата является для многих участников главным мотивом включения в преступную деятельность. Поэтому **финансовое давление** ослабляет не только действующие преступные сообщества, но и их способность привлекать новых участников, расширять сферы влияния и проникать в легальный экономический оборот.

Следовательно, для силовых ведомств финансовая разведка должна стать не узкоспециальной функцией отдельных подразделений, а сквозным принципом всей работы по противодействию организованной преступности в цифровой среде. Она требует подготовки кадров, владеющих методами финансового анализа; налаживания межведомственного обмена сведениями; своевременного доступа к данным о движении средств; выработки единых методик оценки подозрительных операций; сочетания оперативно-розыскных, следственных и аналитических возможностей; постоянного взаимодействия с финансово-контрольными структурами; технологического оснащения для исследования сложных цепочек расчетов; а также четкого понимания, что деньги в преступной среде - это не просто результат преступления, а его кровь, нерв и воля.

В конечном счете наиболее действенный способ ослабления организованной преступности состоит в том, чтобы разрушить не только ее связь, не только ее организационные механизмы, но прежде всего ее **денежную инфраструктуру**. Можно заменить отдельного исполнителя, можно создать новый закрытый канал общения, можно перенести деятельность на иную площадку. Но если перекрыт поток средств, если разорвана цепь распределения доходов, если уничтожены схемы сокрытия имущества, если изъяты накопленные ресурсы, если каждому участнику становится ясно, что преступный доход не будет ни сохранен, ни легализован, ни передан наследникам и сообщникам, тогда преступная организация теряет главное - свою материальную основу, а вместе с ней и способность к выживанию. Именно в этом заключается подлинная сила финансовой разведки: она бьет не по внешним проявлениям преступности, а по ее сердцевине.

4. РЕКОМЕНДАЦИИ ДЛЯ ОРГАНОВ, ОТВЕЧАЮЩИХ ЗА ГОСУДАРСТВЕННУЮ БЕЗОПАСНОСТЬ

4.1. Рассматривать платформенную криминализацию как фактор национальной безопасности

В современных условиях преступность, действующая в цифровой среде, более не может рассматриваться как совокупность разрозненных эпизодов незаконного оборота, мошенничества, вымогательства, незаконного доступа к сведениям или организации теневых расчетов. **Платформенная криминализация представляет собой качественно иной уровень угрозы**, при котором цифровая среда превращается не просто в место совершения преступления, но в полноценную инфраструктуру управления, координации, маскировки, финансирования и расширения преступной деятельности. Именно в этой связи для органов, отвечающих за государственную безопасность, принципиально важно признать: перед государством стоит не частная уголовно-правовая проблема, а явление, способное затрагивать основы общественной устойчивости, управляемости, суверенитета и защищенности важнейших государственных и общественных систем.

Традиционное восприятие преступной деятельности как сферы, ограниченной задачами уголовного преследования, сегодня стремительно утрачивает объяснительную силу. Цифровые преступные сети действуют не как жестко оформленные объединения, а как гибкие, быстро перестраивающиеся структуры, способные объединять участников из различных регионов и государств, распределять функции между анонимизированными исполнителями, скрывать центры принятия решений и в кратчайшие сроки переносить активность на новые технические площадки. **Это означает, что криминальная сеть, действующая через цифровые платформы, все чаще приобретает свойства, характерные не только для организованной преступности, но и для субъектов скрытого подрывного воздействия**. Она может обеспечивать устойчивую логистику запрещенных товаров и услуг, управлять денежными потоками, влиять на массовое поведение, создавать очаги социальной дестабилизации, формировать каналы нелегального трансграничного взаимодействия и использоваться как прикрытие для куда более опасных форм активности.

Особую значимость приобретает тот факт, что платформенная криминализация подрывает общественную стабильность не всегда через прямое насилие. Во многих случаях ее действие носит рассредоточенный, накопительный и внешне малозаметный характер. Массовое вовлечение граждан в теневые схемы расчетов, распространение наркорынков через цифровые каналы, координация незаконной миграционной помощи, вовлечение несовершеннолетних в преступные поручения, систематическое информационное воздействие на тревожные социальные

группы, стимулирование недоверия к государственным институтам - все это по отдельности может казаться задачей правоохранительного реагирования. Однако в совокупности такие процессы создают **долгосрочный эрозионный эффект**, размывающий правопорядок, норму законопослушания и саму способность государства обеспечивать предсказуемость общественной жизни. Когда значительные группы населения начинают воспринимать цифровую преступную среду как привычный, доступный и малоуязвимый порядок удовлетворения спроса, возникает не просто криминологическая, а политико-безопасностная проблема.

Не менее существен и аспект нелегального трансграничного влияния. Цифровая платформа по своей природе способна преодолевать государственные границы с такой легкостью, с какой традиционные преступные структуры никогда не могли перемещать ни людей, ни ресурсы, ни организационные сигналы. **Трансграничность платформенной криминализации означает утрату прежней локальности угрозы**. Каналы координации, хранилища сведений, участники расчетов, организаторы информационного воздействия, поставщики вредоносных средств и исполнители конкретных поручений могут находиться в разных юрисдикциях, пользоваться правовыми разрывами между государствами и сознательно опираться на различие национальных правовых режимов. В результате преступная деятельность перестает быть внутренним делом одной территории: она становится частью внешнего давления, в котором преступный интерес переплетается с геополитическим, разведывательным или идеологическим расчетом. Для органов государственной безопасности это означает необходимость рассматривать каждую устойчивую цифровую преступную сеть не только с точки зрения состава преступления, но и через вопрос о внешних связях, маршрутах управления, зарубежных центрах технологического обеспечения и потенциальной заинтересованности иностранных структур в сохранении и использовании такой сети.

Отдельного внимания заслуживает скрытое финансирование деструктивной деятельности. Одной из наиболее опасных особенностей цифровых преступных платформ является их способность маскировать происхождение, назначение и движение денежных средств, дробить транзакции, распределять их по множеству звеньев, использовать подставных участников, а также создавать иллюзию несвязанных между собой операций. В этих условиях преступная платформа может выступать **не только источником прибыли для незаконного обогащения, но и механизмом финансового обеспечения подрывной активности**, включая экстремистскую, диверсионную, вербовочную, коррупционную и иную деятельность, направленную против интересов государства. Опасность здесь заключается не только в самих денежных средствах, но и в непрозрачной архитектуре их движения. Чем более анонимизированы,

рассредоточены и технологически опосредованы финансовые каналы, тем легче скрыть связь между организаторами преступной платформы и конечными выгодоприобретателями, в том числе находящимися вне пределов государства. Следовательно, задача органов государственной безопасности состоит не в формальной фиксации факта незаконного оборота средств, а в выявлении всей цепи их функционального назначения: кто аккумулирует ресурсы, кто перераспределяет их, на какие действия они направляются, какие политические, экстремистские или разведывательные интересы могут стоять за кажущейся «обычной» криминальной активностью.

С еще большей остротой вопрос встает там, где платформенная криминализация соприкасается с критически важной инфраструктурой. Под таковой следует понимать не только энергетические, транспортные, финансовые, телекоммуникационные и управленческие системы, но и весь комплекс объектов и процессов, нарушение которых способно вызвать масштабный общественный ущерб, дезорганизацию повседневной жизни, экономический шок или кризис доверия к государству. **Проникновение преступных цифровых сетей в такие сферы недопустимо рассматривать как рядовое посягательство на сведения или имущество**. В условиях высокой взаимосвязанности систем даже ограниченное нарушение их целостности, доступности или управляемости может иметь каскадные последствия. Преступная платформа может использоваться для подбора инсайдеров, приобретения служебных сведений, организации незаконного доступа, закупки технических средств обхода защиты, координации атак на уязвимые узлы, сокрытия следов вмешательства и последующей монетизации причиненного вреда. Но еще опаснее то, что подобная деятельность может служить не конечной целью, а подготовительной фазой для более серьезных операций. Здесь криминальная среда превращается в зону предварительного проникновения, тестирования устойчивости и формирования скрытой агентурной или технической опоры.

Именно поэтому положение о возможности использования криминальных сетей как подставного инструмента иностранных субъектов должно рассматриваться не как теоретическая гипотеза, а как рабочая аналитическая модель. В современной практике крайне редко встречаются жестко разграниченные формы враждебной активности. Напротив, наблюдается их намеренное переплетение, при котором государственно враждебное воздействие стремится действовать чужими руками, через посредников, с максимальным размыванием прямой связи между инициатором и исполнителем. **Преступная цифровая сеть в таких условиях становится удобным маскировочным слоем**, позволяющим одновременно решать несколько задач: обеспечивать отрицание причастности, использовать уже существующие каналы нелегальной логистики, опираться на устойчивые схемы теневого финансирования, привлекать исполнителей

без их полного информирования о конечной цели и переводить действия в плоскость, внешне похожую на «обычную» преступность. Подобная подмена особенно опасна тем, что запаздывание в ее распознавании ведет к неверной квалификации угрозы. Там, где следовало бы включать механизмы контрразведывательного анализа и межведомственного противодействия, государство рискует ограничиться процессуальными мерами по отдельным эпизодам, не затрагивая организующий центр и не нейтрализуя стратегический замысел.

Вследствие этого принципиально важно исходить из того, что гибридное сочетание преступной, экстремистской, разведывательной и информационно-деструктивной активности становится не исключением, а одной из вероятных форм развития платформенной криминализации. Сегодня уже недостаточно выявить только факт преступления; необходимо установить, не выполняет ли соответствующая цифровая сеть более широкие функции - мобилизационные, пропагандистские, разведывательно-поисковые, вербовочные, дестабилизирующие. **Главная опасность гибридизации заключается в том, что разные формы угрозы взаимно усиливают друг друга**. Преступная прибыль подпитывает экстремистские структуры; экстремистская повестка облегчает вербовку в преступную среду; информационное воздействие создает атмосферу недоверия и растерянности, в которой легче скрывать нелегальные операции; разведывательный интерес использует криминальные каналы как уже готовую нелегальную инфраструктуру проникновения. Когда все эти элементы соединяются, государство сталкивается уже не с отдельной преступной схемой, а с многоуровневой системой скрытого воздействия на безопасность страны.

Из этого вытекает ключевой практический вывод: если цифровая преступная сеть начинает выполнять функции логистики, влияния, финансирования и скрытой координации, она должна становиться объектом не только полицейского, но и контрразведывательного внимания. Данное положение имеет не декларативное, а методологическое значение. Оно требует переоценки критериев опасности. Недостаточно анализировать лишь предмет преступления, размер незаконного дохода или число эпизодов. Необходимо выявлять **функциональную роль сети в более широком контуре угроз**. Иными словами, государство должно задаваться вопросом не только о том, что именно нарушено, но и о том, какую инфраструктурную, финансовую, коммуникационную или подрывную роль играет обнаруженная цифровая платформа в системе иных скрытых процессов. Если сеть обеспечивает устойчивые анонимные коммуникации, ведет скрытое распределение ресурсов, связывает участников из разных стран, имеет признаки дисциплины, конспирации, технической адаптивности и устойчивого ядра управления, то перед нами

уже не просто уголовно наказуемая группа, а объект повышенного внимания системы обеспечения национальной безопасности.

Следовательно, органам, отвечающим за государственную безопасность, необходимо институционально закрепить подход, при котором платформенная криминализация рассматривается как самостоятельный фактор угрозы национальной безопасности. Это предполагает прежде всего выработку общего понятийного аппарата, исключающего ведомственную разобщенность и разночтения. Пока одни структуры видят в цифровой сети исключительно рынок запрещенных услуг, другие - схему незаконного оборота средств, а третьи - канал информационного влияния, государство реагирует фрагментарно. **Между тем сама природа угрозы требует целостного, синтетического взгляда**, при котором цифровая платформа оценивается одновременно как среда преступления, система управления, финансовый механизм, канал влияния и потенциальный инструмент внешнего вмешательства. Только в этом случае возможна ранняя диагностика перехода от уголовной опасности к угрозе национальной безопасности.

Кроме того, необходим переход от преимущественно событийного реагирования к опережающему выявлению инфраструктурных признаков угрозы. Слишком часто внимание государства концентрируется на уже совершенных деяниях, тогда как цифровые преступные сети раскрывают свою истинную опасность задолго до наиболее разрушительных проявлений. Повышенное внимание должны вызывать признаки устойчивой анонимной координации, наличие распределенных финансовых каналов, использование технических средств сокрытия маршрутов связи, активное вовлечение посредников, попытки вербовки лиц, имеющих доступ к служебно значимым сведениям или объектам, а также совмещение преступной деятельности с управляемым информационным воздействием. **Ранняя фиксация таких признаков способна предотвратить перерастание криминальной сети в инструмент системной дестабилизации**. Здесь особенно важно преодолеть инерцию ведомственного мышления, при котором каждая выявленная функция сети рассматривается отдельно и не складывается в единую картину.

Не менее важным представляется и усиление аналитической составляющей деятельности органов государственной безопасности. Вопрос о платформенной криминализации не может быть исчерпан только оперативным сопровождением и процессуальным документированием. Нужен глубокий стратегический анализ, позволяющий видеть эволюцию сетей, закономерности их роста, способы адаптации к государственному давлению, взаимосвязь с социальными кризисами, трансграничными конфликтами и изменениями международной обстановки. **Без развитой аналитики государство неизбежно будет бороться с последствиями, а не с механизмом угрозы**. Анализ должен охватывать не только технические и

правовые аспекты, но и социальные, экономические, идеологические, психологические и геополитические измерения. Преступная цифровая платформа живет не в пустоте: она питается общественными трещинами, институциональными слабостями, дефицитом доверия, технологическими уязвимостями и пробелами координации между ведомствами. Именно поэтому противодействие ей требует не механического усиления контроля, а интеллектуально насыщенной, многослойной стратегии государственной защиты.

Наконец, необходимо подчеркнуть, что признание платформенной криминализации фактором национальной безопасности не означает подмены уголовно-правового подхода чрезвычайным или произвольным вмешательством. Напротив, речь идет о повышении точности государственного восприятия угрозы, о приведении правовых и организационных механизмов в соответствие с реальной природой явления. **Государство обязано видеть угрозу такой, какова она есть, а не такой, какой ее удобнее описывать в устаревших классификациях**. Когда преступная сеть берет на себя функции скрытой логистики, финансового посредничества, координации, информационного воздействия и трансграничного сопряжения интересов, она перестает быть исключительно объектом уголовного преследования. Она становится элементом среды, в которой может формироваться сложная, многосоставная и глубоко законспирированная угроза безопасности государства.

Именно поэтому для органов, отвечающих за государственную безопасность, вопрос о платформенной криминализации должен быть поставлен с предельной ясностью и принципиальностью. Речь идет не о модной терминологии и не о расширении привычных форм отчетности. Речь идет о способности государства распознать в цифровой преступной сети зародыш той инфраструктуры, через которую могут осуществляться скрытое влияние, подрыв устойчивости, финансирование деструктивных сил и проникновение во внутренние процессы страны. **Промедление в таком распознавании дорого обходится государству**: оно оплачивается ростом теневой управляемости, проникновением криминального начала в общественные ткани и расширением пространства, в котором внешние и внутренние противники правопорядка находят общий язык. Поэтому признание платформенной криминализации фактором национальной безопасности следует считать не частной рекомендацией, а одним из базовых условий современного государственного самосохранения.

4.2. Создание национальной системы раннего предупреждения

В современных условиях вопрос о создании национальной системы раннего предупреждения о криминализации цифровой среды перестал быть предметом узкопрофессионального обсуждения и превратился в одну из центральных задач государственного самосохранения. Речь идет не просто

о совершенствовании ведомственного наблюдения и не о техническом наращивании возможностей отдельных подразделений. Речь идет о формировании целостного государственного механизма упреждающего выявления угроз, способного распознавать зарождающиеся криминальные процессы еще до того, как они приобретут устойчивость, институциональную завершенность и разрушительный социальный масштаб. Именно здесь пролегает принципиальная граница между государством, которое управляет угрозой, и государством, которое лишь запоздало фиксирует ее последствия.

Цифровая среда уже давно перестала быть лишь пространством коммуникации, обмена сведениями и хозяйственной деятельности. Она превратилась в сложную, многослойную, высокоподвижную среду, в которой противоправные структуры получают возможность стремительно образовываться, маскироваться, рассеиваться, а затем вновь собираться в новых конфигурациях. Их сила определяется не только численностью участников, но и способностью использовать анонимизацию, рассредоточение, заменяемость каналов связи, кодированную лексику, закрытые и полузакрытые сообщества, систему посредников, ложные цели присутствия, а также финансовые и организационные механизмы, скрытые от поверхностного наблюдения. В этих условиях традиционная реактивная модель, основанная на выявлении уже совершенных деяний, становится заведомо недостаточной. **Государственная безопасность требует перехода от запоздалой фиксации к упреждающему распознаванию.**

Национальная система раннего предупреждения должна создаваться как постоянно действующая, межведомственно объединенная, научно обоснованная и правовым образом урегулированная система выявления признаков криминализации цифровой среды. Ее основное предназначение состоит в том, чтобы не просто собирать разрозненные сведения, а выявлять динамику опасных процессов, обнаруживать скрытые связи между отдельными проявлениями, распознавать ранние признаки формирования криминальной инфраструктуры и обеспечивать выработку своевременных управленческих решений. Иначе говоря, такая система должна быть ориентирована не на регистрацию уже оформленного преступного массива, а на распознавание предкриминальных и раннекриминальных состояний цифровой среды.

Первым важнейшим элементом этой системы выступает выявление **индикаторов роста опасных сетей**. Подобные индикаторы не могут сводиться к формальным показателям количества сообщений, числу подписчиков того или иного сообщества либо резкому увеличению посещаемости определенных цифровых площадок. Сам по себе количественный рост еще не означает криминализацию. Поэтому индикативная модель должна строиться как многофакторная система признаков, учитывающая скорость образования новых связей, характер их

плотности, появление посреднических узлов, повторяемость маршрутов передачи сведений, распределение ролей между участниками, возникновение устойчивых контуров подчинения, а также синхронность поведенческих действий в различных сегментах цифровой среды. Особое значение имеет распознавание тех случаев, когда прежде разобщенные массивы пользователей начинают демонстрировать признаки скрытого организационного единства: воспроизводят общие речевые формулы, используют единый набор условных обозначений, перенаправляют аудиторию по сходным траекториям, а также формируют устойчивую систему внутренней специализации. Рост опасной сети - это не механическое расширение присутствия, а усложнение структуры, укрепление внутренних связей и повышение способности к самовоспроизводству. Именно такие процессы и должны улавливаться системой раннего предупреждения.

Не менее значимым является **мониторинг новых схем миграции каналов**. Преступная среда в цифровом пространстве отличается исключительной приспособляемостью. При усилении внимания со стороны государства противоправные структуры редко исчезают; гораздо чаще они меняют площадки присутствия, дробят каналы связи, переходят в закрытые режимы взаимодействия, создают цепочки промежуточных узлов, используют маскировочные сообщества и временные точки сбора. Вследствие этого задача состоит не только в наблюдении за конкретными цифровыми ресурсами, но прежде всего в понимании закономерностей их перемещения, распада и повторного сосредоточения. Национальная система раннего предупреждения должна фиксировать типовые сценарии перехода от открытого распространения сведений к полускрытым формам взаимодействия, от массовой агитации к адресной вербовке, от единого канала оповещения к распределенной сети малых групп, связанных внутренними посредниками. Особенно важно выявлять миграцию не в ее техническом, а в организационном смысле: кто инициирует переход, как перераспределяются роли, каким образом сохраняется управляемость при смене среды, какие категории участников остаются в открытом поле, а какие переводятся в закрытый контур. **Тот, кто не отслеживает маршруты перемещения криминальной коммуникации, неизбежно теряет из виду саму логику развития угрозы.**

Одним из наиболее тревожных ранних признаков криминализации цифровой среды являются **всплески вербовочной активности**. Вербовка в современном цифровом пространстве редко осуществляется в прямой и открытой форме. Чаще она скрывается под видом идеологического вовлечения, псевдосолидарности, обещаний материальной поддержки, риторики принадлежности к «избранному» сообществу, романтизации насилия, демонстрации ложной социальной защищенности или эксплуатации личностной уязвимости. Поэтому система раннего

предупреждения должна быть способна различать простую информационную активность и направленное вовлечение в противоправные практики. Для этого требуется учитывать совокупность признаков: резкое увеличение обращений к определенным возрастным, социальным или профессиональным группам; систематическое использование психологически уязвимых тем; появление последовательных ступеней сближения с аудиторией; перевод общения из публичного режима в индивидуализированный; формирование доверительных контуров; обещание вознаграждения, статуса, защиты или мести; возникновение речевых конструкций, размывающих нравственные и правовые запреты. Необходимо понимать, что вербовка - это не одномоментный акт, а процесс постепенного разрушения внутреннего сопротивления личности. Следовательно, раннее предупреждение должно уметь обнаруживать не только итоговую стадию склонения, но и предшествующие ей фазовые изменения в риторике, адресности и эмоциональной интенсивности взаимодействия.

Исключительно важной задачей становится **анализ резких изменений лексики и смысловых кодов**. Криминальные структуры, действующие в цифровой среде, постоянно преобразуют язык своего общения. Они заменяют прямые обозначения завуалированными выражениями, используют сленговые иносказания, намеренно искажают слова, внедряют многозначные формулы, совмещают бытовую и специальную лексику, создают символические маркеры принадлежности и применяют речевые сигналы для опознавания «своих». Более того, смена языка нередко предшествует смене организационной модели. Когда сообщество начинает вырабатывать новые обозначения, это зачастую свидетельствует либо о переходе к более скрытому режиму деятельности, либо о расширении состава участников, либо о подготовке к совершению новых видов деяний. Следовательно, государственная система раннего предупреждения должна включать глубокий смысловой анализ речевых изменений, способный выявлять не только частотность отдельных слов, но и трансформацию смысловых полей, смещение акцентов, появление новых контекстов употребления, усиление агрессивной, конспиративной, мобилизационной или расчеловечивающей риторики. Особую опасность представляют те случаи, когда прежний язык обсуждения бытовых, культурных или околополитических тем начинает насыщаться намеками на насилие, теневые финансовые операции, нелегальные перемещения, сокрытие личности, шифрованные договоренности и ритуалы внутренней лояльности. Именно в таких переходных зонах часто формируется будущий криминальный контур.

Особое место в архитектуре раннего предупреждения занимает **оценка концентрации подозрительных связей между цифровыми узлами**. В условиях сложной сетевой организации преступность все реже проявляет

себя через линейные иерархии и все чаще действует через распределенные, полицентрические, многоуровневые структуры. Это означает, что угроза может исходить не от отдельного заметного центра, а от совокупности на первый взгляд малозначительных узлов, которые в соединении образуют устойчивую инфраструктуру. Поэтому принципиально важно измерять не только наличие связей, но и их насыщенность, повторяемость, устойчивость, роль в передаче сведений, степень посредничества и функцию в перераспределении потоков. Высокая концентрация подозрительных связей может выражаться в резком уплотнении взаимодействий между ранее слабо связанными сообществами, в возникновении узлов-посредников, через которые проходит непропорционально большой объем координирующих сигналов, в образовании закрытых контуров, где информация распространяется с высокой скоростью и низким уровнем утечки вовне. Для государства крайне важно научиться видеть именно эти структурные уплотнения, потому что в них нередко кристаллизуется ядро будущей противоправной сети. **Опасность рождается не только из содержания сообщений, но и из архитектуры их распространения.**

С этим непосредственно связано **автоматическое выявление признаков координации между внешне несвязанными сообществами**. Это положение имеет особое значение, поскольку современная криминальная среда стремится избегать явной организационной общности. Разные сообщества могут декларировать различные цели, использовать неодинаковую символику, апеллировать к несходным аудиториям и даже внешне конфликтовать друг с другом, оставаясь при этом элементами единой скрытой системы. Их общность может проявляться в синхронности действий, тождестве смысловых поворотов, повторении маршрутных схем перемещения участников, согласованном распространении определенных установок, использовании общих посредников, единой временной дисциплины публикаций, параллельном изменении речевых кодов либо в концентрации одних и тех же финансовых и организационных связей. Поэтому система раннего предупреждения должна быть нацелена на распознавание именно латентной координации - того скрытого организационного единства, которое не лежит на поверхности и потому особенно опасно. В противном случае государство будет видеть разрозненные фрагменты там, где в действительности уже действует целая система.

Однако сама по себе даже самая совершенная система наблюдения не сможет выполнять свое предназначение, если она не будет **интегрирована с правоохранительными базами данных, таможенной информацией, пограничной аналитикой, финансовым мониторингом, сведениями о киберинцидентах и аналитическими материалами по организованным группам риска**. Здесь необходимо подчеркнуть принципиальное

обстоятельство: криминализация цифровой среды никогда не ограничивается лишь цифровой средой. Она почти всегда имеет выход в физическое пространство, в логистику, в перемещение лиц и товаров, в нелегальные финансовые потоки, в использование подставных структур, в коррупционные контакты, в организацию трансграничных связей, в техническое обеспечение противоправной деятельности. Следовательно, цифровой сигнал приобретает подлинную оперативно-аналитическую ценность только тогда, когда он соотносится с иными государственными сведениями и включается в единую картину угрозы.

Интеграция с правоохранительными учетами необходима для установления связи между новыми цифровыми проявлениями и уже известными лицами, способами, маршрутами, предметами преступного посягательства, а также с ранее выявленными эпизодами. Нередко один и тот же субъект, формально меняя средства связи, речевые маски и круг контактов, сохраняет устойчивый поведенческий почерк, который становится различимым лишь при сопоставлении с накопленными массивами сведений. Таможенная информация позволяет выявить корреляции между всплесками активности в цифровой среде и перемещением определенных категорий товаров, оборудования, компонентов, денежных суррогатов, носителей сведений или предметов двойного назначения. Пограничная аналитика дает возможность обнаружить пространственное измерение угрозы: пересечение маршрутов въезда и выезда, кратковременные визиты в чувствительные зоны, повторяемость поездок, нетипичную мобильность определенных групп, а также признаки согласованного движения лиц, связанных неформальными цифровыми контактами. Финансовый мониторинг позволяет вскрывать материальную основу скрытых сетей, выявлять нетипичные транзакционные цепочки, расщепление платежей, использование посредников, концентрацию средств в узловых точках, а также связь между вербовочной активностью и финансовым стимулированием исполнителей. Сведения о киберинцидентах необходимы для понимания технического измерения угрозы: какие ресурсы подвергаются атакам, какие инструменты используются для сокрытия следов, как распространяются вредоносные воздействия, каким образом осуществляется разведка инфраструктуры и подготавливается проникновение в значимые системы. Наконец, аналитика по организованным группам риска обеспечивает стратегическую глубину оценки, позволяя увязывать текущие цифровые сигналы с длительно формирующимися преступными образованиями, их специализацией, экономической базой, кадровым резервом, территориальным влиянием и трансграничными контактами.

При этом интеграция не должна пониматься как механическое слияние всех данных в единое хранилище без правового разграничения, научной методики и организационной дисциплины. Напротив, эффективность

национальной системы раннего предупреждения зависит от четкого правового режима доступа, строгого распределения полномочий, верификации источников, разграничения степеней достоверности, сохранения процессуальной пригодности сведений и выработки единых правил межведомственного обмена. **Сильное государство - это не государство беспорядочного накопления сведений, а государство разумного, законного и целевого обращения с ними.** В противном случае возникает риск либо паралича из-за информационного перенасыщения, либо злоупотреблений, дискредитирующих саму идею предупреждения угроз.

Необходимым условием действенности такой системы является также создание единого методологического контура оценки опасности. Если различные ведомства будут исходить из несовпадающих критериев, использовать разные шкалы риска, по-разному определять подозрительные связи и неодинаково трактовать признаки координации, система утратит связность и превратится в совокупность несоединимых фрагментов. Следовательно, требуется разработка общегосударственного понятийного аппарата, стандартизированных моделей индикаторов, типологии уровней угрозы, процедур межведомственного подтверждения сигналов и единых регламентов передачи материалов для дальнейшего реагирования. Особого внимания заслуживает проблема ложноположительных и ложноотрицательных заключений. Первые порождают необоснованную нагрузку на государственные органы и могут затрагивать законопослушных лиц; вторые, напротив, создают иллюзию благополучия там, где уже складывается опасная сеть. Поэтому национальная система раннего предупреждения должна строиться на принципах непрерывной научной проверки, ретроспективной оценки точности выводов, адаптации индикаторов к изменяющимся формам преступности и постоянного сопоставления прогностических заключений с реальными исходами.

Отдельно следует подчеркнуть, что создание такой системы невозможно без серьезной научной и кадровой основы. Для ее полноценного функционирования требуются специалисты, способные соединять юридическое мышление, криминологический анализ, лингвистическую чувствительность, понимание сетевых структур, навыки работы с большими массивами сведений, знание трансграничной преступности, финансовых схем, миграционных процессов и психологических механизмов вовлечения. Иначе говоря, речь идет не просто о техническом обеспечении государственной функции, а о формировании новой культуры безопасности, в которой предупреждение строится на стыке права, науки, стратегии и управленческой воли. Без такой кадровой основы даже самые совершенные вычислительные средства останутся немыми: они смогут фиксировать шум, но не смогут распознавать смысл угрозы.

Существенным требованием является и поэтапная организация реагирования на сигналы раннего предупреждения. Недопустимо, чтобы любой зафиксированный индикатор автоматически порождал одинаковую по интенсивности реакцию. Система должна различать уровни опасности: от слабых предвестников неблагополучия до признаков сформировавшейся координационной сети. Каждому уровню должны соответствовать свои меры - от углубленного наблюдения и дополнительной верификации до межведомственного оповещения, профилактического воздействия, оперативного сопровождения и инициирования процессуальных механизмов. Это особенно важно в условиях, когда криминализация цифровой среды развивается неравномерно: где-то она выражается в первоначальном накоплении враждебной риторики, а где-то - уже в распределении ролей, логистике, финансировании и подготовке конкретных противоправных действий. Государство обязано уметь соразмерять силу вмешательства степени зрелости угрозы, сохраняя при этом способность к стремительному наращиванию ответа при подтверждении опасных тенденций.

Наконец, принципиально важно осознать стратегический смысл раннего предупреждения. Его назначение не исчерпывается техническим выявлением подозрительных цифровых процессов. Оно состоит в том, чтобы предотвратить превращение разрозненных признаков неблагополучия в полноценную криминальную инфраструктуру - устойчивую, самообновляющуюся, экономически подпитанную, социально укорененную и защищенную внутренними механизмами конспирации. Когда государство не располагает системой раннего предупреждения, оно неизбежно действует после того, как угроза уже окрепла, обзавелась кадровым резервом, запасными каналами, финансовыми опорами и легальными прикрытиями. В такой ситуации цена реагирования возрастает многократно: требуются большие силы, более жесткие меры, длительное восстановление нарушенной безопасности и высокий уровень общественных издержек. Напротив, упреждающее выявление позволяет пресекать опасный процесс в фазе его наименьшей устойчивости - тогда, когда сеть еще не обрела внутреннюю дисциплину, не сформировала прочные источники финансирования и не укоренилась в социальной ткани.

Таким образом, создание национальной системы раннего предупреждения о криминализации цифровой среды должно рассматриваться как одна из ключевых опор современной государственной безопасности. Такая система обязана выявлять индикаторы роста опасных сетей, отслеживать схемы миграции каналов, фиксировать всплески вербовочной активности, анализировать резкие изменения лексики и смысловых кодов, оценивать концентрацию подозрительных связей между цифровыми узлами и автоматически распознавать признаки координации между внешне несвязанными сообществами. В то же время ее действенность возможна

лишь при глубокой интеграции с правоохранительными учетами, таможенными сведениями, пограничной аналитикой, финансовым мониторингом, данными о компьютерных инцидентах и аналитическими материалами по организованным группам риска. **Без раннего предупреждения государство обречено опаздывать. С ранним предупреждением оно получает шанс не догонять угрозу, а опережать ее.** Именно в этом и заключается подлинный смысл ответственной государственной политики в цифровую эпоху.

4.3. Обновление нормативной базы

В условиях стремительной технологизации преступной деятельности и возрастающей связанности цифровой среды с экономическими, политическими и социальными процессами вопрос обновления нормативной базы перестает быть сугубо отраслевой задачей правотворчества. Он становится **вопросом сохранения действенности государства**, его способности защищать общество, пресекать деятельность организованных преступных структур и одновременно удерживать правовой порядок в границах конституционной законности. Там, где право запаздывает, преступность получает не просто временное преимущество - она обретает пространство для укоренения, институционализации и последующего давления на государственные механизмы. Именно поэтому современная нормативная политика в сфере государственной безопасности должна носить не фрагментарный, а системный, опережающий и внутренне согласованный характер.

Особую опасность представляет ситуация, при которой цифровая среда развивается быстрее, чем правовые инструменты ее регулирования. В таком случае формируется разрыв между фактическими возможностями преступных субъектов и юридическими возможностями государства. Этот разрыв особенно заметен при расследовании тяжких транснациональных деяний, совершаемых с использованием распределенных сетевых инфраструктур, обезличенных учетных записей, удаленных средств хранения сведений, а также сложных схем сокрытия цифровой активности. Преступные сообщества целенаправленно используют несовпадение национальных правовых режимов, различия в требованиях к допустимости доказательств, неурегулированность вопросов сохранения электронных следов и медлительность межгосударственных процедур. Следовательно, **обновление нормативной базы должно быть направлено не на символическое «осовременивание» законодательства, а на реальное перекрытие тех правовых пустот, которые уже превратились в рабочий ресурс преступного мира**.

Прежде всего требуется **уточнение правового статуса цифровых следов и процедур их сохранения**. До настоящего времени в ряде правоприменительных ситуаций электронные сведения продолжают

восприниматься через призму устаревших категорий вещественных носителей, хотя их сущность, механизм образования, способы изменения и условия утраты принципиально отличаются от традиционных материальных объектов. Цифровой след не существует в упрощенном виде как «файл» или «сообщение»: он представляет собой сложную совокупность метаданных, журналов событий, сетевых идентификаторов, временных отметок, сведений о последовательности действий, признаков взаимодействия пользователя с системой, параметров маршрутизации и иных технически значимых элементов. Именно поэтому правовое определение цифрового следа должно быть широким, технологически нейтральным и одновременно процессуально конкретным.

Необходимо нормативно закрепить, что цифровые следы являются самостоятельной категорией доказательственно значимой информации, требующей особого порядка выявления, фиксации, изъятия, копирования, удостоверения подлинности, передачи, исследования и хранения. При этом закон должен учитывать их высокую изменяемость, зависимость от настроек информационной среды, возможность автоматического удаления, перезаписи или искажения вследствие обычного функционирования технических систем. **Сохранение цифрового следа - это не техническая формальность, а правовая гарантия истины**. Если сведения не зафиксированы своевременно и надлежащим образом, государство рискует утратить возможность доказать сам факт преступного деяния либо установить причастных лиц.

В этой связи требуется детальная регламентация процедур неотложного сохранения цифровых сведений до получения окончательного процессуального решения об их изъятии или исследовании. Закон должен ясно определить основания, пределы, сроки и порядок вынесения обязательных предписаний о временном сохранении данных операторами связи, владельцами информационных ресурсов, посредниками передачи сведений и иными субъектами, располагающими технической возможностью удержать информацию от уничтожения. Особое значение имеет закрепление требований к непрерывности цепи хранения, к удостоверению неизменности сведений, к документированию каждого действия с цифровыми объектами, а также к разграничению доступа должностных лиц к соответствующим материалам. Без таких норм любое значимое электронное доказательство может быть поставлено под сомнение, а сама уголовно-процессуальная перспектива дела - разрушена.

Не менее настоятельной является задача **совершенствования режимов международного обмена электронными доказательствами**. Современная преступность не признает государственных границ, но именно границы нередко становятся ее самым надежным прикрытием. Сведения о переписке, размещенных материалах, финансовых транзакциях, сведениях о подключении, учетных записях и цифровых маршрутах могут находиться

одновременно в нескольких юрисдикциях, подчиняться различным стандартам защиты информации и выдаваться только при соблюдении разноуровневых процедур. В результате следствие сталкивается с парадоксом: технически нужные сведения существуют, но юридически остаются недоступными или поступают тогда, когда их доказательственное значение уже утрачено.

Выход из этой ситуации требует не только двусторонних и многосторонних договоренностей, но и переосмысления самой логики международного правового взаимодействия. Необходимо развивать такие механизмы, которые позволят ускорять направление запросов, унифицировать минимальные стандарты содержания ходатайств, устанавливать предельные сроки ответа по делам о тяжких преступлениях, признавать юридическую значимость надлежащим образом заверенных электронных пакетов сведений, а также заранее согласовывать перечни данных, подлежащих приоритетному сохранению. **Медлительность в международном обмене доказательствами сегодня равносильна утрате доказательств**. Пока государства согласовывают форму обращения, преступные субъекты меняют устройства, удаляют учетные записи, переводят активы и разрывают цифровые связи, ведущие к организаторам деяния.

Особое место должно занимать нормативное обеспечение прямого, но строго контролируемого взаимодействия компетентных органов с зарубежными обладателями технически значимой информации в случаях, когда промедление объективно создает угрозу для жизни, общественной безопасности, устойчивости критически важных систем или расследования особо тяжких транснациональных преступлений. Вместе с тем такое взаимодействие не должно превращаться в правовую самодеятельность. Оно возможно лишь при ясном определении компетенции, оснований срочности, процессуальной формы подтверждения запроса, порядка последующего судебного или прокурорского контроля и правил использования полученных сведений. Сила государства заключается не в произвольном проникновении в информационную сферу, а в способности действовать быстро, законно и доказуемо.

Следующее принципиальное направление - **закрепление обязанностей платформ по взаимодействию в рамках законных процедур**. В современном цифровом пространстве крупные сетевые площадки, службы обмена сообщениями, хранилища данных, посредники распространения информации и иные владельцы информационных инфраструктур фактически выступают узловыми точками, через которые проходят массивы сведений, представляющих интерес для пресечения преступной деятельности. Однако при отсутствии четко сформулированных обязанностей такая роль становится источником правовой неопределенности. Одни субъекты ссылаются на внутренние правила,

другие - на иностранную юрисдикцию, третьи - на отсутствие технической возможности, четвертые - на неопределенность статуса запрашиваемых сведений. Итог один: правоприменитель сталкивается с затягиванием процедур, фрагментарностью ответов и утратой следственной перспективы.

Поэтому необходимо на уровне закона установить исчерпывающий круг обязанностей указанных субъектов при получении законного и надлежащим образом оформленного требования компетентных органов. К таким обязанностям должны относиться своевременное сохранение определенных категорий сведений, предоставление идентифицирующей и технической информации в установленных законом пределах, обеспечение непрерывной связи с уполномоченными подразделениями, наличие официального представительства или назначенного ответственного лица для взаимодействия с государственными органами, а также исполнение требований об ограничении доступа к материалам, прямо связанным с тяжкими преступлениями, если такие требования основаны на судебном или ином предусмотренном законом решении. **Площадка, извлекающая выгоду из организации информационного общения миллионов лиц, не вправе уклоняться от законного участия в защите общественной безопасности**.

Вместе с тем обязанность взаимодействия не должна пониматься как дозволение на произвольное изъятие любых сведений. Напротив, чем шире технические возможности частных обладателей данных, тем точнее должны быть определены пределы государственного вмешательства. Законодатель обязан закрепить перечни запрашиваемых категорий информации, основания дифференциации доступа к ним, требования к судебному санкционированию в наиболее чувствительных случаях, правила уведомления, если оно допустимо, и порядок последующего обжалования. Только при таком сочетании императивности и правовой определенности можно предотвратить одновременно две крайности: беспомощность государства перед преступными сетями и размывание гарантий частной жизни.

Особую актуальность приобретает **разработка критериев для ускоренных процедур реагирования по тяжким транснациональным преступлениям**. Здесь законодательство должно исходить из того, что не все преступления требуют одинаковой процессуальной скорости и одинакового объема неотложных мер. Там, где речь идет о деяниях, сопряженных с террористической деятельностью, незаконным оборотом оружия, эксплуатацией несовершеннолетних, торговлей людьми, координацией массовых беспорядков, вмешательством в работу критически важных объектов, созданием сетей распространения особо опасных материалов, крупномасштабным хищением финансовых средств либо деятельностью устойчивых транснациональных преступных объединений, промедление в часах и даже минутах может иметь необратимые последствия. Именно

поэтому требуются специальные правовые режимы ускоренного реагирования.

Такие режимы должны базироваться на четко закрепленных критериях. Во-первых, необходимо определить характер общественной опасности деяния, включая масштаб возможного вреда, число потенциальных потерпевших, угрозу жизни и здоровью, способность преступной активности к быстрому расширению. Во-вторых, следует учитывать трансграничный характер инфраструктуры преступления, множественность используемых сетевых узлов, распределенность хранения данных и риск мгновенного перемещения следов в иные юрисдикции. В-третьих, важным критерием должно выступать наличие высокой вероятности безвозвратной утраты доказательств при применении обычной, более длительной процедуры. В-четвертых, подлежит оценке устойчивость преступной структуры, ее организованность, наличие распределения ролей, финансовой базы и механизма сокрытия следов. **Ускоренная процедура должна быть исключением, оправданным только там, где обычная процедура уже не защищает право, а фактически обслуживает преступника своим запозданием**.

При этом ускоренные процедуры должны сопровождаться особыми процессуальными предохранителями. Нужны обязательная письменная мотивировка, кратчайшие сроки последующего судебного контроля, повышенные требования к документированию каждого действия, специальный порядок хранения полученных сведений, возможность проверки соразмерности примененной меры и, если это допустимо без ущерба расследованию, последующее уведомление заинтересованных лиц. Такой подход позволит обеспечить не только оперативность, но и легитимность. Ведь государственная решительность, не опирающаяся на право, рано или поздно оборачивается кризисом доверия; однако и право, не способное действовать своевременно, превращается в ритуал бессилия.

Самостоятельным направлением выступает **нормативное определение повышенно опасных цифровых криминальных экосистем**. Право не может эффективно противодействовать тому, что не умеет точно описать. На практике все более заметны такие цифровые образования, которые нельзя свести ни к единичному преступлению, ни к отдельному участнику, ни к конкретному техническому ресурсу. Речь идет о сложных, самовоспроизводящихся системах, объединяющих средства анонимизации, инфраструктуры распространения запрещенных материалов, нелегальные расчетные механизмы, каналы вербовки, средства обучения преступным навыкам, базы похищенных сведений, инструменты координации нападений, посредников сокрытия происхождения цифровых активов, а также механизмы обхода государственного контроля. Подобные образования функционируют как преступная среда полного цикла: они

вовлекают, обучают, обеспечивают, финансируют, защищают и воспроизводят противоправную деятельность.

Нормативное определение таких экосистем необходимо для того, чтобы правоприменитель мог реагировать не только на отдельные проявления, но и на инфраструктурную основу преступности. Закон должен выделять признаки, по которым соответствующая среда признается повышенно опасной: систематическое обеспечение совершения тяжких преступлений; объединение множества участников в устойчивую структуру; использование специальных средств сокрытия личности и маршрутов передачи сведений; наличие сервисов, обслуживающих противоправные операции; вовлечение неопределенного круга лиц в преступную деятельность; транснациональный охват; высокая скорость восстановления после блокирования отдельных элементов. **Преступность побеждает там, где государство видит только эпизоды и не замечает системы**. Следовательно, норма должна позволять квалифицировать, ограничивать, блокировать и исследовать именно систему как источник постоянной угрозы.

Однако здесь особенно важно соблюсти точность законодательных формулировок. Недопустимо, чтобы под расширительные определения подпадали нейтральные технические средства, законные исследовательские сообщества, профессиональные объединения специалистов по защите информации либо иные субъекты, деятельность которых не направлена на совершение преступлений. Определение повышенно опасной цифровой криминальной экосистемы должно строиться не на внешних признаках сложности или технологичности, а на доказуемой совокупности функциональных характеристик, свидетельствующих о ее служебной направленности на поддержание тяжкой противоправной деятельности. Здесь законодатель обязан проявить высшую степень точности, поскольку любая неопределенность будет одинаково выгодна и преступникам, скрывающимся за правовой расплывчатостью, и недобросовестным правоприменителям, склонным к чрезмерному расширению вмешательства.

Наконец, исключительное значение имеет **регламентация межведомственного доступа к данным в рамках процессуальных гарантий**. Современная система обеспечения государственной безопасности включает множество органов и подразделений, располагающих сведениями различной природы: оперативно-розыскной, следственной, пограничной, таможенной, финансовой, миграционной, налоговой, регистрационной, судебной и иной. Разобщенность этих массивов, ведомственная замкнутость и отсутствие единообразных процедур доступа порождают не просто неудобство, а прямую угрозу эффективности государства. Преступные группы давно научились использовать институциональные разрывы: пока одно ведомство проверяет сведения, другое не располагает основанием для

запроса, третье не имеет технической совместимости, а четвертое связано ограничениями, не снабженными понятным механизмом законного преодоления. В итоге фрагменты информации не складываются в доказательственную картину, а время работает против закона.

Законодатель должен создать такой режим межведомственного доступа, при котором сведения могут передаваться быстро, адресно и только при наличии надлежащих правовых оснований. Для этого необходимы четкие категории данных, разграничение уровней допуска, нормативное закрепление целей использования информации, ведение обязательных журналов обращения к сведениям, установление персональной ответственности должностных лиц за неправомерное получение, распространение или использование данных, а также наличие процедур независимой проверки законности доступа. **Межведомственный обмен не должен быть ни хаотическим, ни парализованным**. Его надлежит строить как строго организованную систему, в которой каждая операция обоснована, прослеживаема и поддается последующему контролю.

Особенно важно определить правила сопряжения различных правовых режимов сведений. Одни данные относятся к тайне связи, другие - к персональным данным, третьи - к банковской тайне, четвертые - к налоговой, пятой категорией выступают сведения оперативного учета, шестой - материалы предварительного расследования. Пока законодатель не выработает ясный механизм их соотнесения, должностные лица будут либо чрезмерно осторожны, опасаясь выйти за пределы полномочий, либо, напротив, склонны к расширительному толкованию своей компетенции. В обоих случаях страдает правопорядок. Поэтому закон должен не просто декларировать возможность межведомственного взаимодействия, а подробно описывать юридические основания, условия, пределы, сроки, способы удостоверения запроса и порядок последующего контроля. Только в этом случае возможно соединить эффективность расследования с незыблемостью процессуальных гарантий.

Вся совокупность перечисленных мер требует единого методологического подхода. Обновление нормативной базы в сфере государственной безопасности не может ограничиваться внесением разрозненных поправок в отдельные законодательные акты. Нужна **цельная концепция правового ответа на цифровизацию преступности**, основанная на нескольких фундаментальных началах. Во-первых, технологическая нейтральность: закон должен быть применим не только к уже известным средствам совершения преступлений, но и к новым формам, которые еще не получили широкого распространения. Во-вторых, определенность: каждое полномочие государства должно иметь ясные границы, исключающие произвольное толкование. В-третьих, соразмерность: глубина вмешательства в информационную сферу должна соответствовать тяжести угрозы и процессуальной цели. В-четвертых, проверяемость: любое действие

по получению, сохранению, передаче и использованию цифровых сведений должно быть документировано и доступно для последующей юридической оценки. В-пятых, согласованность: нормы различных отраслей права не должны вступать в разрушительное противоречие друг с другом.

Именно в этом заключается ключевой императив современной правовой политики: **государство обязано быть быстрее преступника, но не вправе становиться произвольнее закона**. Слишком мягкое регулирование создает для преступных сетей убежище в правовых пробелах; слишком размытое и чрезмерное - подрывает доверие общества, ослабляет легитимность правоохранительной деятельности и провоцирует злоупотребления. Следовательно, обновленная нормативная база должна соединить строгость с точностью, оперативность с подотчетностью, силу с юридической культурой. Только такой подход позволит не просто реагировать на отдельные преступления в цифровой среде, а выстроить устойчивую систему правового противодействия, способную защитить безопасность государства, интересы общества и права граждан от угроз нового исторического масштаба.

4.4. Подготовка кадров нового типа

Стремительное усложнение организованной преступности в условиях всеобщей цифровизации общественных отношений требует коренного пересмотра представлений о кадровом обеспечении органов, отвечающих за государственную безопасность. Преступные сообщества более не ограничиваются устойчивыми иерархиями, территориальной привязкой и традиционными способами сокрытия следов. Они действуют в распределённой среде, используют обезличенные расчёты, применяют закрытые каналы связи, подменяют личность цифровыми масками, выстраивают многоступенчатые схемы перемещения средств и создают сложные контуры влияния, в которых правонарушение, финансовая операция, информационное воздействие и международное посредничество сливаются в единый преступный механизм. В этих условиях **государственная безопасность более не может опираться на узкоспециализированного исполнителя**, подготовленного лишь в рамках одной дисциплины. Исторический момент настоятельно требует формирования нового типа специалиста - профессионала сложного, междисциплинарного, способного мыслить одновременно в правовой, технологической, оперативной, финансовой и поведенческой плоскостях.

Именно поэтому центральной задачей становится подготовка кадров, сочетающих юридическую подготовку, понимание устройства цифровых площадок, навыки разведывательной работы в цифровой среде, опыт финансово-аналитического исследования, знание природы транснациональной преступности, а также способность работать с цифровой лингвистикой и закономерностями сетевого поведения. **Речь идёт**

не о механическом соединении разрозненных знаний, а о формировании качественно новой профессиональной целостности. Такой специалист должен не просто знать отдельные правовые нормы, но понимать пределы допустимости доказательств, особенности национальной и международной подсудности, порядок получения сведений у иностранных поставщиков цифровых услуг, правовые режимы хранения и передачи данных, а также различие между оперативно значимой информацией и доказательством, способным выдержать судебную проверку. Его юридическая подготовка должна быть не формальной, а глубокой, поскольку всякая ошибка в процессуальном оформлении цифрового следа способна разрушить даже безупречно проведённую оперативную разработку.

Однако одного знания права уже недостаточно. **Современный сотрудник, обеспечивающий государственную безопасность, обязан понимать внутреннюю логику цифровых площадок**, их архитектуру, порядок распространения сведений, механизмы ранжирования материалов, способы формирования сообществ, принципы анонимизации пользователей, природу цифрового посредничества и закономерности поведения участников сетевых коммуникаций. Необходимо, чтобы он ясно представлял, как именно преступные структуры используют торговые площадки, мессенджеры, игровые сообщества, файловые хранилища, анонимные форумы, криптографически защищённые каналы связи и иные цифровые среды для подбора участников, распределения ролей, координации действий, сокрытия маршрутов поставок, легализации средств и давления на свидетелей. Без такого понимания государство будет всякий раз опаздывать, реагируя лишь на уже совершённое деяние, тогда как задачей подлинно современной системы безопасности должно быть упреждение.

Не меньшую значимость приобретают навыки разведывательной работы в цифровой среде. **Выявление преступной сети сегодня всё чаще начинается не с очного наблюдения, а с обнаружения слабого цифрового сигнала**, который лишь опытный специалист способен отличить от общего информационного шума. Подготовка кадров нового типа должна включать умение устанавливать связи между разрозненными цифровыми следами, выявлять скрытые узлы коммуникации, распознавать координированные действия, восстанавливать структуру преступных контактов, определять центры принятия решений и отличать реальную управленческую вершину преступного сообщества от подставных фигур. При этом особенно важно развивать у сотрудников способность работать не только с явной информацией, но и с косвенными признаками: временем публикаций, повторяемостью речевых оборотов, характером распределения ролей в переписке, изменением привычных моделей поведения участников, маршрутами перемещения средств и совпадением цифровых событий во

времени. Именно из таких, на первый взгляд незначительных, элементов и складывается доказательная картина современного организованного преступления.

Особого внимания заслуживает финансово-аналитическая подготовка. Организованная преступность давно осознала, что власть в преступной среде держится не только на насилии, но и на способности скрытно перемещать, дробить, маскировать и легализовывать доходы. **Тот, кто не понимает движения денежных потоков, видит лишь внешнюю оболочку преступления, но не его экономическое сердце**. Поэтому сотрудник нового типа должен владеть методами анализа транзакционной активности, уметь прослеживать цепочки движения средств через множественные счета, посреднические структуры, виртуальные активы, фиктивные договорные конструкции и зарубежные юрисдикции. Он обязан различать признаки дробления платежей, выявлять искусственное усложнение расчётов, устанавливать выгодоприобретателя за формально независимыми лицами и организациями, а также понимать связь между финансовой архитектурой преступной группы и её оперативной устойчивостью. Финансовый анализ в современных условиях перестаёт быть вспомогательной областью; он становится одним из главных путей раскрытия организованных структур, поскольку деньги, в отличие от легенд и подставных имён, всегда оставляют след.

Необходимым элементом новой подготовки является и глубокое знание транснациональной преступности. Современное преступное сообщество легко пересекает государственные границы - не обязательно физически, но почти всегда организационно, финансово и информационно. **Преступление в цифровую эпоху часто совершается в одной стране, организуется в другой, финансируется из третьей, а его последствия проявляются в четвёртой**. Следовательно, сотрудник, отвечающий за государственную безопасность, должен понимать различия правовых режимов, особенности международного сотрудничества, формы взаимной правовой помощи, основания и пределы направления межгосударственных запросов, а также типичные способы уклонения от международного преследования. Ему необходимо знать, каким образом преступные сети используют правовые различия между государствами, какие юрисдикции становятся удобными для сокрытия данных, регистрации фиктивных организаций, хранения преступных доходов и размещения управляющей инфраструктуры. Только такая подготовка позволяет перейти от бесплодной констатации «зарубежного следа» к реальному преодолению трансграничных барьеров.

Важнейшей составной частью подготовки кадров нового типа выступает работа с цифровой лингвистикой и сетевым поведением. Это направление нередко недооценивается, хотя именно язык, стиль общения, речевые привычки, ритм коммуникации и модели цифрового присутствия позволяют проникнуть в глубинную структуру преступной среды.

Преступная сеть говорит не только словами, но и паузами, повторениями, умолчаниями, условными обозначениями, изменением тональности и ритуалами цифрового общения. Специалист нового поколения должен уметь выявлять скрытые смысловые конструкции, различать речевые маркеры иносказания, понимать способы сокрытия содержания через кодирование бытовыми выражениями, фиксировать признаки управленческого статуса говорящего, распознавать попытки искусственного изменения речевого облика и устанавливать вероятностную связь между различными цифровыми аккаунтами по лингвистическим и поведенческим признакам. Кроме того, требуется знание закономерностей сетевого поведения: способов вхождения в закрытые сообщества, механизмов завоевания доверия, ролей посредников, особенностей вербовки исполнителей, формирования репутации в незаконной среде, методов устрашения и поддержания внутренней дисциплины. Без понимания этих процессов государство рискует бороться с отдельными эпизодами, но не с логикой воспроизводства преступной системы.

Исходя из изложенного, представляется необходимым ввести специализированные программы подготовки, ориентированные не на абстрактное «освоение цифровых технологий», а на решение конкретных задач государственной безопасности. Такие программы должны строиться по принципу содержательного единства права, оперативной деятельности, финансового анализа, международного взаимодействия и исследования цифровых коммуникаций. **Подготовка должна быть не описательной, а прикладной; не книжной, а деятельностной; не ведомственно замкнутой, а направленной на реальную межотраслевую координацию**. В учебный процесс целесообразно включать разбор реальных преступных схем, моделирование кризисных ситуаций, исследование сложных массивов цифровых данных, восстановление цепочек международного взаимодействия, анализ судебной практики по вопросам допустимости цифровых доказательств и оценку типичных процессуальных ошибок. Специалист нового типа формируется не лекционным назиданием, а многократным прохождением через интеллектуально сложные и близкие к действительности профессиональные ситуации.

Особую роль должны сыграть ведомственные магистратуры и курсы повышения квалификации, выстроенные с учётом потребностей действующих сотрудников. Здесь следует подчеркнуть, что кадровое обновление не может быть сведено только к набору молодых специалистов. **Государственная система безопасности нуждается не просто в притоке новых кадров, но и в глубоком переоснащении уже действующего профессионального корпуса**. Следователь, оперативный сотрудник, эксперт, прокурорский работник, аналитик, сотрудник подразделения финансового контроля - все они должны получать возможность планомерного углубления знаний в смежных областях. Ведомственная

магистратура в данном случае призвана стать не формальной ступенью образования, а пространством выращивания профессиональной элиты, способной соединять науку, практику и стратегическое мышление. Курсы повышения квалификации, в свою очередь, должны иметь не общий, а профильный характер, быть краткосрочными по форме, но интенсивными по содержанию, своевременно обновляться с учётом появления новых преступных схем, изменения судебной практики и развития средств сокрытия цифровой активности.

Не менее значимой представляется практика совместных учений. Современная организованная преступность побеждает государство прежде всего там, где государственные органы действуют разобщённо, где информация распылена, полномочия сталкиваются, а профессиональные языки разных ведомств не совпадают. **Совместные учения необходимы для того, чтобы превратить ведомственное соседство в подлинное профессиональное взаимодействие**. В рамках таких мероприятий должны моделироваться ситуации раскрытия многоэпизодных преступных схем, выявления трансграничных финансовых потоков, получения данных у иностранных поставщиков услуг, изъятия и фиксации цифровых носителей, пресечения координированных преступных кампаний, а также защиты свидетелей и потерпевших в условиях информационного давления. Особенно важно, чтобы в учениях участвовали не только представители силовых структур, но и специалисты в области финансового мониторинга, судебной экспертизы, международного права, лингвистического исследования текстов и поведенческого анализа. Лишь в таком составе возможно выработать единое понимание последовательности действий, границ компетенции и механизмов передачи результатов между участниками процесса.

Обязательной должна стать и подготовка по международным механизмам запроса данных. Этот вопрос нельзя оставлять на периферии профессионального образования, поскольку именно незнание процедур, сроков, требований к форме запроса и особенностей взаимодействия с иностранными компетентными органами зачастую приводит к невосполнимой утрате сведений. **В цифровом расследовании время нередко решает всё: запоздалый запрос означает исчезнувшие журналы событий, удалённые учётные записи, уничтоженные следы переписки и выведенные за пределы досягаемости средства**. Поэтому сотрудники должны быть обучены как базовым принципам международной правовой помощи, так и практическим вопросам: определению надлежащего адресата, обоснованию срочности, соблюдению требований к содержанию запроса, обеспечению сохранности получаемых сведений, переводу и легализации документов, а также согласованию международных процедур с требованиями национального уголовного процесса. Особое значение имеет выработка у сотрудников навыка раннего распознавания ситуаций, в которых

иностранный элемент присутствует уже на начальном этапе, хотя внешне дело может выглядеть как внутреннее.

Исключительно важны и тренинги по цифровой доказательственной гигиене. Под этим следует понимать совокупность профессиональных правил, направленных на недопущение утраты, искажения, загрязнения или процессуального обесценивания цифровых сведений. **Цифровое доказательство хрупко не в материальном, а в юридическом и информационном смысле**: его легко испортить неосторожным действием, неверной фиксацией, неправильным извлечением, отсутствием документированной цепи хранения, некорректной интерпретацией метаданных либо использованием неподтверждённых методов исследования. Подготовка сотрудников должна включать устойчивые навыки обращения с электронными носителями, удалёнными хранилищами, журналами событий, данными геолокации, перепиской, мультимедийными файлами и сведениями о сетевой активности. Необходимо обучать правилам документирования каждой операции, разграничению исходных и рабочих копий, обеспечению воспроизводимости результатов, взаимодействию следователя и эксперта, а также заблаговременному выявлению процессуальных рисков. Без такой культуры невозможно обеспечить ни надёжность расследования, ни доверие суда к представленным материалам, ни, в конечном счёте, законность государственного вмешательства.

Вместе с тем подготовка кадров нового типа не должна сводиться лишь к расширению перечня дисциплин. Необходимо изменение самой образовательной философии. **Главной целью должно стать воспитание профессионала, способного мыслить системно, действовать законно, анализировать глубоко и предвидеть развитие преступной ситуации**. Такой специалист должен уметь быстро переходить от нормы права к цифровому следу, от цифрового следа к финансовой схеме, от финансовой схемы к международному элементу, от международного элемента к стратегии пресечения всей преступной сети. Ему необходимо не только владеть знаниями, но и обладать интеллектуальной дисциплиной, устойчивостью к информационному перенасыщению, способностью к межведомственному взаимодействию, привычкой к проверке гипотез, вниманием к деталям и ответственностью за каждое процессуальное решение. Подготовка такого кадра - задача сложная, затратная и длительная, однако иной путь означал бы сознательное согласие государства на хроническое отставание от преступности.

В научном и практическом отношении очевидно, что современная борьба с организованной преступностью требует не просто следователя и не просто специалиста по вычислительной технике, а профессионала гибридного профиля. Но и это определение нуждается в уточнении. **Речь должна идти не о «гибридности» как случайном соединении функций, а о целостной**

профессиональной модели нового государственного защитника, в котором соединяются правовед, аналитик, исследователь цифровой среды, знаток международных механизмов, специалист по финансовым потокам и тонкий интерпретатор речевого и поведенческого материала. Именно такой кадр способен не только реагировать на преступление, но и распознавать его зарождение; не только собирать сведения, но и превращать их в доказательства; не только видеть отдельный эпизод, но и вскрывать всю инфраструктуру преступного сообщества.

Следовательно, вопрос подготовки кадров нового типа является не частной темой образовательной политики, а одним из центральных вопросов национальной безопасности. От того, сможет ли государство создать такую кадровую систему, зависит не только успешность расследования отдельных дел, но и способность страны сохранять суверенитет в условиях цифровой трансформации преступности. **Кадровый вопрос здесь есть вопрос стратегический, вопрос правопорядка, вопрос доверия граждан к государству и вопрос исторической дееспособности самой системы безопасности**. Там, где готовят специалиста вчерашнего дня, государство обречено вести борьбу с преступностью вчерашними средствами. Там же, где формируется специалист нового типа, появляется возможность не догонять угрозу, а опережать её, не латать последствия, а разрушать преступные конструкции в самом основании. Именно к такой модели и должна быть обращена воля государственных институтов, научного сообщества и всей системы профессионального образования.

5. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО: РЕКОМЕНДАЦИИ В РАМКАХ ИНТЕРПОЛА И ДРУГИХ МЕЖДУНАРОДНЫХ СТРУКТУР

5.1. Усиление роли Интерпола в координации платформенно-ориентированных расследований

В современных условиях транснациональной цифровизации преступности вопрос о международном сотрудничестве в сфере противодействия преступным сообществам, использующим коммуникационные платформы в качестве среды функционирования, вербовки, координации, маскировки и перераспределения ролей, приобретает не просто прикладное, но принципиально-цивилизационное значение. Уже недостаточно рассматривать международное полицейское взаимодействие как совокупность формальных процедур передачи запросов, получения справочной информации либо содействия в розыске отдельных лиц. Подобное, во многом архаичное, понимание международного сотрудничества стремительно утрачивает адекватность перед лицом новой преступной реальности, в которой сама преступная деятельность все чаще выстраивается не вокруг устойчивой географической локализации, а вокруг цифровой архитектуры платформ, распределенных каналов связи,

псевдоанонимных учетных записей, временных сетевых сообществ и быстро мигрирующих кластеров участников.

Именно поэтому Интерпол в современных условиях должен осмысляться и использоваться не только как канал межгосударственной передачи информации, но прежде всего как **международный координационно-аналитический центр**, способный выявлять, сопоставлять и интерпретировать трансграничные закономерности существования цифровых преступных экосистем. Речь идет о переходе от реагирования на уже совершенные деяния к формированию системы опережающего аналитического сопровождения расследований, где особое внимание уделяется не единичному эпизоду, а преступной инфраструктуре как таковой: ее узлам, каналам устойчивости, механизмам воспроизводства, правилам адаптации и способам ухода от национального уголовного преследования.

В этой связи в рамках Интерпола представляется целесообразным инициировать создание специализированного направления, предметом которого станут **преступные экосистемы на цифровых коммуникационных платформах**. Подобное направление должно быть ориентировано не на исследование отдельных категорий преступлений в их традиционной отраслевой изоляции, а на выявление той общей организационной среды, в которой объединяются незаконный оборот наркотических средств, торговля людьми, вымогательство, мошенничество, незаконный оборот персональных данных, экстремистская и террористическая агитация, вовлечение несовершеннолетних в противоправную деятельность, а также иные формы криминальной активности. Практика убедительно показывает: одна и та же платформа, один и тот же канал связи, одна и та же модель анонимизации могут обслуживать сразу несколько самостоятельных направлений преступной деятельности. Следовательно, аналитическая работа должна вестись не только по юридическому составу деяния, но и по типу цифровой среды, в которой возникает и воспроизводится преступная сеть.

Создание такого специализированного направления необходимо наполнить не декларативными, а строго институциональными полномочиями. Его задачей должно стать формирование методических подходов к выявлению платформенной преступной организации, накопление типовых сценариев функционирования цифровых криминальных сообществ, разработка понятийного аппарата, пригодного для унифицированного межгосударственного использования, а также выработка согласованных процедур оперативного и следственного реагирования. Особая значимость данного направления обусловлена тем, что преступные сообщества давно научились использовать различия национальных правопорядков как источник собственной устойчивости. Пока одно государство квалифицирует определенную активность как

подготовку к тяжкому преступлению, другое может оценивать ее как административно наказуемое либо вообще правомерное деяние; пока в одной юрисдикции сохраняются сведения о сетевой активности, в другой они безвозвратно уничтожаются в силу истечения кратких сроков хранения; пока одни органы видят лишь отдельный цифровой след, преступная сеть уже успевает рассредоточиться между несколькими государствами. В этой асимметрии процедур и подходов преступность находит для себя пространство почти безнаказанного движения. Следовательно, Интерпол должен стать тем институтом, который сдерживает указанную асимметрию и преобразует разрозненность в координированную систему знания и действия.

Одним из важнейших направлений такой деятельности должно стать **формирование международных профилей угроз по типовым преступным моделям**, возникающим в цифровой платформенной среде. Под международным профилем угрозы следует понимать не краткое описание опасного явления, а сложный аналитический документ, отражающий структурные характеристики преступной модели, стадии ее жизненного цикла, типичную ролевую композицию участников, используемые средства конспирации, признаки расширения сети, способы вовлечения новых лиц, особенности распределения прибыли, каналы легализации преступных доходов, а также факторы, свидетельствующие о скором преобразовании одной преступной формы в другую. Такие профили должны строиться на основе сопоставления материалов из различных государств, поскольку лишь транснациональная перспектива позволяет распознать повторяющиеся конфигурации, незаметные в пределах одной национальной уголовной статистики.

Значение профилей угроз трудно переоценить. Они позволяют перевести борьбу с преступностью из режима описания фактов в режим распознавания моделей. Иными словами, следствие и оперативные подразделения получают возможность видеть не только то, что уже произошло, но и то, во что наблюдаемая коммуникационная активность может перерасти в ближайшей перспективе. Если выявляется характерная комбинация признаков - например, резкое увеличение числа закрытых групп, появление посреднических учетных записей, унификация речевых формул, переход к коротким временным окнам взаимодействия, синхронная миграция участников между площадками, использование множественных цифровых личин, - это должно рассматриваться не как случайное нагромождение обстоятельств, а как симптом становления определенной преступной модели. Именно в этом и состоит преимущество аналитически зрелого международного взаимодействия: оно позволяет научиться распознавать преступность до того, как она закрепится в максимально опасной организационной форме.

Наряду с этим в рамках Интерпола необходимо разработать **унифицированные индикаторы цифровых криминальных сетей**. Без общего набора индикаторов любое международное взаимодействие рискует остаться пленником терминологической разобщенности. Сегодня одно государство акцентирует внимание на содержании сообщений, другое - на маршрутах цифрового перемещения данных, третье - на финансовых следах, четвертое - на особенностях сетевой координации. Между тем преступная сеть существует как совокупность взаимосвязанных признаков, и ее надежное выявление возможно лишь при соединении содержательных, структурных, поведенческих, временных, технических и транзакционных показателей.

Унифицированные индикаторы должны охватывать, по меньшей мере, несколько измерений. Во-первых, это **структурные индикаторы**, отражающие наличие устойчивых узлов координации, иерархии либо, напротив, распределенной сетевой организации с резервными центрами управления. Во-вторых, **поведенческие индикаторы**, позволяющие фиксировать типовые сценарии цифровой активности: синхронность публикаций, повторяемость кодовых формул, алгоритмы включения новичков, дисциплину удаления следов, цикличность смены каналов связи. В-третьих, **содержательные индикаторы**, указывающие на использование специфического словаря, конспиративных обозначений, эвфемистических конструкций и маскировочных речевых стратегий. В-четвертых, **технические индикаторы**, связанные с характером учетных записей, шаблонами регистрации, однотипностью устройств, средствами сокрытия местоположения, особенностями подключения и способами обхода ограничений. В-пятых, **транзакционные индикаторы**, раскрывающие связь между коммуникационной активностью и движением денежных средств, цифровых активов, платежных суррогатов, предоплаченных инструментов и иных форм расчета. Наконец, в-шестых, **эволюционные индикаторы**, позволяющие оценивать способность сети к адаптации, расщеплению, повторной сборке и переносу активности на новые платформы после блокировки прежних.

Разработка подобных индикаторов имеет не только методическое, но и доказательственное значение. В условиях, когда преступные сообщества все реже оставляют прямые признательные следы, а все чаще функционируют через намеки, кодовые конструкции, разрозненные цифровые эпизоды и распределенные роли, именно совокупность индикаторов позволяет построить обоснованную картину организованной преступной деятельности. И здесь особенно важно подчеркнуть: международное правоохранительное взаимодействие должно стремиться не к механическому обмену массивами необработанных сведений, а к согласованному использованию таких показателей, которые обладают устойчивой интерпретационной ценностью в разных юрисдикциях. Только

тогда международное сотрудничество становится не накоплением разрозненных сведений, а подлинным производством юридически и криминалистически значимого знания.

Особого внимания заслуживает предложение о создании **защищенных каналов быстрого обмена платформенными артефактами и аналитическими материалами**. Под платформенными артефактами в данном случае следует понимать не только сообщения, изображения, звуковые записи, видеоматериалы, сведения об учетных записях и цифровых связях между ними, но и значительно более сложные объекты: метки времени, последовательности редактирования, признаки удаления или восстановления данных, характер взаимодействия с публикациями, схемы перехода пользователей между каналами, цифровые следы администрирования сообществ, особенности модерации, признаки распределенного управления и иные элементы, способные раскрыть внутреннее устройство преступной сети.

Необходимость именно быстрого, а не исключительно формально защищенного обмена обусловлена тем, что цифровая преступная среда живет в совершенно иных временных режимах, чем традиционная межгосударственная правовая помощь. Там, где преступная группа способна за несколько часов удалить массив данных, сменить платформу, переименовать каналы, перераспределить роли и раствориться в новом коммуникационном контуре, месячное ожидание межгосударственного ответа фактически означает утрату доказательственной перспективы. И потому речь должна идти о создании особого процессуально и технологически защищенного механизма передачи критически важной информации в режиме, максимально приближенном к реальному времени. Иначе международное сотрудничество будет неизбежно проигрывать преступности не по содержанию, а по темпу, а темп в цифровой среде - это уже не техническая подробность, а сама сущность эффективности.

Однако создание таких каналов невозможно без строгой правовой регламентации. Здесь недопустимы ни правовая расплывчатость, ни соблазн подменить законность оперативной expediency - впрочем, само это иностранное слово здесь уместнее заменить точным русским выражением: соображениями сиюминутной целесообразности. Напротив, требуется тщательно выстроенная система допуска, разграничения уровней доступа, учета целей использования сведений, фиксации всех действий с полученной информацией, проверки достоверности происхождения цифровых материалов, поддержания их неизменности и соблюдения требований национального и международного права о защите прав личности. В противном случае правомерная задача усиления борьбы с транснациональной преступностью рискует вступить в опасное противоречие с началами законности, соразмерности и судебного контроля.

Сила международного сотрудничества должна измеряться не произволом инструмента, а точностью его правового устройства.

Не менее важным направлением представляется **выпуск международных аналитических бюллетеней**, посвященных новым схемам маскировки, миграции и реорганизации преступных сообществ в цифровой среде. Такие бюллетени не должны сводиться к общим обзорам либо к констатации известных угроз. Их задача - обеспечивать государства своевременной, научно обработанной и практически применимой информацией о новых способах сокрытия преступной активности, о преобразовании языковых кодов, об использовании легальных цифровых сервисов в противоправных целях, о трансформации путей вербовки, о переходе от открытых каналов к полузакрытым и полностью закрытым коммуникационным контурам, о методах фрагментации сетей после разоблачения, о технологиях повторного разворачивания сообществ под новым обозначением и с новым визуальным обликом.

Научная и практическая ценность таких бюллетеней состоит в том, что они превращают единичный национальный опыт в коллективный международный ресурс. Если преступная группа отработала эффективную схему сокрытия в одной стране, нет никаких оснований сомневаться, что в кратчайшие сроки данная схема будет воспроизведена в другой юрисдикции, особенно если между участниками преступной среды уже налажен постоянный обмен опытом. Преступность давно усвоила урок международной кооперации - и усвоила его порой лучше, чем сами государства. Именно поэтому каждое промедление с аналитическим распространением сведений об обнаруженных схемах объективно работает на укрепление транснациональной преступной адаптивности. Международный аналитический бюллетень в этом смысле выступает не просто информационным продуктом, а средством предупреждения институциональной слепоты, когда государственные органы разных стран поочередно сталкиваются с одной и той же моделью, но всякий раз как будто впервые.

Следует подчеркнуть и то обстоятельство, что усиление роли Интерпола в координации платформенно-ориентированных расследований должно опираться на более широкий круг международных структур. В зависимости от характера угрозы и предмета расследования необходима тесная сопряженность с региональными полицейскими объединениями, международными судебными и надзорными механизмами, специализированными органами по противодействию легализации преступных доходов, структурами, занимающимися защитой детей, пресечением торговли людьми, борьбой с незаконным оборотом наркотических средств и предупреждением террористической деятельности. Однако координирующая роль Интерпола в данной системе представляется особенно значимой именно потому, что он способен связать

разнородные направления борьбы в единую картину платформенной преступной среды. Там, где отраслевые международные механизмы видят отдельные фрагменты угрозы, Интерпол потенциально способен увидеть ее архитектуру.

Отсюда вытекает и еще один принципиальный вывод. Для повышения результативности международного сотрудничества Интерполу необходимо развивать не только каналы взаимодействия между государствами, но и общие аналитические стандарты, единые подходы к описанию цифровых артефактов, согласованные формы представления сведений, совместимые модели категоризации угроз и общую методику интерпретации платформенной криминальной активности. Без этого обмен сведениями будет оставаться количественно насыщенным, но качественно фрагментарным. Иначе говоря, государства смогут передавать друг другу огромные массивы данных, но не смогут в полной мере извлекать из них доказательственное и прогностическое значение. В эпоху цифровой преступности ценность имеет не просто объем полученной информации, а способность международного сообщества прочесть в этой информации скрытую организационную логику преступной сети.

В конечном счете усиление роли Интерпола в координации платформенно-ориентированных расследований должно рассматриваться как насущная необходимость, продиктованная самой природой современной преступности. Цифровые преступные сообщества стремятся к безграничности, к растворению в транснациональном коммуникационном пространстве, к использованию различий между правовыми системами как средства собственной защиты. Ответ на эту стратегию не может быть локальным, медленным и разобщенным. Он должен быть столь же системным, сколь системна сама угроза; столь же динамичным, сколь динамична преступная миграция между платформами; столь же интеллектуально насыщенным, сколь изощренны способы цифровой маскировки.

Поэтому **Интерпол должен быть переосмыслен как пространство стратегического анализа транснациональных цифровых преступных архитектур**, где международное сотрудничество перестает быть вторичным приложением к национальному расследованию и становится самостоятельным условием его результативности. Лишь при таком подходе можно говорить о подлинном, а не декларативном укреплении международной уголовно-полицейской координации. И если государства действительно намерены противостоять преступности XXI века, они обязаны признать очевидное: сегодня борьба идет уже не только за раскрытие отдельного преступления, но и за способность международного правопорядка понимать, опережать и разрушать цифровые формы организованной преступной власти. Именно в этом - **ключевая задача современного международного сотрудничества** и одно из важнейших

направлений дальнейшего развития Интерпола как института глобальной правозащитной и правоохранительной ответственности.

5.2. Совместные международные оперативные группы

В современных условиях борьба с транснациональной организованной преступностью более не может вестись средствами исключительно национального уголовного преследования. **Преступная сеть давно перестала совпадать с границами государства**, а потому и противодействие ей не может оставаться заключённым в пределах одной юрисдикции. Там, где преступное сообщество распределяет функции между организаторами, посредниками, техническими исполнителями, финансовыми операторами, перевозчиками, вербовщиками и легализаторами доходов в разных странах, любое разрозненное расследование неизбежно оказывается фрагментарным. Оно способно выявить исполнителя низового звена, пресечь отдельный канал, изъять часть материальных следов, но не в состоянии разрушить саму систему. **Изолированное национальное расследование слишком часто поражает только периферию, оставляя нетронутыми центр управления, финансовое ядро, техническую инфраструктуру и механизмы воспроизводства преступной деятельности**. Именно поэтому особое значение приобретают совместные международные оперативные группы, создаваемые при координации Интерпола и иных межгосударственных и региональных механизмов правоохранительного взаимодействия.

Подобные группы представляют собой не просто форму обмена сведениями между ведомствами разных государств, а качественно иной уровень согласованной деятельности, при котором расследование с самого начала строится как единый процесс, а не как механическая сумма параллельных национальных дел. Их назначение состоит в том, чтобы соединить в одном оперативно-правовом контуре возможности правоохранительных органов нескольких государств, подразделений финансовой разведки, специализированных киберподразделений, специалистов по обороту и сокрытию цифровых имущественных ценностей, цифровых криминалистов, а также прокуроров и иных должностных лиц, обеспечивающих допустимость, относимость и надлежащую процессуальную форму международных доказательств. **Только такое соединение сил позволяет перейти от эпизодического реагирования к системному демонтажу преступной сети**.

Участие правоохранительных органов нескольких государств в составе совместной группы обусловлено самой природой транснационального преступления. Одно государство может располагать сведениями о перевозке, другое - о банковских операциях, третье - о размещении вычислительных мощностей, четвёртое - о местонахождении организатора, пятое - о конечной легализации доходов через имущество, подконтрольные

хозяйствующие субъекты или подставных лиц. Пока эти сведения существуют раздельно, преступное сообщество сохраняет преимущество: оно видит всю цепь целиком, а государственные органы - лишь отдельные фрагменты. Совместная международная оперативная группа устраняет эту асимметрию, создавая условия для синхронного сопоставления данных, для выдвижения единой доказательственной версии, для согласованного распределения задач между национальными сегментами расследования и для одновременного проведения процессуальных и оперативных мероприятий. **Смысл такой группы не в дипломатической вежливости между ведомствами, а в восстановлении утраченной целостности правоохранительного зрения**.

Принципиально важным элементом таких групп являются подразделения финансовой разведки. В структуре современной организованной преступности денежный поток давно стал не просто следствием преступления, но его организационной основой. Через движение денежных средств выявляются выгодоприобретатели, посредники, схемы расщепления платежей, точки конвертации, маршруты вывода капитала, связи между внешне несвязанными эпизодами и подлинный масштаб деятельности сети. Там, где показания соучастников могут быть неполными, ложными или мотивированными, финансовые следы обладают особой доказательной устойчивостью. Они фиксируют объективную логику преступного оборота. Поэтому участие финансовой разведки необходимо не только для установления подозрительных операций, но и для построения карты финансовой архитектуры преступного сообщества: от первоначального поступления преступного дохода до его сокрытия, рассредоточения, превращения в имущество, фиктивных обязательств, займов, сделок с ценными бумагами, драгоценными металлами, предметами роскоши и цифровыми имущественными единицами. **Лишить преступную сеть дохода - значит лишить её способности к расширению, подкупу, вербовке и восстановлению после силового удара**.

Не менее значима роль специализированных киберподразделений. Существенная часть транснациональной преступной деятельности сегодня координируется через распределённые средства связи, закрытые сетевые сообщества, анонимизирующие механизмы, удалённые хранилища данных, подставные учётные записи, технически маскируемые узлы доступа и сложные схемы цифрового посредничества. Даже тогда, когда речь идёт о традиционных преступлениях - торговле людьми, незаконном обороте наркотических средств, оружия, культурных ценностей, редких биологических ресурсов, контрабанде табачной продукции, мошенничестве, вымогательстве, легализации преступных доходов, - цифровая среда становится пространством вербовки, координации, финансирования, сокрытия и распределения ролей. Следовательно, без киберподразделений невозможно своевременно обнаружить

инфраструктуру преступной сети, установить технические зависимости между участниками, выявить используемые средства шифрования, определить точки администрирования закрытых площадок, пресечь удалённое уничтожение данных и обеспечить оперативное реагирование на стремительно меняющуюся конфигурацию цифровых следов. **Там, где преступность укрывается за технической сложностью, государство обязано отвечать не отставанием, а превосходством в компетентности**.

Особое место в составе совместных международных оперативных групп занимают специалисты по цифровым имущественным ценностям и их обороту. Использование таких средств в преступной среде связано не только с попытками маскировки происхождения активов, но и с созданием параллельной финансовой экосистемы, в которой традиционные меры банковского контроля оказываются недостаточными. Перевод преступного дохода в цифровую форму, дробление средств по множеству адресов, применение смешивающих сервисов, промежуточных обменных площадок, фиктивных сделок, многоступенчатых переводов и инструментов распределённого учёта позволяет преступным сетям затруднять идентификацию выгодоприобретателя и географию контроля. Однако ошибочно считать такую среду абсолютно непрозрачной. Напротив, при наличии надлежащей специальной подготовки, доступа к аналитическим инструментам, международного обмена сведениями и своевременного судебно-процессуального реагирования возможно прослеживание значительной части цифровых имущественных потоков, установление узловых адресов, выявление связей между операциями и последующее наложение ареста на соответствующие активы. **Для преступника цифровая форма имущества кажется убежищем; для подготовленного следствия она может стать картой его собственных перемещений и связей**.

Цифровые криминалисты в рамках таких групп выполняют задачу, без которой невозможна надёжная материализация электронных следов в судебно значимую доказательственную систему. Их функция не сводится к техническому извлечению данных из изъятых устройств. Речь идёт о научно обоснованной фиксации, сохранении, анализе и интерпретации цифровых объектов с соблюдением строгих требований к непрерывности хранения, воспроизводимости результатов, проверяемости методики, идентификации источника происхождения сведений и исключению неконтролируемого изменения содержимого. В условиях международного расследования значение такой работы возрастает многократно, поскольку любая ошибка в процедуре извлечения, копирования, верификации или описания цифрового массива может привести к утрате доказательственной силы материалов в иностранной юрисдикции. Именно цифровой криминалист превращает хаос электронных фрагментов - переписку, журналы соединений, навигационные данные, сведения о входах в учётные записи, остаточные файлы, удалённые записи, метаданные изображений и

документов - в стройную систему фактов, пригодных для судебной проверки. **Если современное преступление оставляет след в памяти устройства и в сетевой инфраструктуре, то цифровая криминалистика становится языком, на котором этот след начинает говорить в суде**.

Неотъемлемым участником совместной международной оперативной группы должны быть прокуроры, либо иные процессуальные руководители, способные сопровождать международное доказывание с момента выдвижения версии до представления материалов в суд. Их присутствие необходимо потому, что транснациональное расследование терпит поражение не только от недостатка сведений, но и от несогласованности правовых режимов. Доказательство, полученное в одной стране, может оказаться непригодным в другой вследствие различий в порядке санкционирования следственного действия, требованиях к фиксации, стандартах защиты прав личности, объёме судебного контроля, допустимости специальных методов получения информации или порядке сертификации цифровых материалов. Прокурор в составе международной группы должен заранее выстраивать процессуальную стратегию: определять, какие сведения и в каком порядке запрашивать, какие действия проводить синхронно, где необходимо предварительное судебное разрешение, как обеспечивать цепь хранения вещественных доказательств, как формулировать международные поручения, каким образом избежать дублирования или, напротив, пробелов в доказательственной базе. **Оперативный успех, не превращённый в допустимое доказательство, - это не победа, а лишь шумный, но бесплодный эпизод**.

Эффективность совместных международных оперативных групп во многом определяется тем, по какой аналитической модели строится их работа. Одной из центральных моделей является подход, который условно обозначается формулой «следовать за деньгами». Его сущность заключается в признании финансового потока главным ориентиром для выявления организаторов, выгодоприобретателей и механизмов легализации преступных доходов. При использовании данной модели исходной точкой служат не только факты хищения, контрабанды, торговли людьми или незаконного оборота запрещённых предметов, но и любые аномальные имущественные процессы: несоразмерный образ жизни, расчёты через цепочки номинальных лиц, необъяснимое накопление активов, переводы в государства с недостаточной прозрачностью, резкое дробление поступлений, нехарактерные сделки между зависимыми структурами, конвертация средств в труднопрослеживаемое имущество. Последовательное движение по этому следу позволяет выйти на центры распределения доходов, на лиц, принимающих ключевые решения, и на инфраструктуру, обеспечивающую сохранение и воспроизводство преступного капитала. В ряде случаев именно финансовый анализ разрушает ту ложную картину, которую создают преступные сети, выдвигая

на передний план мелких исполнителей и тщательно скрывая тех, кто извлекает основную выгоду. **Деньги редко лгут; они движутся по логике власти, подчинения и интереса, а значит, указывают на подлинное строение преступной организации**.

Вторая модель - «следовать за администраторами» - ориентирована на выявление лиц, фактически осуществляющих управление сетью, поддерживающих её устойчивость, распределяющих роли, контролирующих коммуникацию и принимающих решения о перемещении людей, средств, товаров, документов и данных. Для транснациональной преступной среды характерно сознательное размывание фигуры руководителя: формальный организатор может отсутствовать, а функции управления распределяются между несколькими лицами, из которых одни отвечают за логистику, другие - за финансы, третьи - за безопасность, четвёртые - за набор новых участников, пятые - за техническую инфраструктуру. Тем не менее у любой устойчивой преступной сети существуют точки администрирования: субъекты, обладающие привилегированным доступом к каналам связи, к базам данных, к средствам распределения заданий, к системам подтверждения расчётов, к закрытым площадкам и к механизмам разрешения внутренних конфликтов. Их выявление позволяет нанести удар не по сменяемым исполнителям, а по координационному нерву всей структуры. Для этого требуется сопоставление цифровых, финансовых, миграционных, транспортных, телекоммуникационных и поведенческих данных, позволяющее установить, кто именно задаёт правила, кто подтверждает операции, кто санкционирует перемещения и кто принимает меры конспирации. **Обезглавить сеть - значит лишить её способности к самосохранению, даже если часть периферийных элементов ещё формально остаётся на свободе**.

Третья модель - «следовать за инфраструктурой» - исходит из понимания того, что преступная сеть существует не только как совокупность людей, но и как совокупность обеспечивающих её материальных и цифровых условий. Речь идёт о транспортных маршрутах, складах, перевалочных помещениях, фиктивных предприятиях, банковских и платёжных инструментах, вычислительных мощностях, серверах, доменных именах, анонимизирующих сервисах, поддельных документах, средствах связи, криптографических механизмах, логистических посредниках, коррупционных каналах, юридических оболочках и объектах имущества, используемых для сокрытия следов или легализации доходов. Пока эта инфраструктура функционирует, преступное сообщество способно восполнять кадровые потери и быстро восстанавливать оборот. Поэтому задача международной оперативной группы должна заключаться не только в задержании отдельных участников, но и в демонтаже тех опорных конструкций, которые делают преступление устойчивым и повторяемым. Это требует одновременного воздействия на все элементы инфраструктуры:

ареста имущества, изъятия серверов и средств связи, блокирования платёжных каналов, пресечения деятельности подставных предприятий, отзыва разрешений и регистраций, ограничения доступа к хранилищам и производственным площадкам, выявления коррумпированных посредников и нейтрализации технических администраторов. **Преступность побеждается не тогда, когда схвачен очередной исполнитель, а тогда, когда разрушена среда, в которой преступление может возродиться на следующий день**.

Четвёртая модель - «следовать за путями перемещения» - имеет особое значение в делах, связанных с торговлей людьми, незаконной миграцией, контрабандой, наркопреступностью, перемещением оружия, культурных ценностей, редких животных и растений, а также с иными формами преступной деятельности, основанной на пересечении границ. Здесь центральным объектом анализа становятся маршруты: география набора, транзита, размещения, переправки, складирования, промежуточных остановок, пересечения контрольных пунктов, смены транспортных средств и документов, использования приграничной инфраструктуры и логистических посредников. Исследование путей перемещения позволяет выявить не только фактическую траекторию движения людей или предметов, но и скрытую организационную структуру сети: кто обеспечивает переход границы, кто подготавливает документы, кто встречает груз или потерпевших, кто организует дальнейшее распределение, кто осуществляет охрану, кто берёт на себя принуждение, взыскание долгов, удержание и маскировку. Важнейшее значение здесь имеет сочетание данных пограничного контроля, транспортной аналитики, наблюдения, телефонных и сетевых соединений, финансовых транзакций, показаний потерпевших и свидетелей, результатов осмотра устройств и анализа навигационных данных. **Маршрут - это не просто линия на карте; это схема власти преступной сети, проявленная в пространстве**.

Однако ни одна из перечисленных моделей не должна применяться в отрыве от других. Подлинно эффективное международное расследование строится на их сочетании. Финансовый поток может вывести на администратора, администратор - на техническую инфраструктуру, инфраструктура - на маршруты перемещения, а маршруты - на новые финансовые узлы и ранее неизвестных посредников. Совместная международная оперативная группа именно потому и превосходит разрозненные формы сотрудничества, что позволяет удерживать в едином аналитическом поле всю систему взаимосвязей. **Современная преступная сеть многослойна, следовательно, и ответ государства должен быть многослойным, одновременным и непрерывным**.

Для обеспечения действенности таких групп необходимы чёткие организационные и правовые основы их функционирования. Прежде всего требуется заранее определённый порядок обмена информацией, включая

классификацию сведений по степени доступа, правила защиты персональных данных, условия использования разведывательной информации в уголовном процессе, механизмы подтверждения её происхождения и допустимые пределы последующей передачи третьим государствам. Не менее важно установить единые или взаимно признаваемые стандарты фиксации доказательств, особенно цифровых, чтобы исключить их последующее оспаривание. Следует заблаговременно решать вопросы подсудности, приоритетной юрисдикции, параллельного преследования, выдачи обвиняемых, передачи уголовного преследования и конфискации активов в трансграничном порядке. Без такой нормативной и процедурной предсказуемости даже хорошо оснащённая группа рискует столкнуться с тем, что оперативный материал не будет преобразован в судебный результат. **Преступная сеть выигрывает всякий раз, когда государства медлят в согласовании формальностей; право не должно становиться укрытием для тех, кто систематически разрушает сам правопорядок**.

Необходимо также подчеркнуть значение синхронности действий. Транснациональная сеть быстро приспосабливается к локальным ударам: если задержания и обыски проводятся в одной стране без одновременных мер в других юрисдикциях, организаторы получают время на бегство, уничтожение данных, перевод активов, переоформление имущества, смену маршрутов и вербовку новых исполнителей. Поэтому совместные международные оперативные группы должны планировать решающую фазу вмешательства как единую операцию, в которой временные окна, перечень объектов, адресатов процессуальных действий, меры по замораживанию активов, изъятию носителей информации, блокированию цифровых сервисов и задержанию ключевых лиц согласуются заранее и исполняются одновременно. **В борьбе с транснациональной организованной преступностью опоздание измеряется не часами, а утраченной возможностью пресечь целую систему**.

Самостоятельного рассмотрения заслуживает и вопрос доверия между участниками совместной группы. Международное сотрудничество в уголовно-правовой сфере не может быть сведено к формальному обмену поручениями. Оно требует институционального доверия, основанного на предсказуемости, профессиональной добросовестности, соблюдении режима конфиденциальности, готовности делиться чувствительной информацией и принимать на себя обязательства по своевременному реагированию. Это доверие не возникает само по себе; оно формируется посредством регулярных совместных учений, подготовки кадров, выработки единых методических подходов, обмена аналитическими практиками, взаимного прикомандирования специалистов, создания защищённых каналов связи и постоянного оценивания качества проведённых операций. **Там, где государства действуют как**

соперничающие наблюдатели, преступная сеть остаётся хозяином положения; там, где они действуют как единый правовой организм, пространство безнаказанности стремительно сужается.

Наконец, принципиально важно, чтобы деятельность совместных международных оперативных групп не ограничивалась исключительно репрессивной функцией. Их работа должна порождать и стратегическое знание: выявлять типовые схемы сокрытия доходов, новые способы использования цифровых имущественных средств, уязвимости пограничного режима, коррупционные узлы, пробелы в регулировании, недостатки процедур идентификации личности и регистрации имущества, особенности вербовки и перемещения потерпевших, трансформацию логистических путей. Это знание необходимо преобразовывать в рекомендации для законодательных органов, органов финансового контроля, миграционных служб, пограничных и таможенных структур, судебной системы и подразделений, ответственных за международное сотрудничество. **Если операция завершилась только приговором, но не изменила саму среду, в которой преступность питается и укрывается, значит, государство выиграло бой, но ещё не переломило ход борьбы.**

Таким образом, совместные международные оперативные группы должны рассматриваться как один из ключевых инструментов современного противодействия транснациональной организованной преступности. Их ценность определяется не формальным объединением представителей разных ведомств, а способностью создать единый контур выявления, анализа, пресечения, доказывания и последующего разрушения преступной инфраструктуры. В их составе должны быть представлены правоохранительные органы нескольких государств, подразделения финансовой разведки, киберподразделения, специалисты по цифровым имущественным ценностям, цифровые криминалисты и прокуроры, обеспечивающие процессуальную состоятельность международного доказывания. Их работа должна строиться на сочетании моделей, ориентированных на финансовые потоки, администраторов сети, инфраструктуру и пути перемещения. Лишь при таком подходе возможно нанести удар не по случайному фрагменту, а по самому механизму транснационального преступного воспроизводства. **Организованная преступность глобальна по способу существования; следовательно, и противодействие ей должно быть столь же целостным, стремительным и непреклонным.**

5.3. Стандартизация международного обмена электронными доказательствами

Одной из наиболее острых и в то же время системных проблем современного уголовного судопроизводства в трансграничной среде остается несоразмерность между **скоростью исчезновения электронных следов** и

медлительностью международной правовой помощи. Это противоречие уже давно перестало быть частной процессуальной трудностью. Оно приобрело характер фундаментального вызова для правосудия как такового. Там, где сведения о соединениях, регистрационные сведения учетных записей, журналы действий пользователей, сведения о местоположении, данные о сетевом взаимодействии и иные электронные доказательства могут быть изменены, утрачены, перезаписаны или уничтожены в течение нескольких часов либо даже минут, исполнение международного запроса на протяжении недель и месяцев фактически означает не просто задержку, а **потерю доказательства как юридической реальности**.

В этих условиях вопрос стандартизации международного обмена электронными доказательствами следует рассматривать не как сугубо техническую или ведомственную задачу, а как **необходимое условие сохранения способности государства к защите законности**. Если преступная деятельность осуществляется в среде мгновенного перемещения данных через множество юрисдикций, а государственные механизмы продолжают действовать в ритме бумажной эпохи, правоприменение начинает проигрывать преступной среде не случайно, а структурно. Именно поэтому в рамках Интерпола, региональных межгосударственных объединений, договорных режимов взаимной правовой помощи, а также специализированных площадок межведомственного взаимодействия должно последовательно продвигаться создание единых, заранее согласованных и обязательных к применению правил обращения с электронными доказательствами.

Прежде всего необходимы **ускоренные процедуры сохранения данных**, то есть такие правовые и организационные механизмы, которые позволяли бы незамедлительно направлять уполномоченному иностранному субъекту требование о временном обеспечении неизменности определенного массива сведений до поступления полного запроса о выдаче или раскрытии. Речь идет не о немедленной передаче содержания данных без соблюдения национальных гарантий и судебного контроля, а о минимально необходимой мере, направленной на предотвращение их утраты. В современной цифровой среде именно стадия сохранения имеет решающее значение. Если сведения не были своевременно зафиксированы, дальнейшие процессуальные усилия зачастую теряют смысл. Поэтому международные рекомендации должны закреплять единый перечень оснований для неотложного сохранения, круг уполномоченных органов, допустимые сроки первоначального резервирования, правила продления такого режима, порядок удостоверения момента получения требования и обязанность адресата подтвердить факт принятия мер по обеспечению неизменности данных. Без подобной унификации каждое обращение будет наталкиваться на несовпадение процессуальных форм, ведомственных

инструкций и национальных представлений о допустимом объеме срочности.

Не менее важным является введение **единых форматов описания цифровых объектов**, подлежащих сохранению, исследованию и передаче. Одной из причин отказов, задержек и ошибочного исполнения международных запросов выступает различие в том, как государства описывают один и тот же объект: учетную запись пользователя, сетевой узел, устройство связи, облачное хранилище, журнал событий, запись видеонаблюдения, переписку, файл, образ носителя, сведения о соединениях или сведения о регистрации в службе связи. Там, где нет единообразия в терминологии, неизбежно возникает двусмысленность; там, где есть двусмысленность, неизбежно страдает доказательственное значение полученного материала. Следовательно, международная стандартизация должна включать разработку унифицированных словарей понятий, обязательных реквизитов описания объекта, правил указания временных параметров, привязки к часовым поясам, способов обозначения идентификаторов устройств и учетных записей, а также единых принципов фиксации связей между цифровым объектом, его носителем, источником извлечения и конкретным процессуальным действием. Такая мера не сводится к улучшению делопроизводства. Она устраняет правовую неопределенность, от которой зависит допустимость и достоверность доказательств в суде.

Особое значение имеет разработка **стандартных шаблонов срочных запросов**, поскольку именно на стадии первичного обращения чаще всего утрачивается драгоценное время. В настоящее время срочные обращения нередко составляются в произвольной форме, содержат неполные сведения, не отражают процессуального основания, не позволяют быстро определить характер преступления, объем требуемых мер и пределы допустимого вмешательства в права лица. В результате иностранный адресат вынужден тратить время на уточнения, повторные запросы и ведомственные согласования. Между тем в делах о терроризме, организованной преступности, торговле людьми, незаконном обороте наркотических средств, посягательствах на половую неприкосновенность несовершеннолетних, преступлениях против критически важной информационной инфраструктуры, тяжких насильственных преступлениях и иных деяниях, сопряженных с высокой скоростью сокрытия следов, промедление означает фактическое содействие безнаказанности. Стандартизированный срочный запрос должен содержать сведения об инициирующем органе, правовом основании обращения, квалификации деяния, указании на степень неотложности, точном перечне данных, подлежащих сохранению или выдаче, обосновании связи этих данных с расследуемым событием, указании на риск их скорой утраты, а также сведениях о допустимых способах обратной связи для немедленного подтверждения исполнения. Такие шаблоны должны быть заранее

переведены на рабочие языки соответствующих организаций и сопровождаться едиными правилами заполнения, исключающими смысловые расхождения.

Ключевым элементом международной доказательственной совместимости является **унификация требований к метаданным**. Электронное доказательство ценно не только своим содержанием, но и сведениями о своем происхождении, структуре, времени создания, изменении, передаче, способе извлечения и условиях хранения. Именно эти сведения позволяют установить подлинность объекта, выявить вмешательство, проследить путь движения доказательства и оценить его пригодность для судебного разбирательства. Однако на практике государства по-разному относятся к набору обязательных сопроводительных сведений: где-то достаточно общего указания на источник, а где-то требуется детальное описание носителя, версии программного обеспечения, времени извлечения, способа копирования, примененных средств контроля целостности и всех лиц, имевших доступ к объекту. В отсутствие единых требований доказательство, добытое с соблюдением стандартов одной страны, может оказаться спорным или даже непригодным в другой. Следовательно, необходимо международное согласование минимально обязательного состава метаданных для различных видов электронных доказательств. Такой состав должен включать идентификатор объекта, источник его получения, временные отметки всех значимых действий, сведения о лице и органе, осуществивших извлечение, характеристику исходного носителя или удаленного хранилища, сведения о примененных методах копирования и фиксации, данные о контроле неизменности, а также непрерывно документируемую цепь законного владения доказательством. Без этого международный обмен будет производить не процессуально устойчивые доказательства, а лишь сведения, чья юридическая ценность легко подвергается сомнению.

Важнейшим направлением выступает и **взаимное признание определенных технических форм верификации**, поскольку именно на этой стадии сталкиваются различные национальные подходы к удостоверению подлинности и неизменности электронных данных. В одних правопорядках ключевое значение придается контрольным значениям, в других - процедуре судебного удостоверения, в третьих - участию уполномоченного эксперта, в четвертых - ведомственным стандартам цифрового копирования. Если международная передача электронных доказательств не будет опираться на хотя бы минимально согласованный круг взаимно признаваемых способов подтверждения целостности и происхождения данных, каждое трансграничное дело будет начинаться с сомнения в самой доказательственной основе. Здесь необходим особенно взвешенный подход. Речь не должна идти о полном устранении национальной процессуальной самостоятельности. Напротив, требуется выработать перечень таких

технических форм удостоверения, которые признаются достаточными prima facie для подтверждения того, что объект не подвергался несанкционированному изменению после его извлечения или фиксации. Международные рекомендации могли бы предусматривать согласованные правила формирования контрольных значений, протоколирования операций копирования, удостоверения времени фиксации, составления акта извлечения, документирования используемых средств и ведения непрерывной цепи обращения с доказательством. Такое взаимное признание не отменяет права суда оценивать доказательство, по существу, но устраняет разрушительную ситуацию, при которой трансграничный обмен останавливается на пороге недоверия к базовым техническим процедурам.

Особого внимания требует формирование **процедур экстренного замораживания и сохранения данных по тяжким преступлениям**, то есть такого режима, при котором уполномоченный орган одного государства мог бы в строго ограниченных случаях оперативно инициировать срочное резервирование определенных электронных сведений, находящихся во владении иностранного поставщика услуг, иного держателя данных или компетентного органа другой страны. Здесь следует ясно подчеркнуть: подобный механизм не должен превращаться в средство обхода судебных гарантий, расширительного наблюдения или произвольного вмешательства в частную жизнь. Его назначение строго функционально - **сохранить доказательство до того момента, пока не будет выполнена надлежащая правовая процедура его истребования и передачи**. Но именно это назначение требует предельной оперативности. Когда речь идет о преступлениях, связанных с реальной угрозой жизни, безопасности личности, национальной безопасности, защитой детей, предотвращением террористического акта, раскрытием сети организованной преступности или пресечением массового вредоносного воздействия на жизненно важные системы, государство не вправе оправдывать бездействие сложностью межгосударственной переписки. Международные акты рекомендательного и договорного характера должны закрепить перечень категорий дел, при которых допустима экстренная мера, пределы объема сохраняемых данных, сроки действия режима замораживания, порядок последующего судебного или прокурорского контроля, основания прекращения меры, а также гарантии уведомления и правовой защиты затронутых лиц в тех пределах, в каких такое уведомление совместимо с целями расследования.

Следует подчеркнуть, что стандартизация международного обмена электронными доказательствами не может ограничиваться изданием абстрактных рекомендаций. **Правовая форма без организационного наполнения бесплодна**. Для реального действия таких механизмов необходимы постоянно действующие контактные пункты, доступные в круглосуточном режиме; единые защищенные каналы межгосударственной

передачи запросов и подтверждений; заранее определенные перечни компетентных органов; согласованные сроки первичного реагирования; типовые руководства по квалификации срочности; а также регулярная межгосударственная подготовка следователей, прокуроров, судей, экспертов и сотрудников подразделений международного сотрудничества. Иначе даже самый совершенный нормативный документ будет разбиваться о практику ведомственной несогласованности, языковых ошибок, неточного определения адресата и элементарной неосведомленности исполнителей о существующих возможностях.

Не менее существенно и то, что международная стандартизация должна строиться на **балансе эффективности и гарантий прав человека**. Электронное доказательство почти всегда находится в непосредственной связи с частной жизнью, тайной связи, свободой выражения мнения, защитой персональных данных, неприкосновенностью профессиональной тайны и иными конституционно значимыми благами. Поэтому ускорение процедур недопустимо понимать как отказ от законности. Напротив, именно стандартизация способна стать инструментом повышения правовой определенности и защиты личности. Когда основания, пределы, сроки, формы запроса, требования к содержанию, правила хранения и допустимые способы использования данных четко определены заранее и единообразно, пространство для произвола сужается, а возможности последующего судебного контроля возрастают. Иными словами, хорошо выстроенный международный порядок обращения с электронными доказательствами одновременно служит и интересам уголовного преследования, и интересам правовой защиты человека.

С научной и практической точек зрения представляется оправданным закрепление многоуровневой модели стандартизации. На первом уровне должны быть согласованы базовые понятия, общие принципы срочности, требования к целостности данных и минимальный состав метаданных. На втором уровне - разработаны типовые формы запросов, единые перечни реквизитов и классификаторы цифровых объектов. На третьем уровне - создан порядок взаимного признания отдельных процедур технического удостоверения и сохранения сведений. Наконец, на четвертом уровне - обеспечен контроль исполнения: статистическое наблюдение за сроками реагирования, выявление типичных причин отказов, анализ судебной оценки полученных доказательств, периодический пересмотр стандартов с учетом развития технологий и трансформации преступных практик. Без такого многоуровневого устройства международная стандартизация рискует остаться набором добрых пожеланий, не меняющих повседневную реальность следствия и суда.

Нельзя не сказать и о том, что отсутствие единых международных правил особенно выгодно тем субъектам, которые сознательно выстраивают преступную деятельность на разрывах между юрисдикциями.

Организованные преступные группы, террористические сети, лица, распространяющие материалы сексуальной эксплуатации детей, мошеннические объединения, структуры, осуществляющие вымогательство с использованием вредоносных программ, давно научились использовать не только анонимизацию и техническую маскировку, но и **правовую фрагментарность мирового пространства**. Они знают: там, где государство должно оформлять бумажный запрос неделями, где перевод занимает больше времени, чем существование журналов соединения, где один орган не признает техническую фиксацию другого, там возникает убежище для безнаказанности. Следовательно, стандартизация международного обмена электронными доказательствами - это не вопрос бюрократического удобства, а вопрос устранения тех лазеек, которые сама правовая разобщенность открывает перед преступностью.

В этой связи рекомендации в рамках Интерпола и иных международных организаций должны носить не декларативный, а предметный характер. Они должны предусматривать модельные правила немедленного сохранения данных, унифицированные описания цифровых объектов, обязательные формы срочных обращений, единые требования к метаданным, минимальные стандарты удостоверения целостности, процедуры экстренного замораживания сведений по тяжким преступлениям, а также порядок последующей передачи, исследования и судебной верификации полученного материала. Необходимы и механизмы оценки исполнения таких рекомендаций: сопоставление сроков реагирования государств, анализ причин неисполнения, подготовка обобщенных докладов, формирование перечней лучших практик и создание площадок для согласования спорных вопросов. Международное сотрудничество должно перестать быть пространством вежливых формул и стать пространством измеримой эффективности.

Итоговый вывод здесь предельно ясен. **Если данные исчезают за часы, а международный запрос исполняется месяцами, правосудие терпит поражение еще до начала судебного разбирательства**. В цифровую эпоху сохранение доказательства означает сохранение самой возможности установить истину. Поэтому стандартизация международного обмена электронными доказательствами должна быть признана одной из центральных задач современной уголовной политики, международного процессуального сотрудничества и правовой науки. От того, будет ли создан единый, быстрый, юридически выверенный и технически надежный порядок обращения с такими доказательствами, зависит не только эффективность расследования отдельных дел, но и способность государства в целом удерживать верховенство права перед лицом преступности, действующей со скоростью электронного сигнала.

5.4. Взаимодействие с Интерполом, Европолом, Управлением Организации Объединённых Наций по наркотикам и преступности и региональными структурами

В современных условиях борьба с трансграничной преступностью более не может строиться по лекалам прошлого, когда преступное деяние, его подготовка, совершение, сокрытие следов и извлечение дохода укладывались в пределы одной территории, одной правовой системы и одного набора доказательств. Цифровая среда разрушила эти границы. Сегодня преступная сеть может вербовать исполнителей в одном государстве, размещать управляющую инфраструктуру в другом, использовать средства сокрытия в третьем, выводить преступные доходы через цепочки распределённых расчётов в четвёртом, а поражать потерпевших одновременно на нескольких континентах. В этих условиях **международное сотрудничество должно пониматься не как дипломатическое приложение к национальному расследованию, а как его неотъемлемая, исходная и постоянно действующая основа**.

Наряду с каналами Интерпола, особое значение приобретает системное задействование возможностей Управления Организации Объединённых Наций по наркотикам и преступности, Европола, механизмов, совместимых с требованиями Группы разработки финансовых мер борьбы с отмыванием денег, региональных антитеррористических и антикриминальных центров, а также сетей национальных служб реагирования на компьютерные происшествия при пересечении общеуголовных и цифровых угроз. Речь должна идти не о механическом расширении перечня международных партнёров, а о формировании **единой оперативно-аналитической среды**, в которой сведения, методики, признаки преступной деятельности, следственные ориентировки и правовые решения соотносятся между собой в режиме, соответствующем скорости самой преступности.

Управление Организации Объединённых Наций по наркотикам и преступности обладает исключительным потенциалом в части выработки международных подходов к противодействию цифровой организованной преступности. Его значение заключается не только в экспертном сопровождении государств, нуждающихся в совершенствовании законодательства, но и в способности соединять уголовно-правовую, криминологическую, процессуальную и институциональную повестку. Именно на этой площадке возможно продвигать унифицированные определения новых форм преступной деятельности, общие критерии отнесения деяний к транснациональной организованной цифровой преступности, типовые модели закрепления полномочий следственных органов, а также согласованные подходы к собиранию, закреплению, исследованию и международной передаче цифровых доказательств. Без такой теоретико-нормативной опоры борьба с преступностью неизбежно будет разъедаться правовой неоднородностью: одно и то же деяние в одной

юрисдикции будет рассматриваться как тяжкое преступление, в другой - как административное правонарушение, а в третьей - вовсе не получит должной квалификации. **Там, где нет единства понятий, не может быть устойчивого единства действий**.

Особое место в европейском пространстве занимает Европол как структура, способная обеспечивать углублённую уголовно-аналитическую обработку массивов данных, координацию многосторонних расследований, сопоставление разрозненных эпизодов в единую преступную картину, а также сопровождение совместных мероприятий против сложных сетевых объединений. Его значение особенно велико в тех делах, где преступная деятельность носит серийный, распределённый, конспиративный характер и сопровождается активным использованием зашифрованных средств общения, анонимизирующей инфраструктуры, подставных учётных записей, многоступенчатых расчётных цепочек и удалённого управления преступными действиями. В подобных обстоятельствах одно государство почти никогда не видит преступление целиком: оно видит лишь фрагмент. Лишь наднациональная аналитическая сборка позволяет установить связи между, казалось бы, несопоставимыми фактами: совпадение цифровых отпечатков, повторяемость преступных приёмов, общность управляющих узлов, миграцию одних и тех же участников между различными преступными схемами, синхронность атак и последующего вывода средств. Поэтому **аналитическое взаимодействие с Европолом должно быть не эпизодическим, а встроенным в повседневную практику выявления, документирования и пресечения преступлений**.

Не меньшую значимость имеют механизмы, совместимые с требованиями международных стандартов в сфере противодействия отмыванию преступных доходов. В условиях цифровизации незаконный доход всё чаще принимает форму, затрудняющую его немедленное распознавание: распределённые расчётные единицы, платёжные суррогаты, расчёты через игровые и торговые площадки, многоступенчатые переводы через номинальных посредников, дробление сумм, использование трансграничных расчётных коридоров и фиктивных хозяйственных операций. Если финансовая составляющая преступления остаётся вне поля международного контроля, борьба с ним превращается в борьбу с последствиями, а не с причиной. Преступная сеть может потерять исполнителей, отдельные серверные мощности или каналы распространения, но пока сохраняется механизм извлечения, перемещения и легализации дохода, она воспроизводит себя снова. Поэтому взаимодействие с органами и площадками, реализующими подходы к финансовой прозрачности, должно быть направлено не только на выявление подозрительных операций, но и на выработку общих критериев цифрового финансового риска, типологий криминального использования новых расчётных средств, процедур замораживания активов,

согласованных моделей раскрытия конечных выгодоприобретателей и механизмов оперативного межгосударственного обмена сведениями о движении преступного капитала. **Удар по преступной инфраструктуре без удара по преступным доходам всегда остаётся неполным**.

Региональные антитеррористические и антикриминальные центры следует рассматривать как важнейшее звено в тех случаях, когда цифровая преступность переплетается с насильственным экстремизмом, незаконным оборотом оружия, торговлей людьми, контрабандой, наркотрафиком, финансированием террористической деятельности и дестабилизацией общественного порядка. Цифровая среда всё чаще выступает не отдельной сферой преступления, а связующим слоем между различными видами противоправной активности. Через неё координируются поставки, обеспечивается рекрутирование, осуществляется легализация доходов, распространяются инструкции, ведётся разведка уязвимостей, подбираются цели, организуется скрытое перемещение средств и формируется ложная информационная оболочка. В силу этого региональные структуры должны не только аккумулировать сведения о традиционных угрозах, но и обладать устойчивыми возможностями цифрового анализа: сопоставлением сетевых связей, отслеживанием каналов связи, изучением особенностей незаконных площадок, выявлением признаков подготовки распределённых преступных акций. Их ценность состоит в близости к конкретной криминальной среде, знании языковых, этнокультурных, экономических и географических особенностей региона, без чего многие трансграничные преступные связи остаются нераспознанными. **Глобальная координация без региональной глубины неизбежно слепнет; региональная осведомлённость без международной стыковки столь же неизбежно дробится**.

Сети национальных служб реагирования на компьютерные происшествия должны подключаться к антикриминальному взаимодействию всякий раз, когда техническое происшествие оказывается не просто нарушением работоспособности информационной системы, а элементом уголовно наказуемой деятельности. На практике разграничение между техническим и криминальным измерением угрозы часто является искусственным. Массовое вредоносное воздействие на сети может служить прикрытием вымогательства; компрометация учётных записей - подготовкой хищения; распространение вредоносных программ - инструментом шантажа, саботажа или незаконного сбора сведений; блокирование ресурсов - способом давления на потерпевших или устранения конкурентов в теневом секторе. Если службы реагирования действуют изолированно от правоохранительных органов, теряется критически важное время, а вместе с ним - и следовая информация: журналы событий очищаются, временные данные исчезают, скомпрометированные узлы переустанавливаются, а злоумышленники успевают свернуть инфраструктуру. Следовательно, требуется такая модель взаимодействия, при которой при наличии

признаков преступления техническое реагирование и уголовно-процессуальное документирование запускаются параллельно, а не последовательно. **В цифровой среде промедление есть не просто организационный недостаток, а прямой путь к безвозвратной утрате доказательств**.

Исходя из этого, особого развития требуют совместные оценки угроз. Такие документы не должны быть общими декларациями о росте опасности, не несущими прикладной ценности. Они обязаны строиться на верифицируемых данных, учитывать отраслевую и региональную специфику, выделять устойчивые преступные модели, описывать так называемый жизненный цикл преступной схемы - от подготовки до извлечения дохода и сокрытия следов, - а также включать признаки раннего выявления и перечни наиболее уязвимых точек вмешательства. Совместная оценка угроз ценна именно тем, что превращает разрозненные наблюдения разных государств в общую картину развития преступной среды. Она позволяет заранее увидеть смещение преступной активности из одной сферы в другую, понять, какие инструменты набирают популярность, какие уязвимости эксплуатируются повторно, какие посреднические узлы используют преступники и как меняются способы маскировки.

Необходимо также формировать общие массивы сведений о типичных способах подготовки, совершения и сокрытия преступлений. Такие сведения должны включать описание преступных приёмов, повторяющихся последовательностей действий, цифровых и поведенческих признаков, используемых средств анонимизации, моделей вербовки исполнителей, способов обналичивания, методик удаления следов, приёмов давления на потерпевших и характерных ошибок злоумышленников, позволяющих их раскрывать. Подобные массивы данных особенно важны для выявления серийности, атрибуции преступных групп и подготовки ориентировок для следственных, оперативных и экспертных подразделений. **Преступник может менять названия учётных записей, узлы связи и расчётные средства, но он редко мгновенно меняет всю совокупность своих устойчивых поведенческих признаков**.

Международные перечни цифровых индикаторов также должны стать обязательным элементом такого сотрудничества. Речь идёт не только о сетевых адресах, доменных именах, контрольных суммах вредоносных файлов или признаках вредоносной активности, но и о более сложных индикаторах: характере взаимодействия узлов, временных закономерностях операций, повторяющихся шаблонах регистрационных данных, следах автоматизации, особенностях языкового оформления сообщений, структуре расчётных маршрутов, параметрах используемого программного обеспечения и признаках связности между различными преступными платформами. Правильно организованный международный обмен такими индикаторами позволяет не просто реагировать на уже

состоявшееся преступление, а предупреждать новые эпизоды и быстро устанавливать, что кажущиеся самостоятельными события являются частями одной организованной деятельности.

Крайне востребован и обмен практическими методиками изъятия, фиксации и анализа данных, находящихся в распоряжении цифровых площадок. Здесь особенно велика опасность разнородности: одно государство умеет эффективно обеспечивать срочное сохранение данных, но сталкивается с трудностями их последующего получения; другое располагает сильной судебной практикой, но недостаточно быстро реагирует на краткоживущие цифровые следы; третье имеет развитые экспертные возможности, но не выстроило механизмов межведомственного взаимодействия. Между тем платформенные данные сегодня во многих делах приобретают решающее значение: они позволяют установить цепочку управления учётными записями, подтвердить синхронность действий участников, выявить скрытых администраторов, восстановить удалённые эпизоды общения, проследить перемещение средств, сопоставить преступные кампании между собой. Поэтому международный обмен должен охватывать не отвлечённые рассуждения, а конкретные, проверенные практикой модели действий: как формулировать запросы, какие данные просить в первую очередь, как обосновывать срочность, каким образом сохранять доказательственную целостность полученных сведений, как описывать их происхождение и как представлять их в суде.

Наконец, важнейшим направлением остаются совместные образовательные программы. Их задача состоит не в формальном проведении мероприятий ради отчётности, а в выработке общего профессионального языка между следователями, оперативными сотрудниками, прокурорами, судьями, специалистами по компьютерной криминалистике, работниками служб реагирования, подразделений финансовой разведки и международных координационных структур. В условиях, когда преступление развивается на стыке права, техники, финансов и межгосударственного взаимодействия, узкая ведомственная подготовка оказывается недостаточной. Необходимы такие учебные курсы, которые объединяют правовые основания, технические навыки, вопросы допустимости доказательств, особенности международной правовой помощи, методы финансового прослеживания и приёмы оперативного анализа. Только при этом условии международное сотрудничество перестанет быть обменом бумаг и превратится в **согласованное действие профессиональных сообществ, объединённых общей задачей, единым пониманием угрозы и одинаково высоким стандартом доказательственной работы**.

Таким образом, международные организации и специализированные сети должны использоваться не для внешнего соблюдения требований международной вежливости, а как действующий механизм построения общей оперативно-аналитической среды. Это означает постоянную

циркуляцию данных, сопоставимость методик, согласованность квалификаций, совместимость технических процедур, скорость экстренного реагирования и доверие, основанное на профессиональной предсказуемости. **Либо государства создадут такую среду, либо преступные сети и далее будут пользоваться преимуществами глобальной связности в большей степени, чем закон и правопорядок**.

5.5. Продвижение международных стандартов ответственности цифровых площадок

Одним из наиболее острых и в то же время принципиально неизбежных вопросов современной уголовной политики является определение объёма обязанностей цифровых площадок по содействию законному расследованию тяжких преступлений. Этот вопрос не может решаться ни в логике полного устранения государства из цифровой среды, ни в логике передачи частным владельцам информационных систем функций правоохранительных органов. Обе крайности одинаково опасны. Первая превращает площадки в зоны фактической недосягаемости права; вторая подрывает основы законности, подменяя публичную власть частным усмотрением. Следовательно, международному сообществу необходимо настойчиво добиваться такого баланса, при котором **цифровые площадки не становятся карательным субъектом, но и не сохраняют иммунитет от обязанностей по разумному, законному и своевременному содействию правосудию**.

Прежде всего требуется выработка минимальных международных стандартов реагирования площадок на законные запросы компетентных органов. Сегодня одной из ключевых проблем является крайняя фрагментарность существующей практики. Одни владельцы цифровых систем отвечают быстро, но неполно; другие требуют избыточно формализованных процедур, несовместимых со срочностью расследования; третьи, по существу, создают видимость взаимодействия, затягивая сроки или ссылаясь на внутренние правила, не имеющие приоритета перед надлежащим правовым требованием; четвёртые применяют настолько неодинаковые подходы к сходным запросам, что это разрушает саму идею равенства правоприменения. Между тем для расследования тяжких преступлений значение имеют не абстрактные ответы, а временные пределы, полнота предоставляемых сведений, ясность критериев допустимости запроса, наличие понятного канала срочной связи и возможность проверить, какие действия площадка предприняла для сохранения или выдачи данных. Международный стандарт в этой части должен устанавливать минимально необходимый набор обязанностей: регистрацию запроса, подтверждение его получения, оценку срочности, сохранение релевантных данных до разрешения вопроса по существу, мотивированный ответ в разумный срок, наличие круглосуточного канала связи по неотложным случаям и документирование всех этапов

взаимодействия. **Правовой порядок начинается там, где вместо произвольного усмотрения возникает предсказуемая и проверяемая процедура**.

Особое значение имеет международная регламентация сроков сохранения данных, имеющих значение для расследования тяжких преступлений. В цифровой среде следы часто носят кратковременный характер. Сведения о соединениях, данных сеанса, метаданных сообщений, адресной информации, привязке устройств, технических журналах, внутренних идентификаторах, истории управления учётной записью и иных цифровых параметрах могут исчезнуть задолго до того, как правоохранительный орган завершит межгосударственные формальности. Преступники прекрасно знают эту уязвимость и сознательно используют платформы, где скорость естественного исчезновения следов высока, а процедура их сохранения затруднена. Вследствие этого международные стандарты должны исходить из простой, но решающей мысли: по делам о тяжких преступлениях время хранения релевантных данных не может определяться исключительно коммерческими интересами владельца площадки или его внутренней политикой минимизации издержек. Необходимы согласованные минимальные сроки сохранения определённых категорий данных, дифференцированные по степени общественной опасности деяния, характеру расследуемого события и доказательственной значимости сведений. При этом такие сроки должны сочетаться с гарантиями законности, целевой определённости и недопустимости произвольного расширения хранения вне рамок правомерной цели. **След, который право не успело сохранить, слишком часто становится следом, который уже невозможно восстановить**.

К числу первоочередных задач относится и создание международно согласованных процедур срочного предотвращения уничтожения цифровых следов. Речь идёт о так называемом неотложном сохранении данных в ситуациях, когда имеется обоснованное предположение, что их утрата может наступить в течение часов или даже минут. Такой механизм должен действовать до завершения сложных процедур межгосударственного получения информации, выступая не заменой судебного или иного законного разрешения, а его временным обеспечительным дополнением. В противном случае международная правовая помощь постоянно будет опаздывать к уже исчезнувшему предмету доказывания. Однако и здесь критически важно соблюсти правовой баланс. Процедура срочного сохранения должна иметь чёткие основания применения, ограниченный предмет, фиксированные сроки действия, обязательность последующего подтверждения компетентным органом и возможность последующей проверки законности её использования. Иначе экстренный механизм рискует превратиться в средство необоснованного вмешательства. Но при надлежащей

регламентации он становится тем инструментом, который спасает доказательства в первые часы после выявления преступной активности, когда промедление особенно губительно.

Не менее важны обязательства цифровых площадок по прозрачности взаимодействия с компетентными органами. Прозрачность здесь должна пониматься в двух измерениях. Первое - внешнее, общественное: публикация обобщённых сведений о количестве запросов, категориях правовых оснований, доле удовлетворённых требований, средних сроках ответа, применяемых критериях локализации данных и общих принципах внутреннего рассмотрения обращений. Второе - процедурное, адресованное непосредственно государственным органам: ясное описание форматов запросов, перечней доступных категорий данных, правил подтверждения полномочий, каналов срочной связи, условий сохранения данных и оснований отказа. Непрозрачность выгодна лишь тем, кто стремится уклониться от ответственности, затруднить надзор и представить произвольное поведение как проявление корпоративной автономии. Напротив, прозрачность создаёт условия для сопоставимости практики, выявления злоупотреблений, защиты прав пользователей и повышения доверия к законным формам взаимодействия. **Там, где нет прозрачности, неизбежно возникает зона институциональной тени, в которой одинаково страдают и интересы расследования, и гарантии правомерности**.

Международное значение приобретают и протоколы уведомления о выявлении масштабных криминальных сетей, действующих через цифровые площадки. На практике нередки ситуации, когда владелец площадки раньше государства видит аномальную активность, массовое создание взаимосвязанных учётных записей, координированное использование автоматизированных средств, признаки торговли запрещёнными предметами, систематическое вовлечение несовершеннолетних, сеть вымогательства, финансовое мошенничество либо иной крупный преступный контур. Если при этом отсутствует международно признанная процедура уведомления компетентных органов, ценнейшее время упускается, а преступная сеть успевает изменить конфигурацию, удалить сведения и мигрировать на иные площадки. Необходимо выработать такой порядок, при котором при выявлении признаков крупномасштабной и социально опасной преступной деятельности площадка обязана в установленной форме уведомить уполномоченные органы соответствующей юрисдикции либо специально определённый координационный центр. Разумеется, подобное уведомление не должно превращаться в обобщённую обязанность тотального доноса или произвольного сообщения о любой необычной активности. Оно должно быть ограничено тяжкими формами преступности, основано на заранее установленных критериях существенности и сопровождаться последующей правовой оценкой компетентного органа. Но

игнорирование этого направления означало бы добровольный отказ от одного из немногих ранних сигналов, позволяющих пресекать преступную деятельность до того, как она приобретёт необратимый масштаб.

При разработке международных стандартов необходимо особо подчеркнуть, что цифровые площадки не должны подменять собой правоохранительные органы. Они не вправе самостоятельно определять виновность, выносить квазисудебные решения по уголовно значимым обстоятельствам или по своему усмотрению формировать репрессивную практику, выходящую за пределы закона. Их функция иная: обеспечивать сохранность необходимых данных, исполнять законные и надлежащим образом оформленные требования, своевременно информировать о выявленных признаках особо опасной деятельности, поддерживать понятные и проверяемые процедуры взаимодействия и не создавать искусственных препятствий расследованию. Эта позиция принципиальна. **Содействие правосудию не тождественно присвоению его полномочий**. Но столь же принципиально и обратное: владение критически важными доказательствами и управление средой, в которой совершаются тяжкие преступления, не может служить основанием для ухода от ответственности под предлогом технологической нейтральности.

В международной плоскости продвигать такие стандарты следует последовательно и настойчиво, сочетая уголовно-правовые, процессуальные, договорные и организационные меры. Важно добиваться не только принятия общих деклараций, но и включения конкретных обязанностей в многосторонние соглашения, типовые рекомендации, межведомственные протоколы, практические руководства и стандартизированные формы взаимодействия. Необходимо также обеспечивать совместимость этих стандартов с гарантиями прав человека, защитой тайны частной жизни, судебным контролем и принципом соразмерности вмешательства. Лишь тогда международная модель ответственности площадок будет одновременно эффективной и правомерной. Если же ограничиться одними призывами к добровольному сотрудничеству, без чётких правил, сроков и механизмов проверки, то преступные сети и далее будут извлекать выгоду из правовой размытости, коммерческой осторожности площадок и межгосударственных расхождений.

В конечном счёте вопрос об ответственности цифровых площадок - это вопрос о способности права не капитулировать перед новой архитектурой преступности. Государство не может позволить, чтобы пространство, в котором совершаются вербовка, координация, расчёты, сокрытие следов и распространение преступных услуг, оказалось выведенным из сферы разумных обязанностей по содействию законному расследованию. Но и вмешательство в эту сферу должно быть строго подчинено закону, судебным гарантиям и международно признанным процедурам. Следовательно,

подлинная задача международного сообщества состоит в том, чтобы построить **ясный, обязательный и справедливый режим взаимодействия**, при котором тяжкие преступления не растворяются в цифровой безответственности, а закон получает необходимые средства для их своевременного пресечения и доказывания. Именно в этом и заключается подлинный смысл международных стандартов: не в умножении формальностей, а в восстановлении действенности права там, где преступность попыталась поставить себя выше границ, сроков и национальных юрисдикций.

6. ПРОФИЛАКТИКА И ИНФОРМАЦИОННО-ПРАВОВОЕ ВОЗДЕЙСТВИЕ

6.1. Профилактика спроса на криминальные услуги

Профилактика спроса на криминальные услуги в цифровой среде должна рассматриваться не как вспомогательное направление государственной политики, а как **одно из центральных условий подрыва экономической, социальной и организационной основы преступной деятельности**. До тех пор, пока сохраняется массовый, скрытый или полуоткрытый общественный запрос на незаконные цифровые услуги, любые, даже самые технологически совершенные меры пресечения будут носить в значительной степени реактивный характер. Преступность в данной сфере питается не только профессиональными организаторами, техническими исполнителями и финансовыми посредниками, но и широким кругом потребителей, которые нередко стремятся представить собственное участие в противоправных схемах как нечто малозначительное, бытовое, почти нейтральное. Именно в этом состоит одна из наиболее опасных нравственно-правовых деформаций современности: **преступление начинает маскироваться под услугу, а соучастие - под удобство**.

В этой связи профилактика спроса требует не фрагментарных, эпизодических разъяснений, а системной, научно обоснованной и постоянно воспроизводимой деятельности государства, образовательных учреждений, средств массовой информации, правоохранительных органов, институтов гражданского общества и профессиональных объединений. Ее предметом является не только формальное информирование населения о запретах, но и **последовательное преобразование общественных представлений о допустимом, выгодном, безопасном и морально безразличном поведении**. Речь идет о глубинном воздействии на правосознание, ценностные установки и повседневные модели выбора. Там, где человек перестает видеть в незаконной цифровой услуге преступление, государство обязано вернуть правовую ясность, нравственную определенность и социальную ответственность.

Прежде всего необходимо добиваться **снижения терпимости к криминальному цифровому содержанию и к сопутствующим практикам его**

потребления. Особая сложность данной задачи обусловлена тем, что противоправный материал в цифровой среде часто подается в форме, лишенной внешних признаков опасности: как развлечение, как “полезный совет”, как способ обойти ограничения, как средство ускорить получение желаемого результата, как часть якобы нормальной повседневной культуры. В результате формируется крайне опасная привычка к эмоциональному и нравственному безразличию. Незаконное распространение персональных сведений, инструкции по мошенническим действиям, предложения о приобретении вредоносных программных средств, сведения о способах сокрытия доходов, услуги по незаконному получению доступа к учетным записям, материал, оправдывающий травлю, вымогательство, незаконный оборот запрещенных веществ или иные преступления, начинают восприниматься значительной частью аудитории не как проявление общественной угрозы, а как разновидность допустимого информационного фона.

Подобная терпимость не возникает внезапно. Она формируется постепенно: через многократное повторение, через снижение эмоциональной чувствительности, через распространение циничной установки, согласно которой незаконным считается лишь то, за что последовало немедленное наказание. Поэтому государственная профилактика должна разрушать сам механизм привыкания к преступному содержанию. Здесь требуется не сухая декларация запретов, а **настойчивое и убедительное раскрытие того, что за каждым цифровым продуктом криминального характера стоят конкретные потерпевшие, конкретный ущерб, конкретное разрушение человеческих судеб, имущественных интересов, деловой репутации, общественной безопасности и доверия к правопорядку**. Необходимо возвращать обществу способность видеть за безличным интерфейсом живую реальность преступления. Если гражданин воспринимает незаконно полученную базу данных лишь как “удобный набор сведений”, значит, профилактическая работа оказалась недостаточной; ему должно быть ясно, что в действительности речь идет о вторжении в частную жизнь, об угрозе шантажу, мошенничеству, дискредитации личности и иным тяжким последствиям.

Не менее важным направлением является **разъяснение юридических последствий участия в теневых схемах**, причем в максимально конкретной, предметной и лишенной отвлеченности форме. Существенный изъян многих профилактических кампаний состоит в том, что они ограничиваются общими предупреждениями о “возможной ответственности”, не раскрывая ни правовой природы деяния, ни форм вины, ни различий между организатором, исполнителем, пособником, посредником и потребителем незаконной услуги. В итоге у значительной части граждан возникает ложное представление, будто риск уголовного или административного преследования касается исключительно “крупных

игроков", тогда как рядовой заказчик, получатель услуги, пользователь анонимного канала передачи данных, приобретатель похищенных сведений, распространитель незаконного материала или лицо, передающее свои реквизиты для проведения сомнительных операций, якобы остается в тени правовой оценки. Подобное представление необходимо последовательно опровергать.

Профилактическое информационно-правовое воздействие должно содержать ясное указание на то, что **участие в теневой цифровой схеме редко ограничивается одной-единственной ролью и почти всегда образует цепь взаимосвязанных правонарушений**. Гражданину необходимо разъяснять, что даже, на первый взгляд, "пассивное" приобретение незаконной услуги может влечь последствия как в сфере уголовного, так и в сфере административного, гражданско-правового, налогового, трудового и репутационного характера. Следует детально показывать, каким образом незаконное получение доступа к чужим сведениям, использование подставных счетов, содействие обналичиванию, регистрация фиктивных учетных записей, передача средств связи, оформление карт на третьих лиц, участие в схемах сокрытия происхождения денежных средств или приобретение похищенных цифровых продуктов образуют составы противоправного поведения либо выступают звеньями более широкого преступного механизма. В научно выверенной и одновременно публицистически сильной форме необходимо утверждать очевидное: **не существует "безобидного" участия в преступной инфраструктуре**. Каждое звено, каким бы малым оно ни казалось, укрепляет систему, питающую мошенничество, вымогательство, незаконный оборот запрещенных предметов, хищение средств, посягательства на частную жизнь и иные общественно опасные деяния.

Особое место занимает **демонстрация прямой связи между так называемой "удобной услугой" и реальным преступлением**. Именно здесь должна быть преодолена одна из ключевых когнитивных уловок современной теневой среды: стремление отделить потребительский интерес от преступного происхождения услуги. Теневая цифровая сфера строится на языке эвфемизмов, подмен, нейтральных обозначений и псевдотехнических формул. Незаконное вмешательство в информационные системы выдается за "помощь в восстановлении доступа", сбыт похищенных сведений - за "информационное сопровождение", обман граждан - за "арбитражные схемы", распространение запрещенного материала - за "альтернативный контент", участие в финансовых преступлениях - за "дистанционную подработку". Подобная языковая маскировка разрушает способность общества к правовой квалификации происходящего.

Поэтому профилактика должна последовательно вскрывать реальное содержание теневой услуги. Необходимо показывать, что за обещанием "быстро решить вопрос" скрываются либо кража, либо вымогательство, либо

незаконный доступ, либо пособничество мошенничеству, либо легализация преступных доходов, либо иная форма общественно опасного поведения. Требуется наглядно и доказательно связывать каждую услугу с фактической цепочкой причинения вреда. Если гражданину предлагают приобрести сведения о частной жизни другого лица, ему должно быть ясно, что речь идет не об “информации”, а об инструменте давления, шантажа, дискредитации и разрушения конституционно охраняемых благ. Если ему предлагают за вознаграждение использовать банковские реквизиты для “перевода средств”, он должен понимать, что становится частью механизма сокрытия денежных потоков, обслуживающего мошенничество, наркопреступность, коррупционные сделки или иные тяжкие деяния. Если подростку предлагают распространять в сети определенный материал за “простое вознаграждение”, необходимо показывать, что это может быть участие в экстремистской, мошеннической, порнографической, наркотической или иной преступной деятельности. **Правовое просвещение в данной сфере должно не просто информировать, а срывать маску с преступления**.

Исключительно важной представляется **специальная предупредительная работа с молодежью**, поскольку именно молодые люди чаще всего оказываются объектом поэтапного вовлечения в теневые цифровые практики. Здесь преступная среда действует расчетливо, тонко и безжалостно. Она использует возрастные особенности: стремление к признанию, поиску самостоятельного заработка, интерес к запретному, недооценку отдаленных последствий, доверчивость к авторитету “опытного собеседника”, склонность воспринимать цифровую среду как пространство условности и игры. На этой почве выстраиваются механизмы вовлечения, которые нередко начинаются с внешне нейтральных действий: выполнения мелких поручений, регистрации учетных записей, передачи средств связи, размещения объявлений, доставки предметов, приема и пересылки денежных средств, распространения сообщений, участия в закрытых сообществах. По существу же речь идет о постепенном разрушении правовых барьеров и нравственной чувствительности личности.

Следовательно, профилактика среди молодежи не может ограничиваться абстрактными призывами “не нарушать закон”. Нужна глубокая, возрастно дифференцированная и педагогически выверенная работа, в основе которой лежит **раскрытие типичных сценариев вовлечения, признаков манипуляции, способов психологического давления, механизмов вербовки и последующего использования зависимого положения вовлеченного лица**. Подросток и молодой человек должны уметь распознавать не только прямой преступный призыв, но и начальные стадии втягивания: обещание “легких денег”, предложение сохранить “полную анонимность”, убеждение, будто “ничего серьезного не происходит”, ссылки на массовый характер практики,

апелляцию к нужде, к обиде, к чувству исключительности или протесту. Необходимо внятно разъяснять, что преступная среда никогда не предлагает равноправного сотрудничества: она ищет исполнителя, которого можно заменить, использовать, шантажировать, подставить и в критический момент сделать крайним. **За фасадом мнимой свободы здесь почти всегда скрывается эксплуатация, а за обещанием заработка - перспектива судимости, утраты образования, разрушения семьи и социального будущего**.

Вместе с тем профилактическое воздействие в молодежной среде должно опираться не только на страх наказания, но и на формирование устойчивой правовой идентичности. Недостаточно сказать молодому человеку, чего нельзя делать; необходимо показать, **почему соблюдение закона является формой личного достоинства, гражданской зрелости и подлинной свободы**, а не внешним ограничением. В противном случае любые предупреждения быстро вытесняются соблазном выгоды. Здесь особенно велика роль образовательной среды, семьи, наставничества, а также примеров социально одобряемой самореализации. Молодежь должна видеть перед собой не только перечень запретов, но и ясную альтернативу - законные пути профессионального роста, творческого развития, общественного участия, получения дохода и признания. Там, где законное пространство пустеет, его немедленно заполняет преступный посредник.

Особое значение имеет **адресная работа с уязвимыми социальными группами**, поскольку спрос на криминальные цифровые услуги нередко усиливается не только из-за правового невежества, но и вследствие бедности, социальной изоляции, долговой нагрузки, низкого уровня образования, зависимости, семейной дезорганизации, безработицы, миграционной неустроенности, цифровой неграмотности, психологической нестабильности и иных факторов социального неблагополучия. Игнорировать эти обстоятельства - значит подменять реальную профилактику декларацией. Человек, поставленный в условия хронической нужды, гораздо легче принимает предложение об участии в сомнительной схеме; лицо, испытывающее одиночество и отсутствие признания, быстрее попадает под влияние закрытых сообществ; гражданин с низким уровнем правовой культуры чаще верит в безнаказанность незаконных операций. Следовательно, спрос на криминальные услуги должен рассматриваться не только как продукт индивидуального выбора, но и как следствие накопленных социальных деформаций.

Адресная профилактика предполагает выявление тех групп населения, для которых риск вовлечения особенно высок, и выстраивание с ними **не усредненной, а содержательно и социально соразмерной коммуникации**. Для несовершеннолетних это одни формы воздействия; для безработных молодых мужчин - другие; для лиц пожилого возраста, уязвимых перед мошенничеством, - третьи; для граждан, уже имевших опыт

административных или уголовных правонарушений, - четвертые. При этом речь не должна идти о стигматизации. Напротив, эффективная профилактика исходит из признания человеческого достоинства каждого лица и из необходимости предупреждать преступление прежде, чем оно превратится в личную катастрофу. Государство обязано не только запрещать, но и предлагать выход: юридическую помощь, социальное сопровождение, программы трудоустройства, просветительские мероприятия, психологическую поддержку, восстановление образовательной траектории, семейное консультирование. **Там, где уязвимый человек получает законную опору, спрос на преступную услугу теряет значительную часть своей притягательности**.

Информационно-правовое воздействие в целом должно быть построено на принципе непрерывности, доказательности и жизненной достоверности. Эпизодические кампании, приуроченные к отдельным происшествиям, не способны существенно изменить ситуацию, если они не превращаются в длительное присутствие права в общественном сознании. Следует исходить из того, что современная цифровая среда непрерывно воспроизводит новые формы соблазна, нейтрализует прежние предупреждения, обновляет способы маскировки и создает иллюзию нормальности там, где действует преступный расчет. В ответ на это государство и общество должны формировать **устойчивый режим правовой видимости преступления**, при котором ни одна теневая услуга не воспринимается как нейтральная, техническая или бытовая. Для этого необходимо сочетание правового просвещения, общественной дискуссии, аналитических публикаций, судебной практики, разъяснений компетентных органов, научной экспертизы, работы образовательных и культурных институтов.

Принципиально важно, чтобы профилактическая риторика не сводилась к казенному перечислению запретов. В научно-публицистическом измерении она должна обладать нравственной энергией, интеллектуальной глубиной и фактической безупречностью. Общество должно слышать не безликое уведомление, а **ясный голос правопорядка**, который называет вещи своими именами: незаконный доступ есть посягательство на безопасность; приобретение преступной услуги есть вклад в расширение преступного рынка; использование похищенных сведений есть участие в причинении вреда; передача своих реквизитов преступникам есть не “помощь знакомым”, а открытие канала для дальнейшего хищения и сокрытия следов; равнодушное потребление криминального содержимого есть форма общественного соучастия в разложении правовой среды. Когда эти смыслы не проговариваются, преступление получает важнейшее преимущество - право быть неправильно понятым.

В конечном счете необходимо твердо признать: **нельзя ограничиваться только борьбой с предложением; необходимо последовательно, настойчиво и целенаправленно сокращать сам спрос на криминальные цифровые**

услуги. Там, где сохраняется потребитель незаконного продукта, неизбежно возникает и его поставщик; там, где общество терпимо к теневой выгоде, преступность будет вновь и вновь воспроизводить себя в новых организационных формах; там, где гражданин ищет удобство любой ценой, право будет вытесняться расчетом, а общественная безопасность - частным корыстным интересом. Поэтому подлинная профилактика - это не периферийная мера, а **стратегия гражданского самоохранения общества**, его нравственной мобилизации и правового самоуважения. Лишь при таком подходе возможно не просто реагировать на уже совершенные деяния, но и разрушать саму среду, в которой незаконная цифровая услуга кажется выгодной, привычной и допустимой. Именно здесь проходит рубеж между формальным противодействием и подлинной защитой общества от современной преступности.

6.2. Переход от абстрактной пропаганды к доказательной профилактике

В современном обществе профилактика преступности в цифровой среде не может более оставаться областью общих призывов, нравоучительных формул и отвлечённых предостережений, рассчитанных на неопределённого адресата. Подобная форма информационного воздействия утратила действенность именно потому, что преступная среда радикально изменила способы собственного воспроизводства. Она больше не действует исключительно через грубое принуждение, открытые угрозы или очевидное склонение к противоправному поведению. Напротив, её сила заключается в способности растворяться в привычных формах повседневной коммуникации, подражать обычным способам занятости, имитировать законный заработок, маскироваться под бытовые услуги, посредническую деятельность, помощь в расчётах, доставку, оформление заказов, удалённое содействие, инвестиционное сопровождение, подбор персонала, обучение, консультирование и иные внешне безобидные формы социальной активности. В этих условиях прежняя абстрактная пропаганда оказывается не просто слабой, но в известной мере беспомощной, поскольку она борется не с реальными механизмами вовлечения, а с их упрощённым и устаревшим образом.

Именно поэтому профилактика должна строиться на доказательной основе, то есть на систематическом исследовании фактических способов вовлечения, на точном описании преступных сценариев, на выявлении закономерностей поведения вербовщиков, посредников и организаторов, на анализе судебной практики, следственных материалов, показаний потерпевших, статистически подтверждённых моделей коммуникации и повторяющихся элементов преступной маскировки. Речь идёт о переходе от словесного осуждения к познавательно насыщенному, юридически выверенному и психологически точному разъяснению опасности. Только тогда профилактика перестаёт быть внешним шумом и становится инструментом распознавания угрозы.

Особое значение в такой системе приобретает **кейс-аналитика**, то есть исследование конкретных случаев вовлечения лиц в противоправную деятельность с последующим выделением типичных признаков, последовательности действий и устойчивых механизмов воздействия. Конкретный случай обладает несравненно большей убедительностью, чем любой отвлечённый призыв, потому что он демонстрирует не абстрактную возможность риска, а уже реализованный путь преступного втягивания. В одном случае это может быть предложение «временной подработки» с минимальными требованиями и обещанием ежедневной оплаты; в другом - просьба оформить на себя счёт, платёжный инструмент или средство связи «для нужд организации»; в третьем - вовлечение в пересылку посылок, получение денежных средств, регистрацию учётных записей, размещение объявлений, получение кодов подтверждения, передачу реквизитов, формальное участие в цепочке расчётов. Внешне такие действия не всегда воспринимаются как уголовно наказуемые, особенно если они совершаются частями, под видом разовых поручений и без немедленного раскрытия конечной цели. Однако именно кейс-аналитика позволяет показать, как из совокупности, казалось бы, нейтральных действий складывается полноценное участие в преступной схеме.

Научно обоснованная профилактика должна не просто пересказывать отдельные примеры, а **раскрывать модели вовлечения**, лежащие в их основе. Эти модели имеют определённую внутреннюю логику. Как правило, вовлечение начинается с устранения настороженности. Для этого используются признаки обыденности: вежливое обращение, деловой тон, отсутствие прямых требований нарушить закон, обещание простых обязанностей, понятная бытовая легенда, указание на срочность, но не чрезвычайность, подчёркивание доступности работы для всех, в том числе для студентов, безработных, лиц с низким доходом, мигрантов, граждан, находящихся в долговой зависимости, а также тех, кто ищет быстрый способ получить средства без длительного трудоустройства. Далее следует стадия постепенного смещения нравственных и правовых ориентиров: лицу предлагают действие, которое кажется незначительным, временным, техническим и не несущим самостоятельной общественной опасности. После этого запускается механизм дробления ответственности: каждое отдельное действие подаётся как второстепенное, не связанное с итоговым преступным результатом. Наконец, когда лицо уже включено в цепочку операций, ему сообщают либо часть истинной цели, либо создают ситуацию фактической зависимости, при которой отказ становится психологически, материально или организационно затруднительным.

Раскрытие моделей вовлечения особенно важно потому, что преступность в цифровой среде действует через нормализацию опасного поведения. Человеку внушается мысль о том, что его участие - лишь техническая помощь, временная формальность, мелкое содействие, не имеющее

отношения к тяжкому деянию. Так формируется ложная дистанция между исполнителем отдельного поручения и конечным преступным результатом. Между тем право оценивает поведение не по субъективной словесной оболочке, навязанной организатором, а по реальному содержанию действий, их направленности, осведомлённости лица, характеру его содействия и месту в общей схеме. Следовательно, профилактика должна заранее разрушать иллюзию правовой нейтральности промежуточных действий. Необходимо настойчиво и доказательно объяснять: передача реквизитов, оформление средств идентификации на подставное лицо, приём и пересылка денежных средств, регистрация фиктивных учётных записей, хранение и передача предметов неизвестного происхождения, участие в ложной переписке с потерпевшими, обработка заказов, не имеющих прозрачной хозяйственной цели, - всё это может выступать звеньями единого преступного механизма и влечь самостоятельную уголовно-правовую оценку.

Существенным элементом доказательной профилактики является **систематизация типовых схем обмана**. Преступник редко действует в полной импровизации; куда чаще он воспроизводит уже проверённые конструкции психологического воздействия. Одни схемы строятся на обещании лёгкого дохода при минимуме усилий, другие - на эксплуатации доверия к якобы официальным структурам, третьи - на подражании законной коммерческой деятельности, четвёртые - на эмоциональном давлении, жалости, страхе потерять возможность заработка, желании срочно решить материальную проблему. При этом типовая схема обмана всегда сочетает несколько обязательных компонентов: создание видимости законности, дозированное раскрытие информации, перевод общения в закрытые каналы, подмена понятий, исключение времени на обдумывание, смещение акцента с цели на процедуру, уверения в безопасности, ссылки на массовый характер практики, а также постоянное словесное обезвреживание сомнений. Человеку не говорят: «соверши преступление». Ему говорят: «это обычная формальность», «так делают все», «ты лишь помогаешь провести платёж», «ничего незаконного здесь нет», «ответственность несёт руководство», «твоя задача только передать», «это временно», «это проверка», «это внутренний порядок», «это защита от ограничений», «это необходимо для обслуживания клиента». Вся риторика строится на вытеснении существа действий их внешней технической оболочкой.

Именно поэтому профилактическая работа должна не просто перечислять опасные предложения, но **разбирать язык обмана как инструмент криминального воздействия**. Слова в подобных схемах выполняют не описательную, а маскирующую функцию. Они не сообщают действительное положение вещей, а переупаковывают его в форму, удобную для восприятия жертвой или промежуточным исполнителем. Под видом нейтральной

лексики скрывается перераспределение риска: всю опасность берёт на себя вовлечённое лицо, тогда как организатор остаётся в тени, сохраняя дистанцию, а следовательно, и больший объём защиты от немедленного выявления. Поэтому профилактика должна обучать не просто осторожности, а распознаванию словесных индикаторов подмены: чрезмерно расплывчатого описания обязанностей, отказа заранее раскрыть содержание работы, требования использовать личные документы или платёжные реквизиты в интересах третьих лиц, обещания несоразмерно высокого вознаграждения за примитивные действия, уклонения от письменного оформления, навязывания срочности, а также категорического требования не обсуждать поручение с родственниками, знакомыми, юристами или представителями государственных органов.

Неотъемлемой частью доказательной профилактики выступает **обращение к реальным судебным последствиям**. Общество должно видеть не только момент вербовки, но и весь правовой итог преступного вовлечения. Пока профилактика ограничивается фразами о «возможной ответственности», она остаётся в сфере условного предупреждения и не достигает необходимой убедительности. Иное дело - системное разъяснение того, как квалифицируются соответствующие деяния, какие именно составы преступлений усматриваются в действиях посредников, номинальных исполнителей, лиц, предоставляющих свои данные, перевозчиков, получателей, хранителей, связных, лиц, осуществляющих коммуникацию с потерпевшими или перевод денежных средств, и как суд оценивает их доводы о незнании, техническом характере участия или отсутствии личной заинтересованности в конечном результате. Судебная практика убедительно показывает: ссылка на то, что лицо «только передало», «только оформило», «только получило», «только перевело», далеко не всегда устраняет уголовную ответственность. Напротив, при наличии совокупности объективных и субъективных признаков такие действия рассматриваются как пособничество, соисполнительство, участие в легализации преступных доходов, содействие мошенничеству, незаконному обороту запрещённых веществ, преступлениям против собственности, преступлениям в сфере компьютерной информации либо иным деяниям в зависимости от конкретной фактической конструкции.

Разъяснение судебных последствий выполняет двойную функцию. Во-первых, оно разрушает миф о безнаказанности периферийных участников преступной сети, которых часто убеждают в том, что вся ответственность лежит исключительно на «главных организаторах». Во-вторых, оно возвращает правовой разговор к его подлинному основанию: уголовное право реагирует не на самооправдание лица, а на его реальный вклад в общественно опасное деяние. При этом крайне важно освещать не только факт назначения наказания, но и сопутствующие последствия: судимость, ограничения в сфере трудоустройства, подрыв деловой и личной

репутации, имущественные взыскания, арест имущества, процессуальные издержки, ограничения на занятие определённых должностей и осуществление определённой деятельности, миграционно-правовые последствия для иностранных граждан, осложнение семейного положения, психологические последствия участия в уголовном процессе. Чем конкретнее раскрыт весь спектр правовых и социальных последствий, тем сильнее профилактический эффект.

Однако подлинная доказательность профилактики не исчерпывается юридическим описанием санкций. Она требует **углублённого разбора механизмов манипулирования доверием**, поскольку современное преступное вовлечение строится прежде всего не на демонстрации силы, а на эксплуатации базовых свойств человеческого сознания и социального поведения. Доверие - фундаментальная предпосылка нормального общежития; без него невозможны ни хозяйственный обмен, ни профессиональное взаимодействие, ни семейная и соседская взаимопомощь. Именно поэтому преступник стремится не разрушить доверие как таковое, а перехватить его, встроившись в привычные формы общения. Он использует символы законности, интонации компетентности, визуальные признаки официальности, последовательность делового взаимодействия, имитацию процедур, ссылки на правила, подтверждения, отзывы, рекомендации, мнимую прозрачность действий. Всё это создаёт у адресата чувство знакомой и потому безопасной среды.

Манипулирование доверием обычно осуществляется через несколько последовательно действующих психологических механизмов. Прежде всего это механизм авторитетности: сообщение оформляется так, чтобы у адресата возникло ощущение контакта с лицом, обладающим статусом, знаниями, специальными полномочиями или организационным ресурсом. Далее включается механизм взаимности: после минимального «доброжелательного» контакта от человека ожидают встречного шага - передачи данных, выполнения поручения, подтверждения операции, временного содействия. Затем действует механизм постепенного вовлечения: сначала предлагается незначительное действие, после которого повышается вероятность согласия на следующее. Немалую роль играет и механизм дефицита времени: спешка лишает человека способности к критической проверке обстоятельств. Наконец, особую опасность представляет механизм социальной нормализации, когда потенциальной жертве внушают, что подобные действия являются массовой, привычной и общепринятой практикой. Всё это требует от профилактики не лозунгового осуждения доверчивости, а тонкого и уважительного объяснения того, каким образом нормальные человеческие качества - отзывчивость, стремление к заработку, готовность помочь, вера в порядок, склонность следовать формальным инструкциям - превращаются в точки криминальной уязвимости.

Отсюда вытекает ещё одна принципиальная задача: **демонстрация того, как преступные сети маскируются под обычный сервис**. Это, пожалуй, одна из наиболее опасных особенностей современной криминальной организации. Преступная деятельность всё реже предъявляет себя в явном противоправном виде; напротив, она стремится быть неузнаваемой, похожей на повседневную услугу, на промежуточное обслуживание, на логистическое сопровождение, на расчётное посредничество, на операторскую поддержку, на помощь в оформлении, на деятельность по привлечению клиентов, на работу по обработке сообщений, на исполнение поручений, не выходящих за пределы бытовой рутины. В этом и состоит глубокий общественный вызов: преступление мимикрирует под удобство, скорость, доступность и бытовую полезность. Оно обещает снять затруднение, сократить путь, облегчить процедуру, устранить ограничения, сэкономить время, найти клиента, перевести средства, принять заказ, подтвердить личность, оформить доставку, помочь с расчётами. Но за этой оболочкой нередко скрывается распределённая криминальная система, в которой каждое «обычное» действие выступает функциональным элементом общего противоправного результата.

Научно ориентированная профилактика обязана вскрывать сам **механизм такой маскировки**. Во-первых, преступная сеть дробит свою структуру на множество малозаметных ролей, каждая из которых выглядит неопасной в отдельности. Во-вторых, она избегает полной информированности участников, чтобы каждый видел лишь свой фрагмент и не осознавал целого. В-третьих, она использует внешние признаки обычной хозяйственной или коммуникационной деятельности: переписку в деловом тоне, обозначение должностей, инструкции, графики, шаблоны ответов, формализованные поручения. В-четвёртых, она стремится переложить на вовлекаемое лицо правовой след: документы, платёжные операции, средства связи, физическое получение предметов, регистрацию учётных записей, подтверждение действий. В-пятых, она быстро заменяет одних исполнителей другими, сохраняя устойчивость системы даже при выявлении отдельных участников. Следовательно, профилактика должна показывать не только отдельный рискованный контакт, но и архитектуру преступной сети как целого: кто получает выгоду, кто несёт основной риск, кто остаётся невидимым, каким образом распределяются роли, почему периферийный участник чаще всего оказывается самым уязвимым перед уголовным преследованием.

Наиболее эффективна не устрашающая риторика, а ясное объяснение того, как цифровая повседневность превращается в среду криминального втягивания. Эта мысль имеет принципиальное методологическое значение. Устрашение действует кратковременно и часто лишь на тех, кто и без того склонен к осторожности. Более того, чрезмерно резкие и схематичные предупреждения нередко порождают обратный эффект: человек не узнаёт в

реальной ситуации описанную в назидательном сообщении угрозу именно потому, что действительность оказывается внешне намного прозаичнее, спокойнее и обыденнее. Цифровая повседневность опасна не своей исключительностью, а своей привычностью. Преступное предложение приходит в виде обычного сообщения. Незаконное поручение выглядит как мелкая услуга. Вербовка маскируется под трудоустройство. Передача реквизитов объясняется хозяйственной необходимостью. Переписка с потерпевшим подаётся как работа с клиентом. Получение и пересылка денежных средств именуются обработкой платежей. Принятие посылки называется логистической помощью. Оформление учётной записи - технической регистрацией. И если профилактика не разоблачает эту подмену формы и содержания, она проигрывает ещё до начала правового воздействия.

Именно поэтому современная профилактика должна носить **разъяснительно-аналитический характер**. Её предметом должен быть не отвлечённый образ «плохого деяния», а последовательность конкретных бытовых действий, которые в определённом сочетании образуют криминальную цепь. Необходимо показывать гражданину его собственную жизненную траекторию внутри риска: как предложение о подработке приходит в мессенджере; как собеседник избегает прямых ответов о работодателе; как сначала просят выполнить безобидное поручение; как затем появляется требование использовать личные документы, счёт, устройство или адрес; как создаётся искусственная срочность; как вводится запрет на разглашение; как обещается быстрый расчёт; как исчезает лицо, давшее поручение, после первой же проблемы; как именно вовлечённый остаётся единственным видимым участником всей схемы для потерпевшего, банка, оператора связи и правоохранительного органа. Только такая предметная реконструкция даёт человеку шанс своевременно распознать угрозу в реальной жизни, а не в учебной абстракции.

Для повышения эффективности информационно-правового воздействия следует добиваться **максимальной конкретности профилактического сообщения**. Недостаточно говорить: «не доверяйте подозрительным предложениям». Необходимо пояснять, какие именно признаки должны вызвать сомнение, почему они опасны, каким образом соотносятся с уже известными формами преступной деятельности и какие правовые последствия могут наступить. Недостаточно утверждать: «не передавайте свои данные». Требуется раскрывать, как именно личные данные, банковские реквизиты, идентификаторы связи, адреса получения, средства доступа и учётные записи используются в преступных целях, каким образом с их помощью создаётся ложная правовая видимость законности операций и почему именно владелец таких сведений первым оказывается в зоне следственного интереса. Недостаточно формально упоминать о манипуляции. Нужно показывать её поэтапно: установление контакта,

снижение критичности, создание мнимой выгоды, дробление поручений, подмена терминов, формирование зависимости, разрыв обратной связи после использования вовлечённого лица.

Вместе с тем доказательная профилактика должна сохранять **уважительный характер по отношению к адресату**. Публичное назидание, упрёк в доверчивости, морализаторство, высокомерное противопоставление «разумных» и «неразумных» граждан методологически несостоятельны и социально вредны. Они не укрепляют способность к распознаванию угроз, а лишь усиливают стыд, вытесняют опыт пострадавших в зону молчания и снижают готовность граждан обращаться за помощью. Между тем для профилактики исключительно ценен именно живой опыт тех, кто уже оказался вовлечён в преступную схему, кто сначала не распознал опасность, а затем столкнулся с уголовно-правовыми, имущественными и личными последствиями. Такой опыт должен быть не предметом осмеяния, а источником знания. Общество обязано извлекать из него выводы, а государственные и научные структуры - переводить эти выводы в ясные профилактические формулы.

Следовательно, **переход от абстрактной пропаганды к доказательной профилактике** представляет собой не частную методическую поправку, а глубокую смену самой философии предупреждения преступности. Речь идёт о переходе от лозунга к анализу, от устрашения к пониманию, от общих слов к юридически и психологически точному описанию угрозы, от формального информирования к выработке способности распознавать преступную маскировку в повседневной цифровой среде. Такая профилактика должна опираться на кейс-аналитику, раскрывать модели вовлечения, систематизировать типовые схемы обмана, демонстрировать реальные судебные последствия, вскрывать механизмы манипулирования доверием и последовательно показывать, как преступные сети прячутся под оболочкой обычного сервиса. Лишь в этом случае информационно-правовое воздействие перестанет быть ритуалом и станет действенным средством гражданской защиты.

В конечном счёте речь идёт о защите не только отдельных лиц, но и **самой ткани общественного доверия**, которая сегодня подвергается целенаправленной криминальной эксплуатации. Если государство, наука и общество не научатся объяснять гражданину, как именно преступление входит в его повседневность под видом удобства, заработка, услуги и простого поручения, то никакая внешняя строгость формулировок не восполнит дефицита подлинного понимания. Но если профилактика станет доказательной, предметной, юридически точной и психологически убедительной, она приобретёт ту силу, которой всегда недоставало отвлечённой пропаганде: силу разоблачения. А разоблачённый механизм вовлечения теряет значительную часть своей власти.

7. ПРАКТИЧЕСКИЕ ПРИОРИТЕТЫ НА БЛИЖАЙШУЮ ПЕРСПЕКТИВУ

В ближайшей и среднесрочной перспективе государственная политика противодействия организованной преступности, действующей в платформенной среде, не может ограничиваться отдельными мерами, рассчитанными на уже совершённое преступление. Перед правопорядком встаёт качественно новая задача: не просто реагировать на частные правонарушения, а выстраивать целостную систему раннего выявления, доказательственного закрепления, межведомственного сопоставления, финансового отслеживания, международного пресечения и упреждающего воздействия на те преступные образования, которые используют цифровую инфраструктуру как пространство рекрутирования, координации, маскировки и извлечения прибыли. Именно поэтому практические приоритеты на ближайшую перспективу должны быть поняты не как перечень разрозненных административных поручений, а как программа институционального переустройства государства перед лицом новой криминальной реальности.

Прежде всего необходимо **создание единых национальных центров анализа платформенной преступности**. Сегодня одна из главных слабостей государственного реагирования заключается в ведомственной дробности. Сведения о преступной активности распределены между органами внутренних дел, следственными органами, подразделениями финансового контроля, таможенными структурами, органами прокуратуры, службами безопасности, органами, осуществляющими надзор в сфере связи, и иными уполномоченными учреждениями. При этом преступные сети, напротив, действуют как единый организм: они быстро меняют каналы общения, переносят денежные потоки, дробят роли, используют подставные учётные записи, удалённый доступ и трансграничную инфраструктуру хранения сведений. Государство, сталкиваясь с такой формой организованности, не может отвечать ей ведомственным разобщением.

Единый национальный центр анализа платформенной преступности должен стать не ещё одной бюрократической надстройкой, а **центром собирания, сопоставления и прогностического осмысления криминально значимой информации**. Его задача - не подменять следствие или дознание, а обеспечивать аналитическое превосходство государства. Такой центр должен аккумулировать сведения о типичных преступных схемах, устойчивых цифровых следах, способах конспирации, повторяющихся признаках координации, маршрутах движения преступных доходов, взаимосвязях между площадками распространения незаконного содержания, посредническими звеньями и конечными выгодоприобретателями. Особое значение имеет выработка единых методик выявления криминальных платформ: от анализа структуры сетевого взаимодействия до установления признаков централизованного управления, распределения ролей, повторяемости преступного поведения и

сопряжённости цифровой активности с реальными экономическими и насильственными преступлениями.

Не менее существенным является **утверждение стандартов цифровой фиксации доказательств**. Правоприменительная практика показывает, что именно доказательственная уязвимость нередко превращает очевидную преступную деятельность в юридически расплывчатую картину, недостаточную для вынесения обоснованного процессуального решения. Цифровая среда отличается быстротой изменения, лёгкостью удаления сведений, возможностью ретроспективного редактирования, множественностью промежуточных посредников и высокой зависимостью от правильности процессуального закрепления. В таких условиях произвольные, фрагментарные и технически несопоставимые способы фиксации становятся прямой угрозой правосудию.

Государству необходимы **обязательные единые правила удостоверения цифровых следов**, охватывающие порядок обнаружения, изъятия, копирования, описания, хранения и представления сведений, имеющих значение для уголовного судопроизводства. Речь идёт о процессуально выверенной фиксации переписки, файлов, метаданных, сведений о времени, маршрутах передачи, идентификаторах устройств, сетевых журналах, сведениях о платежах, действиях пользователей, параметрах доступа и следах изменения информации. Такие стандарты должны предусматривать требования к непрерывности цепи хранения, к подтверждению целостности изъятых данных, к документированию применённых технических средств, к допустимости удалённого осмотра информации, к удостоверению происхождения файлов, к отражению всех манипуляций, произведённых с цифровым носителем. Без этого государство будет постоянно сталкиваться с опасной ситуацией, когда преступник выигрывает не потому, что он невиновен, а потому, что следы его деятельности были закреплены юридически ненадлежащим образом.

Следующий приоритет - **запуск межведомственных баз индикаторов криминальных сетей**. Современная организованная преступность редко обнаруживает себя единичным ярким событием. Гораздо чаще она проявляется россыпью, на первый взгляд, несвязанных признаков: сходством речевых формул в разных каналах общения, совпадением временных интервалов публикаций, повторяемостью способов вербовки, типичными маршрутами перевода средств, общими техническими параметрами учётных записей, схожими способами маскировки товаров и услуг, повторяющимися посредническими кошельками, адресами, устройствами и контактами. Когда эти признаки остаются разрозненными, преступная сеть сохраняет невидимость. Когда же они системно накапливаются и сопоставляются, перед государством проступает структурная карта преступного объединения.

Подобные базы должны включать не только данные о конкретных лицах, но прежде всего **систему криминалистически значимых индикаторов**, то есть признаков, позволяющих устанавливать принадлежность отдельных цифровых эпизодов к более широкой организованной деятельности. Важно, чтобы такие массивы сведений формировались на законной основе, с ясным разграничением доступа, со строгими гарантиями прокурорского и судебного контроля там, где это требуется, и с возможностью оперативного обновления данных. Практическая ценность межведомственных баз заключается в том, что они позволяют перейти от эпизодического пресечения к выявлению всей архитектуры преступной сети: организаторов, администраторов, кураторов, исполнителей, поставщиков технических ресурсов, финансовых операторов и лиц, обеспечивающих легализацию доходов.

Особого внимания требует **укрепление финансовой и криптоаналитики**. Следует прямо признать: в условиях платформенной преступности движение денежных средств становится не вторичным сопутствующим элементом, а центральной осью преступной деятельности. Именно через финансовые потоки проявляется внутренняя структура преступного объединения, распределение ролей, масштабы операций, территориальный охват и степень устойчивости сети. Деньги - это язык организованной преступности, и, если государство не научится читать этот язык во всей его сложности, оно будет постоянно опаздывать.

Финансовая аналитика должна охватывать как традиционные формы расчётов, так и расчёты, осуществляемые с использованием цифровых активов, распределённых реестров и производных способов сокрытия происхождения средств. Здесь требуется сочетание правовых, экономических и криминалистических подходов. Необходимо развивать методы выявления аномальных переводов, дробления сумм, каскадного перераспределения средств, использования множественных посреднических кошельков, быстрого преобразования цифровых активов в обычные денежные средства и обратных конверсионных операций, направленных на разрыв следа происхождения имущества. Но не менее важно уметь интерпретировать эти процессы в доказательственном ключе: связывать движение средств с конкретными преступными эпизодами, с лицами, управлявшими расчётами, и с конечными выгодоприобретателями. **Без глубокого финансового анализа никакое пресечение платформенной преступности не может быть признано завершённым**, поскольку изъятие отдельных исполнителей без разрушения финансового контура преступной сети лишь создаёт условия для её быстрого восстановления.

К числу неотложных задач относится и **создание процедур срочного международного сохранения данных**. Цифровая преступность давно вышла за пределы национальной юрисдикции не только по последствиям, но и по инфраструктуре. Сведения, имеющие решающее значение для

расследования, могут храниться на серверах в одной стране, управляться из другой, затрагивать потерпевших в третьей, а использоваться преступной группой, распределённой между несколькими государствами. При этом ключевая проблема заключается не только в получении таких данных, но прежде всего в их оперативном сохранении. Пока проходят традиционные, зачастую затяжные процедуры международной правовой помощи, сведения нередко удаляются, изменяются или становятся фактически недоступными.

Следовательно, международное сотрудничество должно включать **ускоренные механизмы срочного закрепления и сохранения цифровой информации** до момента последующего процессуального и дипломатического оформления её передачи. Такие процедуры необходимы в отношении журналов доступа, регистрационных сведений, данных о соединениях, содержимого переписки в пределах, допускаемых правом соответствующего государства, технических характеристик учётных записей, платёжной информации, сведений о привязанных устройствах и иных данных, подверженных риску быстрой утраты. Здесь требуется не только договорная база, но и сеть постоянно действующих контактных пунктов, способных реагировать круглосуточно, по единым протоколам и в короткие сроки. Иначе организованная преступность будет и далее пользоваться асимметрией времени: государствам нужны недели и месяцы, преступникам - минуты.

В этом же контексте принципиальное значение имеет **инициирование в Интерполе специализированных рабочих направлений по платформенной организованной преступности**. Международные полицейские структуры объективно сталкиваются с необходимостью обновления приоритетов. Если в центре внимания прежних десятилетий находились в основном традиционные формы транснациональной организованной преступности - наркотрафик, торговля людьми, незаконный оборот оружия, отмывание доходов, - то сегодня все эти явления всё чаще организуются, маскируются и масштабируются через цифровые площадки. Это требует не простого расширения уже существующих форм работы, а формирования самостоятельного направления, посвящённого именно платформенной природе современного организованного преступления.

Такое направление должно заниматься **систематизацией типологий преступных платформ, обменом лучшими следственными и аналитическими практиками, координацией международных операций, выработкой единых понятий и созданием каналов быстрого оповещения о новых преступных моделях**. Важнейшим результатом станет формирование общей международной картины угрозы, при которой отдельные государства перестанут видеть лишь локальные эпизоды и смогут соотнести свои данные с более широкими трансграничными процессами. Платформенная преступность не уважает государственные границы; стало быть, и ответ на неё не может оставаться узко национальным.

Однако никакие организационные реформы не будут действенны без **разработки программ подготовки кадров гибридного профиля**. Сегодня особенно отчётливо обнаруживается дефицит специалистов, способных одинаково уверенно мыслить в правовой, криминалистической, технической, финансовой и международно-правовой плоскостях. Старые модели профессиональной подготовки, основанные на жёстком разделении компетенций, уже не соответствуют сложности современных преступных экосистем. Следователь, не понимающий природы цифрового следа, рискует упустить важнейшие доказательства. Технический специалист, не владеющий уголовно-процессуальными требованиями, может получить сведения, недопустимые в суде. Сотрудник финансового контроля, не распознающий организованную структуру преступной сети, видит лишь отдельные подозрительные операции, но не всю систему.

Поэтому требуется формирование **нового поколения специалистов междисциплинарного типа**, которые способны соединять юридическую точность, аналитическую глубину, техническую грамотность и стратегическое понимание организованной преступности. Речь идёт не только о повышении квалификации действующих сотрудников, но и о пересмотре образовательных программ ведомственных учебных заведений, университетов и центров профессиональной подготовки. В таких программах должны сочетаться уголовное право, уголовный процесс, криминалистика, теория доказательств, финансовый мониторинг, международное сотрудничество, основы работы цифровых платформ, методы анализа сетевых связей, психология вовлечения в преступные сообщества, вопросы легализации преступных доходов и методика расследования трансграничных преступлений. **Государство, не подготовившее кадров для новой криминальной эпохи, неизбежно будет вести борьбу средствами прошлого против противника будущего**.

Стратегически значимым является и **включение оценки цифровых криминальных платформ в систему национальной безопасности**. Это положение требует особой настойчивости, поскольку до сих пор во многих государствах подобная преступность воспринимается как узкоспециальная проблема правоохранительных органов. Между тем платформенные преступные структуры затрагивают не только общественный порядок, но и экономическую устойчивость, доверие к институтам государства, безопасность несовершеннолетних, информационный суверенитет, устойчивость платёжной системы, санитарную и лекарственную безопасность, электоральные процессы, миграционную сферу и даже международную репутацию страны. Когда преступная сеть получает способность массово воздействовать на социальное поведение, управлять теневыми рынками и извлекать доходы из цифровой анонимности, речь идёт уже не о совокупности отдельных составов преступлений, а об угрозе системного характера.

Следовательно, оценка криминальных платформ должна быть встроена в государственные механизмы стратегического прогнозирования, в документы планирования в сфере безопасности, в систему национальных индикаторов угроз, в процедуры межведомственного обмена значимой информацией и в режимы реагирования на кризисные ситуации. Необходимо разрабатывать методики оценки масштаба, устойчивости и общественной опасности таких платформ, определять отрасли и социальные группы повышенного риска, учитывать влияние преступной цифровой инфраструктуры на легальную экономику и институты публичной власти. **Признание платформенной организованной преступности угрозой национальной безопасности - это не риторический жест, а необходимое условие мобилизации ресурсов государства**.

Наряду с мерами силового и организационного характера чрезвычайно важно **развивать превентивную информационно-правовую работу**. Ошибочно полагать, будто борьба с организованной преступностью исчерпывается раскрытием и наказанием. Платформенная среда живёт по законам постоянного расширения аудитории, и потому преступные сети неизменно стремятся не только скрываться, но и вовлекать. Они нормализуют противоправное поведение, представляют преступный заработок как обычную жизненную стратегию, маскируют насилие под услугу, а участие в преступной схеме - под малозначительную подработку. Особенно уязвимыми оказываются молодёжь, лица с низкой правовой осведомлённостью, пользователи, находящиеся в трудном материальном положении, и граждане, не способные критически распознавать манипулятивные практики.

Поэтому превентивная работа должна быть выстроена как **системная государственная политика правового просвещения и общественного предупреждения**. Она должна раскрывать реальные механизмы вовлечения в преступные схемы, показывать правовые последствия участия даже в «низовых» ролях, разъяснять признаки вербовки, способы психологического давления, формы использования персональных данных, риски передачи платёжных средств третьим лицам, опасность участия в посреднических переводах и хранения чужих цифровых активов. Но не менее важно публично разрушать миф о безнаказанности и «безличности» платформенной преступности. Общество должно ясно понимать: за фасадом безличных каналов связи стоят конкретные организаторы, конкретные жертвы, конкретные разрушенные судьбы и конкретный ущерб государству. Превенция здесь - не украшение карательной политики, а её необходимое продолжение и опора.

Наконец, необходимо **добиваться международной стандартизации взаимодействия с платформами**. В условиях, когда значительная часть коммуникативной, торговой и платёжной активности сосредоточена на частных цифровых площадках, эффективность противодействия

преступности в значительной мере зависит от того, насколько единообразно и предсказуемо выстроены отношения государств с такими субъектами. Сегодня эта сфера во многом страдает от фрагментарности: разные государства предъявляют различные требования к срокам реагирования, к порядку раскрытия сведений, к процедурам удаления противоправного содержания, к сохранению данных, к идентификации пользователей и к исполнению запросов компетентных органов. Такой разнобой создаёт правовую неопределённость и даёт преступным сетям возможность выбирать наиболее выгодные юрисдикции и площадки.

Международная стандартизация должна быть направлена на **выработку согласованных минимальных обязанностей платформ в сфере сохранения данных, реагирования на законные запросы, уведомления о выявленных признаках тяжкой организованной преступной деятельности, защиты доказательственной целостности информации и соблюдения прав пользователей**. Здесь крайне важно соблюсти правовой баланс: государство не должно превращать частные площадки в бесконтрольный карательный инструмент, но и платформы не вправе прикрываться технической нейтральностью там, где их инфраструктура систематически используется для координации тяжких преступлений, торговли запрещёнными предметами, отмывания доходов, эксплуатации уязвимых лиц и вербовки исполнителей. Требуется международно согласованная модель, при которой обязанности платформ будут чётко очерчены, процедуры - прозрачны, контроль - законен, а права личности - гарантированы. Только при таком подходе возможно преодолеть нынешнюю ситуацию, когда трансграничная частная инфраструктура развивается быстрее, чем механизмы публичной ответственности.

Подводя итог, следует подчеркнуть: перечисленные приоритеты образуют **единую архитектуру практического ответа государства на платформенную организованную преступность**. Национальные аналитические центры без единых стандартов доказательственной фиксации окажутся перегруженными спорными данными. Стандарты фиксации без межведомственных баз индикаторов не позволят увидеть сеть целиком. Финансовая аналитика без международного сохранения данных будет запаздывать. Международное сотрудничество без подготовки кадров превратится в формальность. Стратегическое признание угрозы без превенции не сократит социальную базу вовлечения. А взаимодействие с платформами без международной стандартизации останется неравномерным и уязвимым.

Именно поэтому в ближайшей перспективе от государств требуется не косметическое усовершенствование отдельных процедур, а **политическая воля к системному переосмыслению самого характера борьбы с организованной преступностью в цифровую эпоху**. Время половинчатых решений прошло. Преступные сети уже научились превращать

платформенную среду в пространство власти, прибыли и контроля. Вопрос теперь заключается в том, сумеет ли государство превратить эту же среду в пространство законности, доказуемости, международной координации и неотвратимого правового воздействия. От ответа на этот вопрос зависит не только эффективность уголовной политики, но и способность современного государства сохранить суверенитет права в условиях стремительно меняющейся технологической действительности.

8. ЗАКЛЮЧЕНИЕ

Современный этап развития общественных отношений убедительно показывает: цифровая среда перестала быть лишь вспомогательным пространством общения, обмена сведениями и повседневной координации действий. Она превратилась в одну из ключевых сред социальной организации, внутри которой формируются устойчивые связи, распределяются роли, поддерживаются модели доверия, воспроизводятся поведенческие стереотипы и закрепляются практики коллективного взаимодействия. Именно поэтому цифровые коммуникационные площадки, используемые миллионами людей в обыденной жизни, все чаще выступают не просто фоном, на котором присутствует преступность, а полноценной средой ее функционирования. В этих условиях организованная преступность получает качественно новые возможности: скрывать структуру взаимодействий, быстро перераспределять функции между участниками, восполнять утраченные звенья, переносить активность между различными каналами связи и сохранять устойчивость даже при частичном разрушении отдельных элементов своей сети.

Принципиальная опасность данного явления заключается в том, что речь идет уже не о единичных противоправных эпизодах, совершаемых с использованием технических средств, а о глубокой перестройке самой логики преступной организации. Если ранее преступная среда в значительной степени зависела от территориальной близости участников, от личных контактов, от материально фиксируемых каналов связи и от сравнительно медленного процесса вербовки, координации и перераспределения ресурсов, то сегодня значительная часть этих ограничений утрачивает свое прежнее значение. Цифровая коммуникационная среда снижает издержки преступного взаимодействия, расширяет географический охват, повышает скорость принятия решений и позволяет поддерживать относительную анонимность при внешней видимости обычной повседневной коммуникации. Тем самым создается ситуация, при которой преступная деятельность не противостоит социальной реальности извне, а все плотнее встраивается в ее обыденные механизмы.

Необходимо подчеркнуть, что **угроза определяется не только техническими характеристиками используемых площадок**. Безусловно, имеют значение

шифрование, распределенность серверной инфраструктуры, быстрое удаление сведений, возможность создания множества учетных записей, высокая скорость передачи сообщений, сложность установления действительного местонахождения участников. Однако сводить проблему лишь к этим обстоятельствам означало бы неоправданно сужать ее содержание. Не меньшую, а во многих случаях и большую роль играют социальная встроенность указанных площадок, их массовая легитимность в глазах населения, психологическая привычность использования и тот факт, что преступное взаимодействие маскируется под обычную, ничем не выделяющуюся повседневную активность. Там, где миллионы законопослушных граждан ежедневно обмениваются сообщениями, совершают покупки, ищут работу, участвуют в обсуждениях и поддерживают личные контакты, преступные структуры получают беспрецедентную возможность растворяться в общем потоке коммуникации, пользоваться его объемом и ритмом как естественным прикрытием.

Психологическая привычность цифровой среды создает для организованной преступности особое преимущество. Человек склонен воспринимать регулярно используемое средство связи как нейтральное, безопасное и бытовое. Это снижает уровень настороженности, облегчает вовлечение новых участников, размывает ощущение границы между дозволенным и противоправным, способствует формированию у исполнителей ложного представления о дистанцированности от последствий совершаемых деяний. Когда преступное поручение передается в форме краткого сообщения, когда координация действий осуществляется через привычный интерфейс, когда вербовка происходит в пространстве, которое ассоциируется с обыденным общением, противоправное действие утрачивает в восприятии части участников свою очевидную исключительность. Возникает опасный эффект нормализации, при котором преступление перестает ощущаться как выход за пределы социально допустимого и начинает восприниматься как одна из разновидностей прагматической занятости, посреднической деятельности или «обычной» услуги. Подобная психологическая трансформация особенно разрушительна в молодежной среде, где навыки цифрового взаимодействия предшествуют полноценному формированию правосознания и гражданской ответственности.

Не менее существенным является и то обстоятельство, что **цифровая преступная инфраструктура обладает высокой восстановительной способностью**. Традиционные меры пресечения, даже будучи успешными на уровне отдельных эпизодов, учетных записей, групп или посредников, нередко оказываются недостаточными для достижения устойчивого результата. Закрытие одного канала связи, удаление одной преступной группы, задержание одного координатора или изъятие одного массива

сведений не ведут автоматически к разрушению всей сети. Напротив, сетевой принцип организации позволяет преступным структурам быстро воспроизводить утраченные элементы, переносить коммуникацию на соседние площадки, дублировать каналы координации, использовать заранее подготовленные резервные учетные записи и восстанавливать нарушенные связи в течение крайне короткого времени. В этой способности к самовоспроизведению проявляется одно из важнейших качеств современной организованной преступности - ее структурная гибкость, благодаря которой даже результативные силовые действия нередко дают лишь временный, а не окончательный эффект.

Именно поэтому **для правоохранительных органов и иных силовых ведомств назрела необходимость перехода к принципиально новой модели деятельности**. Прежние подходы, основанные преимущественно на расследовании уже совершенных эпизодов, на реагировании по факту наступивших последствий и на ведомственной замкнутости, более не соответствуют масштабу и динамике угрозы. Современная модель противодействия должна быть межведомственной по своему устройству, аналитически насыщенной по методам, технологически оснащенной по инструментарию и согласованной по целям и процедурам. Под межведомственностью в данном случае следует понимать не формальное распределение полномочий, а реально действующий режим совместной работы, при котором сведения, поступающие в распоряжение различных органов, не рассеиваются по замкнутым контурам, а интегрируются в единое представление о структуре угрозы. Организованная преступность выигрывает там, где государство раздроблено на ведомственные участки ответственности; следовательно, эффективное противодействие возможно лишь там, где сведения, компетенции и оперативные возможности соединяются в единую систему.

Аналитическое насыщение противодействия предполагает отказ от узкого понимания расследования как простой фиксации уже выявленного события. Необходим переход к выявлению закономерностей, устойчивых связей, ролевого распределения, способов маскировки, каналов финансового обеспечения, механизмов кадрового воспроизводства, маршрутов распространения запрещенных предметов и сведений, а также к раннему обнаружению признаков формирования новых преступных контуров. В центре внимания должны находиться не только конкретные исполнители, но и повторяющиеся модели поведения, которые указывают на существование организующей структуры. Речь идет о необходимости видеть преступление не как отдельный акт, а как проявление более крупной системы, имеющей свою внутреннюю дисциплину, специализацию функций, каналы пополнения и механизмы самозащиты. Только в этом случае возможно перейти от фрагментарного пресечения к системному ослаблению преступной среды.

Технологическая оснащенность государства также требует принципиального переосмысления. В условиях, когда преступные сообщества оперативно осваивают новые способы сокрытия, автоматизируют отдельные процессы, используют распределенные схемы коммуникации и стремятся минимизировать число прямых контактов между участниками, государственные структуры не могут оставаться в положении догоняющей стороны. Однако и здесь необходима важная оговорка: технологическое усиление не должно пониматься исключительно как накопление технических средств наблюдения. Подлинная оснащенность означает наличие кадров, способных правильно интерпретировать цифровые следы, наличие единых методик их фиксации и оценки, наличие правовых оснований для своевременного реагирования, наличие защищенных контуров взаимодействия между ведомствами и наличие организационной культуры, ориентированной на быстрое преобразование разрозненных сведений в доказательственно и оперативно значимый результат. Техника без методологии и без квалифицированного анализа не создает преимущества; она лишь увеличивает объем необработанного материала.

Особого внимания заслуживает положение **органов государственной безопасности**, поскольку платформенная криминализация затрагивает не только уголовно-правовую сферу в ее традиционном понимании. По мере того как цифровые площадки становятся каналом для координации незаконного оборота запрещенных веществ, торговли оружием, вербовки исполнителей, легализации преступных доходов, распространения насильственных практик, подрыва общественного порядка и скрытого внешнего воздействия на внутренние процессы, проблема выходит за пределы обычной криминальной статистики. Она начинает затрагивать устойчивость государства как сложной политико-правовой системы. Когда криминальные сети получают возможность опираться на трансграничные цифровые коммуникации, использовать экономические и социальные уязвимости населения, влиять на локальные сообщества, финансировать деструктивные действия и маскировать их под повседневные цифровые практики, возникает уже не частная, а системная угроза.

Вопрос здесь стоит о защите общественной безопасности, институциональной устойчивости и элементов национального суверенитета. Суверенитет в современных условиях проявляется не только в контроле над территорией, границами и формальными юридическими режимами, но и в способности государства обеспечивать нормативный порядок внутри тех коммуникационных пространств, через которые осуществляется значительная часть общественной жизни. Если критически важные сегменты социальной координации опосредуются цифровыми площадками, находящимися вне реальной юрисдикционной доступности, если преступные сети используют эти площадки для устойчивого

воспроизводства своей деятельности, а государство вынуждено постоянно реагировать постфактум, не имея возможности влиять на структурные условия функционирования таких сред, то речь идет не просто о сложностях следственной практики. Речь идет о постепенном размывании способности государства гарантировать правопорядок в тех формах общественного взаимодействия, которые стали базовыми для современного человека. Отсюда вытекает необходимость рассматривать платформенную криминализацию как явление, имеющее не только уголовно-правовое, но и стратегическое значение.

Вместе с тем было бы ошибкой полагать, будто данная проблема может быть решена исключительно усилиями одного государства, сколь бы развитыми ни были его правовые и институциональные механизмы. **Трансграничный характер цифровой преступности** объективно делает международное измерение центральным условием результативного противодействия. Учетные записи могут создаваться в одной юрисдикции, координация - осуществляться через инфраструктуру другой, хранение сведений - происходить на технических мощностях третьей, а последствия преступной деятельности - проявляться на территории четвертой. Такая рассредоточенность разрушает традиционную линейную модель правоприменения, при которой государство, столкнувшись с правонарушением на своей территории, обладает достаточным набором средств для быстрой идентификации виновных и пресечения их деятельности. В цифровой среде эта цепочка разрывается множеством межгосударственных барьеров: различием правовых режимов, продолжительностью процедур международной правовой помощи, несовпадением требований к хранению и выдаче сведений, отсутствием единых стандартов реагирования со стороны цифровых посредников.

Именно поэтому **международному сообществу необходимо перейти от декларативных формул к реально действующим механизмам взаимодействия**. Слишком долго проблема обсуждалась преимущественно в терминах общих призывов к сотрудничеству, тогда как преступные сети тем временем выстраивали практические, быстрые и крайне эффективные схемы трансграничной координации. Государства не могут позволить себе роскошь медлительности там, где преступная коммуникация измеряется секундами, а официальные запросы - неделями и месяцами. Нужны механизмы ускоренного обмена значимыми сведениями, согласованные процедуры сохранения цифровых следов, общепризнанные критерии их допустимости, совместные оперативные мероприятия, а также единые или по меньшей мере сопоставимые подходы к ответственности тех посреднических структур, которые фактически обеспечивают среду для массового криминального взаимодействия. Без этого разрыв между скоростью преступной адаптации и скоростью государственного реагирования будет лишь увеличиваться.

Особого рассмотрения требует и **вопрос об ответственности цифровых посредников**. В современном публичном дискурсе нередко сталкиваются две крайности: либо на посредников возлагается почти вся вина за происходящее в цифровой среде, либо, напротив, они рассматриваются как полностью нейтральные носители чужой активности, не способные и не обязанные влиять на происходящее. Обе позиции представляются методологически несостоятельными. Цифровой посредник действительно не тождественен преступному сообществу, использующему его инфраструктуру, однако и его роль не может быть сведена к простому техническому присутствию. Чем масштабнее площадка, чем глубже она интегрирована в повседневную жизнь, чем активнее она формирует правила доступа, режимы распространения сведений, порядок хранения данных, механизмы идентификации пользователей и процедуры реагирования на обращения государственных органов, тем очевиднее ее влияние на общую конфигурацию криминогенных рисков. Следовательно, вопрос должен ставиться не в плоскости абстрактного обвинения, а в плоскости четко сформулированных, юридически определенных и международно согласованных обязанностей по содействию пресечению организованной преступности при неукоснительном соблюдении законности и прав человека.

В конечном счете **главный вывод исследования** состоит в том, что борьба с организованной преступностью в цифровой среде не может ограничиваться реагированием на отдельные сообщения, отдельные учетные записи, отдельные эпизоды распространения запрещенного содержания или отдельные преступные действия. Подобный подход заведомо обречен на стратегическую недостаточность, поскольку он работает по периферии явления, не затрагивая его воспроизводящее ядро. Современная организованная преступность существует как целостная инфраструктура: она обладает каналами связи, системами вербовки, внутренним разделением труда, финансовыми маршрутами, правилами конспирации, дисциплинарными механизмами, логистикой, процедурами замещения утраченных участников и способами интеграции в повседневную цифровую среду. Пока государство борется лишь с видимыми фрагментами этой системы, сама система продолжает существовать, перестраиваться и возвращаться в новом обличье.

Отсюда следует, что **объектом противодействия должна стать именно инфраструктура преступного взаимодействия** - во всей совокупности ее организационных, коммуникационных, финансовых, правовых и социальных измерений. Необходимо выявлять центры координации, разрывать устойчивые каналы связи, блокировать механизмы воспроизводства кадрового состава, пресекать источники материального обеспечения, устранять условия безнаказанной маскировки под обычную цифровую активность и формировать такую правовую и

институциональную среду, в которой преступной сети будет невыгодно, трудно и опасно существовать. Лишь инфраструктурный подход позволяет перевести борьбу с преступностью из режима бесконечного догоняющего реагирования в режим системного ослабления ее жизнеспособности.

При этом чрезвычайно важно понимать, что **устойчивый результат возможен только при соединении силового, правового, аналитического и общественного измерений противодействия**. Силовое воздействие необходимо, когда требуется пресечь конкретную угрозу и изъять из обращения преступные ресурсы. Правовое воздействие необходимо для создания ясных правил ответственности, процедур доступа к значимым сведениям и пределов допустимого вмешательства. Аналитическое воздействие необходимо для понимания скрытой структуры преступной сети и прогнозирования ее дальнейшей эволюции. Наконец, общественное измерение необходимо потому, что любая преступная инфраструктура питается не только техническими возможностями, но и социальными слабостями: правовой неосведомленностью, экономической уязвимостью, деформацией ценностных ориентиров, терпимостью к теневым практикам, привычкой воспринимать цифровую среду как пространство безответственности. Там, где общество не вырабатывает внутреннего иммунитета к криминальной нормализации, государство неизбежно сталкивается с постоянным воспроизводством новых исполнителей и новых посредников.

Таким образом, современная организованная преступность, опирающаяся на цифровые коммуникационные площадки, представляет собой не временную аномалию и не частный технологический вызов, а одно из наиболее серьезных испытаний для правопорядка в XXI веке. **Ее сила - в скорости, гибкости, трансграничности и способности использовать повседневную цифровую среду как базовый ресурс собственного существования**. Следовательно, ответ государства и международного сообщества должен быть не менее системным, не менее быстрым и, главное, не менее целостным. Исторический опыт убедительно свидетельствует: преступность побеждает там, где закон отстает от реальности, где ведомства действуют разобщенно, где международное взаимодействие тонет в формальностях, а общество не осознает масштаба угрозы. Но этот же опыт показывает и другое: там, где государственная воля соединяется с научной ясностью, институциональной дисциплиной и стратегическим предвидением, даже самые сложные формы преступной организации могут быть последовательно лишены своей устойчивости.

Именно поэтому заключительный тезис должен звучать предельно определенно: **в цифровую эпоху защита правопорядка требует борьбы не с поверхностными проявлениями преступности, а с самой архитектурой ее сетевого существования**. Лишь такой подход отвечает подлинному масштабу вызова. Лишь он способен обеспечить не кратковременный, а

долговременный результат. И лишь он позволяет сохранить то, что составляет основу государственности и общественного мира: безопасность человека, устойчивость институтов, действенность закона и суверенное право государства защищать собственное правовое пространство от тех сил, которые стремятся превратить повседневную коммуникацию в орудие организованного криминального господства.