МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение
высшего образования
«Уфимский юридический институт Министерства внутренних дел
Российской Федерации»

Кафедра уголовного права и криминологии

ДИПЛОМНАЯ РАБОТА

на тему **«УГОЛОВНО-ПРАВОВЫЕ СРЕДСТВА ПРОТИВОДЕЙСТВИЯ НЕЗАКОННОМУ ОБОРОТУ НАРКОТИЧЕСКИХ СРЕДСТВ, ПСИХОТРОПНЫХ ВЕЩЕСТВ ИЛИ ИХ АНАЛОГОВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ (ПО МАТЕРИАЛАМ СУДЕБНОЙ ПРАКТИКИ)»**

Выполнил
Гатценбиллер Илья Андреевич
обучающийся по специальности
40.05.02 Правоохранительная деятельность
2021 года набора, 123 учебного взвода

Руководитель
доцент кафедры,
кандидант юридических наук
Гумерова Рамиля Рамилевна

К защите рекомендуется
рекомендуется / не рекомендуется
Начальник кафедры _____ И.Р. Диваева
подпись
Дата защиты «___» _____ 2026 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

Проблема незаконного оборота наркотических средств и психотропных веществ остается одной из наиболее острых угроз национальной безопасности, здоровью населения и общественному порядку. В последние десятилетия характер наркопреступности претерпел качественную трансформацию, обусловленную стремительным развитием цифровых технологий.

Современный наркорынок практически полностью переместился в виртуальное пространство. Использование теневого сегмента интернета (Darknet), мессенджеров с высокой степенью шифрования (например, Telegram), криптографических платежных систем и бесконтактных способов передачи («закладок») позволяет преступным сообществам сохранять высокий уровень анонимности. Дистанционный характер взаимодействия между продавцом и покупателем значительно затрудняет процесс выявления, документирования и доказывания преступной деятельности.

Несмотря на внесение изменений в Уголовный кодекс РФ (в частности, дополнение статьи 228.1 УК РФ квалифицирующим признаком – использование электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»), правоприменительная практика по-прежнему сталкивается с рядом проблем. К ним относятся сложности квалификации деяний, разграничение смежных составов преступлений, а также несовершенство механизмов международного взаимодействия при расследовании трансграничных киберпреступлений в сфере наркооборота. Необходимость комплексного анализа уголовно-правовых средств борьбы с «цифровой» наркопреступностью и выработки рекомендаций по совершенствованию законодательства определяет актуальность данной работы.

Целью работы является комплексное теоретико-прикладное исследование уголовно-правовых средств противодействия незаконному обороту наркотических средств и психотропных веществ, совершаемых с использованием информационных технологий, а также разработка научно

обоснованных предложений по совершенствованию норм уголовного законодательства и практики их применения.

Для достижения поставленной цели необходимо решить следующие задачи:

– изучить уголовно-правовой анализ незаконного оборота наркотических средств, психотропных веществ и их аналогов использованием информационно-телекоммуникационных технологий (далее – ИТТ);

– проанализировать специфику использования информационных технологий как способа совершения наркопреступлений;

– выявить проблемы квалификации незаконного оборота наркотиков, совершенного с использованием информационных технологий (далее – ИТ), в системе норм УК РФ;

– изучить судебную практику по делам о дистанционном сбыте наркотических средств (через сеть Интернет);

– раскрыть особенности применения уголовного закона при выявлении преступлений, совершенных с использованием информационных технологий;

– сформулировать предложения по совершенствованию уголовно-правовой нормы об ответственности за сбыт с использованием информационных технологий.

Объектом исследования являются общественные отношения, возникающие в сфере обеспечения здоровья населения и общественной нравственности, нарушаемые в результате незаконного оборота наркотических средств, психотропных веществ или их аналогов с применением информационных технологий.

Предметом исследования выступают нормы уголовного законодательства Российской Федерации, регулирующие ответственность за незаконный оборот наркотиков, международно-правовые акты, материалы судебной практики, статистические данные, а также научные труды в области уголовного права и криминологии по рассматриваемой проблематике.

Методологическую основу исследования составили общенаучные методы (анализ, синтез, дедукция, индукция) и частнонаучные методы познания: формально-юридический, сравнительно-правовой, статистический и метод анализа документов.

Научная новизна исследования заключается в попытке системного осмысления уголовно-правовых мер противодействия наркопреступности в условиях функционирования современных платформ анонимизации и распределенных реестров, а также в обосновании необходимости уточнения ряда дефиниций в уголовном законе.

Структура работы обусловлена целью и задачами исследования и включает в себя введение, две главы, разделенные на 6 параграфов, заключение и список использованной литературы.

ГЛАВА 1. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА НЕЗАКОННОГО ОБОРОТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Уголовно-правовой анализ незаконного оборота наркотических средств, психотропных веществ и их аналогов

Уголовно-правовая регламентация ответственности за незаконный оборот наркотических средств (далее – НС) и психотропных веществ (далее – ПВ), совершаемый с применением информационно-телекоммуникационных сетей (далее – ИТС), базируется на специфике объективных и субъективных признаков данных деяний. Ключевым элементом выступает п. «б» ч. 2 ст. 228.1 УК РФ[1], который выделяет использование электронных или ИТС, включая сеть «Интернет», в качестве квалифицирующего признака сбыта. Данный признак характеризует способ совершения преступления, который существенно повышает общественную опасность деяния за счет анонимности, трансграничности и возможности охвата неограниченного круга потенциальных потребителей.

Родовым объектом преступлений, связанных с незаконным оборотом наркотических средств, выступает совокупность общественных отношений, обеспечивающих общественную безопасность и общественный порядок. Видовой объект локализуется в сфере здоровья населения, под которым понимается состояние защищенности жизни и здоровья неопределенного круга лиц, а также сохранение генофонда и санитарно-эпидемиологическое благополучие общества.

Непосредственный объект преступления охватывает общественные отношения, обеспечивающие установленный государством порядок законного

[1] Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая. 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Рос. газ. 1996. 25 июня.

оборота наркотических средств, психотропных веществ, их прекурсоров или аналогов, а также растений, содержащих указанные компоненты. Данный порядок регламентирован императивными нормами федерального законодательства, исключающими неконтролируемое распределение и немедицинское потребление субстанций, вызывающих зависимость.

Использование информационно-телекоммуникационных сетей (включая сеть «Интернет») в качестве способа совершения деяния трансформирует характер угрозы защищаемому объекту. Цифровая среда расширяет пространственные границы посягательства, позволяя вовлекать в противоправный оборот неопределенное число субъектов и нивелируя эффективность традиционных мер государственного контроля. В квалифицированных составах, предусмотренных Уголовным кодексом РФ, использование IT-технологий выступает конструктивным или квалифицирующим признаком, повышающим степень общественной опасности деяния.

Предмет преступления является материальным выражением посягательства на объект и представлен веществами, включенными в Перечень наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации[1]. Химические характеристики, физическое состояние и правовой статус предмета определяют вектор воздействия на объект правовой охраны, при этом дистанционный способ передачи информации о местах хранения или способах приобретения веществ усиливает латентность посягательства.

В рамках уголовно-правовой доктрины объект рассматриваемого преступления остается неизменным вне зависимости от применяемого инструментария. Однако информационные технологии выступают катализатором деструктивного воздействия на здоровье населения, поскольку

[1] Об утверждении перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации [Электронный ресурс] : постановление Пленума Верховного Суда РФ от 30 июня 1998 № 681. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.10.2025).

анонимизация транзакций и использование криптографических протоколов создают условия для систематического нарушения установленного порядка оборота контролируемых средств в глобальном масштабе.

Объективная сторона характеризуется действиями по незаконному сбыту, под которым, согласно Постановлению Пленума Верховного Суда РФ № 14[1], понимаются любые способы их возмездной или безвозмездной передачи. Использование ИТС в данном процессе выполняет роль посреднического звена. Квалифицирующий признак «с использованием информационно-телекоммуникационных сетей» признается оконченным с момента совершения действий, направленных на передачу НС или ПВ лицу, использующему сеть. При этом фактическая передача товара может происходить позже. Специфика заключается в том, что информационная сеть используется для размещения предложений о продаже, согласования цены, места «закладки» или способа пересылки, а также для осуществления расчетов с применением криптовалют или электронных платежных систем.

Важным аспектом объективной стороны является момент окончания преступления при дистанционном способе продажи. Если лицо разместило информацию в сети, подготовило товар, но было задержано до момента сообщения покупателю координат тайника, деяние квалифицируется как покушение на сбыт по ч. 3 ст. 30 и соответствующей части ст. 228.1 УК РФ. Использование мессенджеров (например, Telegram, Signal) или теневых маркетплейсов для передачи геолокации и фотографий места размещения НС является юридически значимым действием, подтверждающим реализацию умысла на сбыт именно дистанционным способом.

Субъективная сторона характеризуется только прямым умыслом и целью сбыта. Виновный осознает, что использует ИТС для поиска покупателей или координации действий соучастников, и желает совершить продажу именно

[1] О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами [Электронный ресурс] : постановление Пленума Верховного Суда РФ от 15 июня 2006 № 14. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.10.2025).

таким образом. Мотив чаще всего корыстный, однако он не является обязательным для квалификации по статье 228.1 УК РФ. Особенности доказывания умысла при использовании ИТ-технологий связаны с анализом цифровых следов: логов серверов, переписки в мессенджерах, истории транзакций в блокчейн-сетях. Отсутствие прямого визуального контакта между продавцом и покупателем не исключает наличия умысла, если совокупность технических данных подтверждает направленность действий на распространение запрещенных веществ.

Субъект преступления общий – вменяемое физическое лицо, достигшее 16-летнего возраста. Однако в условиях цифровой среды субъектный состав часто представлен организованными группами или преступными сообществами с четким разделением ролей. В таких структурах выделяются «администраторы» (создатели интернет-магазинов), «операторы» (взаимодействующие с клиентами через сеть), «складмены» (оптовые курьеры) и «закладчики» (розничные сбытчики). Квалификация действий каждого соучастника требует установления их осведомленности об использовании ИТС для функционирования всей схемы. Если рядовой «закладчик» получает указания исключительно через мессенджер, его действия подпадают под квалифицированный признак использования сетей, даже если он лично не размещал объявления в интернете[1].

Применение ИТ-технологий влияет на разграничение составов. Например, пропаганда наркотиков в сети (ст. 6.13 КоАП РФ[2]) должна четко отграничиваться от склонения к потреблению НС с использованием ИТС (п. «д» ч. 2 ст. 230 УК РФ). Склонение предполагает активное воздействие на психику конкретного лица или группы лиц с целью возбуждения желания употребить наркотик. Использование интернета позволяет мультиплицировать это

---

[1] Алехин В.П., Мельник Н.А. Особенности уголовно-правового регулирования незаконного оборота наркотических средств, осуществляемого при помощи сети Интернет // Вестник экономики и права. 2020. № 38. С. 19.

[2] Кодекс Российской Федерации об административных правонарушениях: федер. закон Рос. Федерации от 30 декабря 2001 г. № 195-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 20 дек. 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 26 дек. 2001 г. // Рос. газ. 2001. 31 декабря.

воздействие, что обусловило выделение данного признака в качестве отягчающего в статье 230 УК РФ.

Проблематика квалификации аналогов НС и ПВ в цифровой среде сопряжена с быстротой обновления ассортимента в интернет-магазинах. Аналоги – это вещества, имеющие сходную химическую структуру и психоактивное действие, но не включенные в официальные списки. Для признания вещества аналогом в рамках уголовного дела требуется проведение судебно-химической и судебно-психиатрической экспертиз. Распространение информации о химических формулах в сети способствует появлению новых психоактивных веществ (НПВ), что требует от правоприменителя оперативной оценки действий лиц по ст. 234.1 УК РФ (оборот новых потенциально опасных психоактивных веществ), если вещество еще не включено в перечень НС и ПВ.

Квалифицирующий признак использования ИТС по п. «б» ч. 2 ст. 228.1 УК РФ поглощает действия по поиску покупателей, рекламе и согласованию условий сделки. Однако если использование сети интернет сопряжено с совершением иных преступлений (например, неправомерный доступ к компьютерной информации для сокрытия следов сбыта), требуется квалификация по совокупности со статьями главы 28 УК РФ. Не меньшей актуальностью обладает тема легализации (отмывания) денежных средств, полученных от цифрового наркосбыта, предусмотренное ст.ст. 174, 174.1 УК РФ. При этом в данной преступной деятельности использование криптоволютных бирж является составляющей.

Отдельного внимания требует доказывание квалифицирующего признака «группа лиц по предварительному сговору» или «организованная группа» в сочетании с ИТС. Технологии позволяют находиться соучастникам абсолютно в разных местах, что составляет проблему для правоохранительных органов для обнаружения состава преступления, предусмотренного ст. 210 УК РФ. Обратим внимание, что для этого требуется доказанность не только непосредственной связи через сеть Интернет, но и установление уровня отношений между участниками, то есть иерархичность.

Технологические способности посредством использования VPN, Tor, прокси-сервера позволяют модифицировать способ совершения преступления, тем самым ИТС выступает одновременно способом совершения преступления и инструмент, затрудняющий идентификацию лица, что обуславливает повышенную репрессивность норм: санкции за сбыт через сеть значительно выше, чем за «традиционный» сбыт без использования технических средств связи.

Взаимосвязь между цифровым способом связи и моментом перехода права владения наркотиком определяет различие между оконченным составом и приготовлением. Если лицо создало интернет-ресурс для продажи НС, но не успело приобрести сами вещества для реализации, деяние может быть квалифицировано как приготовление к сбыту (при условии крупного или особо крупного размера). Если же вещества приобретены и расфасованы, а информация о них размещена в сети – это покушение. Полная реализация алгоритма «заказ – оплата – получение координат – изъятие покупателем» (или сообщение координат покупателю) завершает состав оконченного преступления.

Анализ судебной практики показывает, что суды признают использованием ИТС даже единичную отправку сообщения в мессенджере с указанием места нахождения наркотика. Не требуется, чтобы вся цепочка сбыта была цифровизирована; достаточно использования сети на любом этапе реализации умысла на передачу вещества, что подчеркивает превентивную направленность уголовно-правовой нормы, стремящейся минимизировать использование любых технологических преимуществ преступниками.

Таким образом, уголовно-правовой анализ состава преступления, предусмотренного п. «б» ч. 2 ст. 228.1 УК РФ, позволяет сделать вывод о том, что информационно-телекоммуникационная сеть в данном случае выступает в качестве технического условия, трансформирующего объективную сторону данного состава преступления. Одновременно она вызывает сложность в идентификации субъекта преступления, поскольку анонимность создает дополнительные преграды в фиксации цифровых следов. Совершенствование

правоприменения требует признания цифровых данных (логов, транзакций, переписки) полноценными объектами уголовно-правовой оценки, а также уточнения момента окончания преступления при передаче информации о товаре без его физического перемещения в момент транзакции.

§ 2. Специфика использования информационных технологий как способа совершения наркопреступлений

Способ совершения преступления – это система приемов действий операциональных комплексов, обусловленных целью и мотивами действия, психическими и физическими особенностями действующего лица, в котором проявляются психофизиологические и характерологические особенности человека, его знания, умения, навыки, привычки и отношение к различным сторонам действительности. Для каждого преступления существует свой системный «набор», комплекс действий и операций.

Н.П Яблоков считает, что способ совершения преступления представляет любую «объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющую различного рода характерные следы вовне, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и, соответственно, определить наиболее оптимальные методы решения задач раскрытия преступления»[1].

Таким образом, под способом совершения преступления мы понимаем действия или систему действий, направленные на по подготовку, совершение и сокрытие преступлений, обусловленные внешней средой и психофизиологическими свойствами личности.

---

[1] Яблоков Н.П. Криминалистика: учебник / Н.П. Яблоков. 3-е изд., М.: Юристъ, 2005. С. 120.

Специфика, рассматриваемого способа обусловлена в первую очередь, использованием информационных технологий, в связи с чем возникает необходимость уяснить, что же под ними понимается.

Согласно в п. 2, ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ сказано, что информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Цель информационной технологии – производство информации для ее анализа человеком и принятия на его основе решения по выполнению какого-либо действия. Указанные информационные технологии при совершении преступлений в сфере незаконного оборота наркотиков могут использовать любой из участников преступной группы.

Трансформация традиционных методов распространения наркотических средств и психотропных веществ (НС и ПВ) в цифровую плоскость обусловлена интеграцией высокотехнологичных инструментов, обеспечивающих анонимность, масштабируемость и минимизацию физических контактов между субъектами преступной деятельности. Преступные онлайн-сообщества опираются на сложные технологии анонимизации, такие как I2P и Tor. Принцип их работы основан на перенаправлении трафика через множество случайных узлов с каскадным шифрованием, что делает невозможным отслеживание реального местоположения сервера или пользователя. Такие теневые площадки устроены довольно технологично: они включают автоматизированные системы расчетов, встроенные службы арбитража и депонирование средств (Escrow), что выводит криминальный сервис на уровень легальных маркетплейсов.

Взаимодействие между участниками преступных групп строится на криптографической защите. Использование PGP-шифрования стало стандартом для передачи чувствительных данных, например, локаций «закладок», что исключает риск утечки при перехвате трафика. Параллельно с этим злоумышленники активно эксплуатируют мессенджеры с E2EE-протоколами и

режимами самоудаления переписки. В результате доказательная база становится труднодоступной: даже при наличии специализированных криминалистических комплексов для взлома смартфонов (Cellebrite и аналоги), следствие часто сталкивается с невозможностью извлечения данных из-за полнодискового шифрования или скрытых разделов, созданных в таких программах, как VeraCrypt.

В сфере наркобизнеса расчеты давно перешли в цифровую плоскость, полностью исключив использование классических фиатных денег. Основным инструментом здесь выступают криптовалюты (Bitcoin, Ethereum, Dash), а в последнее время – активы с повышенным уровнем анонимности, такие как Monero. Преступники отдают предпочтение XMR из-за встроенных криптографических методов защиты: кольцевые подписи и технология «скрытых адресов» делают отслеживание отправителя, получателя и суммы платежа через публичные реестры блокчейна практически невыполнимой задачей.

Чтобы еще сильнее запутать следы, участники сделок прибегают к услугам криптовалютных миксеров. Эти сервисы «размывают» историю происхождения средств, перемешивая активы множества пользователей, что нивелирует эффективность таких инструментов киберразведки, как Chainalysis или Crystal Blockchain. Современные даркнет-площадки максимально упростили этот процесс: они интегрируют API бирж напрямую в свои системы. В итоге, как только сеть подтверждает транзакцию, маркетплейс автоматически выдает покупателю геолокацию тайника – человеческий фактор здесь сведен к минимуму.

Параллельно трансформировалась и логистика сбыта, перейдя на модель «бесконтактного» взаимодействия. В ее основе лежат геоинформационные технологии и спутниковое позиционирование. Весь процесс передачи товара теперь расщеплен на два этапа: виртуальный и материальный. На первом этапе курьер («закладчик») создает своего рода цифровое досье. В него входят точные географические координаты (фиксируемые с высокой погрешностью, буквально

до миллиметров), детальные снимки места с нанесенными графическими подсказками и сопутствующие текстовые инструкции.

Важной технической деталью является использование специализированных камер и приложений, которые автоматически вшивают в метаданные изображения (EXIF) GPS-координаты и временные метки. Передача этого цифрового пакета через ИТС квалифицируется как покушение на сбыт или оконченный сбыт в зависимости от момента получения доступа к информации конечным потребителем. Использование ботов в мессенджере Telegram, написанных на Python с использованием библиотек aiogram или telebot, позволяет полностью автоматизировать процесс распределения адресов, исключая участие человека на этапе розничной продажи.

Организационная структура наркопреступности в цифровой среде характеризуется высокой степенью фрагментации и распределенности. Использование ИТС позволяет формировать преступные сообщества, участники которых могут находиться в разных юрисдикциях, никогда не встречаться лично и не знать настоящих анкетных данных друг друга. Взаимодействие осуществляется через защищенные каналы связи с использованием псевдонимов. Иерархия включает в себя роли администраторов (владельцев ресурса), операторов (техническая поддержка и связь с клиентами), кадровиков (рекрутинг новых участников через социальные сети и форумы), химиков (производителей), перевозчиков и розничных курьеров. Специфика здесь заключается в использовании методов социальной инженерии для вербовки несовершеннолетних через игровые платформы или мессенджеры, где обещание «легкого заработка» маскируется под легальную курьерскую деятельность. Особую сложность представляет атрибуция цифрового профиля конкретному физическому лицу. Преступники используют виртуальные машины (VirtualBox, VMware), операционные системы, работающие в режиме «live» с внешних носителей (Tails, Whonix), что минимизирует количество следов на жестком диске. Технология Anti-Forensics (стирание метаданных, использование шредер-

программ для безвозвратного удаления файлов) является стандартным протоколом безопасности в современных наркошопах.

Юридическая квалификация деяний, совершенных с использованием ИТС, требует учета положений п. «б» ч. 2 ст. 228.1 УК РФ. Использование информационных сетей здесь выступает не просто как средство связи, а как неотъемлемый элемент способа совершения преступления, расширяющий пространственные границы деяния. Специфика проявляется в том, что момент окончания преступления может быть дистанцирован во времени и пространстве от момента физического размещения наркотика в тайнике. Если информация о месте закладки размещена на сервере автопродаж, но еще не куплена, деяние характеризуется как создание условий для совершения преступления. Использование ИТ-технологий также облегчает совершение сопутствующих преступлений, таких как вовлечение несовершеннолетних в совершение преступления (ст. 150 УК РФ) через игровые чаты или пропаганда наркотиков (ст. 6.13 КоАП РФ) в социальных сетях.

Технологический стек наркопреступности постоянно эволюционирует, включая в себя элементы искусственного интеллекта. Современные преступные сообщества активно внедряют нейросетевые алгоритмы для оптимизации своей деятельности. Искусственный интеллект стал незаменим в создании правдоподобных легенд для фейковых аккаунтов, написании качественных описаний «товаров» и мониторинге тематических форумов для отслеживания интереса со стороны силовых структур. Чтобы скрыть следы в сети, злоумышленники выстраивают сложную систему защиты: они объединяют цепочки VPN-туннелей, проходящих через разные государства, с протоколами прокси (в частности, SOCKS5). Подобная многослойная архитектура делает попытки деанонимизации практически бессмысленными. Главная сложность для следствия здесь кроется в географической разобщенности участников: преступная инфраструктура может быть раскидана по всему миру – от европейских хостингов до администраторов в Юго-Восточной Азии и непосредственных исполнителей в России. Такая трансграничность серьезно

тормозит расследование, так как получение цифровых доказательств требует долгих бюрократических процедур международного обмена правовой помощью.

Особый интерес представляет финансовая сторона, построенная на базе P2P-сделок. В этой схеме ключевую роль играют «дропы» – подставные лица, предоставляющие свои банковские карты или кошельки (например, популярных платежных систем) для транзита денег. Фактически же доступ к этим финансам осуществляется удаленно, через RDP-соединения или специально подготовленные мобильные устройства. Информационно-телекоммуникационные системы здесь выступают в роли бухгалтера: боты-координаторы берут на себя рутину по распределению прибыли. Как только сделка по продаже наркотиков закрывается, система мгновенно конвертирует активы и раскидывает «зарплату» по кошелькам участников преступной цепочки в автоматическом режиме, исключая ручное управление.

Специфика использования ИТ проявляется и в методах контрнаблюдения. Использование дронов (БПЛА) для проверки отсутствия засад в местах оптовых закладок, установка скрытых IP-камер с облачным хранением данных для мониторинга работы курьеров, использование специализированного ПО для обнаружения «маячков» и трекеров в упаковках с товаром – всё это свидетельствует о высокой технологической оснащенности современной наркопреступности. Цифровая среда позволяет проводить обучение «персонала» через закрытые вебинары, распространять инструкции по технике безопасности и методам уклонения от следствия в формате зашифрованных PDF-файлов[1].

При совершении преступлений по статье 229.1 УК РФ (контрабанда НС) ИТ-технологии используются для отслеживания почтовых отправлений через международные трекинг-сервисы. Заказ товара осуществляется на теневых форумах у зарубежных поставщиков, оплата производится в криптовалюте, а коммуникация ведется через почтовые сервисы с повышенным уровнем

[1] Третьякова Е. И. Информационные технологии в механизме преступлений, связанных с незаконным оборотом наркотических средств // Криминалистика: вчера, сегодня, завтра. 2022. № 3(23). С. 145.

приватности (например, ProtonMail). Специфика заключается в том, что отправитель и получатель могут использовать подставные данные («дроп-адреса»), а управление логистикой осуществляется через зашифрованные мессенджеры, что делает физический перехват посылки лишь начальным этапом в сложной цепочке установления организаторов.

Информационные технологии позволяют реализовывать схемы «мультисбыта», когда одна и та же партия товара предлагается на разных площадках одновременно, а автоматизированная система управления запасами (Inventory Management System) обновляет остатки в режиме реального времени. Это роднит наркобизнес с легальным e-commerce, заимствуя у него методы анализа рынка, таргетированной рекламы и систем лояльности (скидки, бонусы за отзывы, реферальные программы). Специфика здесь в том, что цифровая платформа становится саморегулируемой экосистемой, способной функционировать даже после задержания отдельных её участников.

Квалификация использования ИТС как способа совершения преступления требует от следствия не только юридической грамотности, но и глубоких знаний в области сетевых протоколов, криптографии и функционирования блокчейн-сетей. Отсутствие единого реестра цифровых адресов и возможность мгновенного уничтожения доказательств путем удаленной команды на очистку памяти (Remote Wipe) определяют высокую латентность данных преступлений. Специфика совершения наркопреступлений в цифровую эпоху – это симбиоз криминального умысла и передовых достижений информатики, где виртуальное пространство выступает идеальной средой для анонимной и высокодоходной противоправной деятельности.

Специфика использования информационных технологий в наркопреступности заключается в создании комплексной цифровой инфраструктуры, которая обеспечивает полную анонимность транзакций, автоматизацию процесса сбыта и географическую распределенность участников. Использование Darknet, криптовалют и зашифрованных мессенджеров трансформирует объективную сторону состава преступления, делая его

дистанционным и высокотехнологичным. Основная проблема противодействия таким деяниям кроется в разрыве между физическим актом сбыта и его цифровым сопровождением, что требует изменения подходов к доказыванию, признания цифровых метаданных ключевыми уликами и совершенствования методик деанонимизации субъектов в зашифрованных сетях. Уголовно-правовое значение ИТС как способа совершения преступления заключается в его способности многократно увеличивать общественную опасность содеянного за счет вовлечения неограниченного круга лиц и создания устойчивых, неуязвимых для традиционных методов расследования криминальных структур.

Таким образом, в доктрине уголовного права применение IT-технологий при совершении деяний, предусмотренных статьей 228.1 УК РФ, обоснованно выделено в качестве квалифицирующего признака. Способ совершения в данном случае выступает катализатором общественной опасности, поскольку цифровые инструменты позволяют масштабировать противоправное воздействие на неограниченный круг лиц, включая наиболее уязвимые социальные группы, и нивелируют эффективность традиционных мер пограничного и таможенного контроля.

Процессуальная специфика расследования наркопреступлений, совершаемых с использованием сетевых технологий, требует переориентации доказательственной базы с вещественных источников на цифровые следы. Основу обвинения начинают составлять результаты анализа IP-адресов, данных биллинга, логов серверов и криптографических транзакций. Эффективное противодействие данной категории посягательств невозможно без имплементации в следственную практику механизмов деанонимизации пользователей и расширения межгосударственного взаимодействия в сфере оборота электронных доказательств.

§ 3. Проблемы квалификации незаконного оборота наркотиков, совершенного с использованием ИТ, в системе норм УК РФ

Проблемы квалификации незаконного оборота наркотических средств, психотропных веществ или их аналогов, совершаемого с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»), обусловлены стремительной цифровизацией преступной деятельности и несовершенством понятийного аппарата уголовного закона. Ключевая сложность заключается в интерпретации квалифицирующего признака, предусмотренного пунктом «б» части 2 статьи 228.1 УК РФ. Законодатель не дает исчерпывающего перечня действий, составляющих «использование» ИТС, что порождает правовую неопределенность при разграничении обычного сбыта и сбыта с применением высоких технологий. В судебной практике возникают споры о том, является ли использование мессенджеров исключительно для связи между соучастниками достаточным основанием для вменения данного признака, или же ИТС должны выступать непосредственным инструментом поиска покупателей и витриной товара.

Трансформация объективной стороны сбыта НС и ПВ в цифровой среде требует переосмысления момента окончания преступления. Согласно Постановлению Пленума Верховного Суда РФ № 14, сбыт считается оконченным с момента выполнения всех действий по передаче товара. Однако в условиях бесконтактного способа реализации, опосредованного ИТС, возникает временной и пространственный разрыв между размещением наркотика в тайнике и получением координат покупателем. Проблема квалификации здесь связана с определением статуса действий «закладчика», который загрузил данные о месте нахождения вещества в автоматизированную систему (бот), но покупка еще не совершена. Квалификация таких действий как оконченного состава (через призму «создания условий для получения доступа») вступает в противоречие с традиционным пониманием передачи предмета преступления, что зачастую приводит к неоправданному расширению сферы применения статьи 228.1 УК РФ.

Сложность представляет разграничение приготовления к сбыту, покушения на сбыт и оконченного преступления при обнаружении «оптовых

закладок», информация о которых еще не была передана через ИТС конечным потребителям. Если лицо администрирует интернет-магазин и хранит партию НС для последующей реализации, техническое использование ИТС (настройка сайта, создание карточек товаров) уже началось, но физическое перемещение вещества отсутствует. В таких случаях следственные органы сталкиваются с проблемой доказывания умысла именно на использование ИТС для сбыта конкретной партии, а не простого хранения. Отсутствие в законе четкой корреляции между цифровыми следами (логи, переписка) и материальными объектами (пакеты с веществом) затрудняет точную квалификацию по части 3 статьи 30 и соответствующей части статьи 228.1 УК РФ.

Квалификация соучастия в наркопреступлениях, совершаемых с использованием ИТ, сталкивается с проблемой определения формы соучастия. Групповой характер такой деятельности часто подпадает под признаки организованной группы (часть 4 статьи 228.1 УК РФ) или преступного сообщества (статья 210 УК РФ). Однако цифровая анонимность и отсутствие личного контакта между «оператором», «складменом» и «курьером» затрудняют доказывание признака устойчивости и сплоченности. Проблема заключается в том, что участники могут не осознавать своей принадлежности к единой структуре, взаимодействуя только с программным интерфейсом или анонимным аккаунтом. Это порождает коллизии при вменении статьи 210 УК РФ, так как традиционные критерии структурированности и иерархичности в децентрализованных Darknet-сообществах приобретают специфические формы, не всегда укладывающиеся в сложившиеся доктринальные представления.

Проблема субъективной стороны преступления при использовании ИТ связана с установлением прямого умысла на использование именно ИТС[1]. В ряде случаев подсудимые заявляют, что использование мессенджера было случайным или вынужденным, а не направленным на расширение аудитории сбыта.

[1] Самолаева Е.Ю. Проблемы квалификации сбыта наркотических средств и психотропных веществ, совершенных с использованием информационно-телекоммуникационной сети «Интернет» // Эпоха науки. 2017. № 11. С. 79.

Квалификация по пункту «б» части 2 статьи 228.1 УК РФ требует доказательства того, что информационная сеть использовалась как средство повышения эффективности преступной деятельности, облегчения доступа к неограниченному кругу лиц или обеспечения анонимности. Недостаточная проработка критериев «использования» в законе позволяет защите оспаривать данный признак, указывая на отсутствие влияния технологий на общественную опасность конкретного акта передачи наркотика.

Использование криптовалют (Bitcoin, Monero, Ethereum) в качестве платежного средства за наркотики создает дополнительные проблемы квалификации по статьям 174 и 174.1 УК РФ (легализация преступных доходов). Судебная практика долгое время не имела единого подхода к признанию преобразования криптовалюты в фиатные деньги актом легализации. Основная сложность заключается в определении момента, когда транзакция в блокчейне превращается в действие, направленное на придание правомерного вида владению средствами. Квалификация совокупности сбыта и легализации требует доказывания цели придания легального статуса, что в условиях использования криптомиксеров и анонимных кошельков технически затруднено. Часто суды ограничиваются квалификацией только по статье 228.1 УК РФ, игнорируя финансовую составляющую, что искажает реальный масштаб преступной деятельности.

Проблемы территориальной подсудности и места совершения преступления напрямую влияют на квалификацию и расследование. При использовании ИТС местом совершения преступления может считаться место нахождения сервера, место нахождения администратора или место физического размещения наркотика. В условиях, когда управление интернет-магазином осуществляется из одной юрисдикции, сервер находится в другой, а сбыт происходит в третьей, возникают конфликты квалификации по признаку места совершения деяния.

Действия лиц, обеспечивающие функционирование технических площадок, квалифицировать проблематично, вызывает много дискуссионных

моментов. Анализ практической деятельности показывает, что данные лица привлекаются к уголовной ответственности по ч. 5 ст. 33 и ст. 228.1 УК РФ, то есть пособничество в сбыт. Однако следует обратить внимание, если действия указанных лиц включают создание специализированных программных обеспечений, то возникает вопрос о квалификации действий по главе 28 УК РФ (преступления в сфере компьютерной информации). Возникает конкуренция правовых норм, которая не разрешена законодателем, требует проработки, поскольку результатом выступает неоднородность судебных решений.

Особую категорию проблем составляет квалификация склонения к потреблению НС и ПВ (статья 230 УК РФ) с использованием ИТС. Цифровая среда позволяет осуществлять пропаганду и склонение через социальные сети, таргетированную рекламу и скрытый маркетинг в игровых сообществах. Сложность заключается в разграничении состава статьи 230 УК РФ и пропаганды наркотиков (статья 6.13 КоАП РФ). Уголовно-правовая квалификация требует установления умысла на возбуждение желания употребить наркотик у конкретного лица или группы лиц, что в условиях массовых рассылок или публикации контента в открытых группах доказать крайне сложно. Отсутствие четких критериев «склонения» в цифровом пространстве ведет к тому, что общественно опасные деяния остаются в плоскости административных правонарушений.

Проблема квалификации по весу (размеру) наркотического средства при серийном сбыте через ИТС связана с принципом сложения партий. В условиях работы интернет-магазина курьер может совершить десятки закладок малого размера за один выход. Квалификация таких действий как одного продолжаемого преступления в крупном размере или как множества самостоятельных эпизодов в значительном размере зависит от доказанности единого умысла. Использование ИТС, где заказы обрабатываются дискретно, часто подталкивает следствие к дроблению эпизодов, что не всегда отражает реальную направленность умысла сбытчика на реализацию всей имеющейся у него массы вещества.

Квалификация контрабанды НС (статья 229.1 УК РФ), совершенной через ИТС, осложняется использованием международных почтовых отправлений и курьерских служб, где заказ оформляется анонимно[1]. Проблема заключается в определении момента пересечения таможенной границы и установлении лица, ответственного за перемещение, если заказ был сделан через автоматизированный скрипт. Часто возникают ситуации «подставных получателей», когда лицо, принимающее посылку, не осведомлено о её содержимом. Квалификация действий организатора, находящегося в другой стране и использующего ИТС для координации всей цепочки, требует применения норм о дистанционном соисполнительстве, что технически затруднено отсутствием физических доказательств связи.

Существуют проблемы квалификации при использовании ИТС для хищения либо вымогательства НС (статья 229 УК РФ). Речь идет о так называемых «чайках» (лицах, похищающих чужие закладки путем взлома баз данных магазинов или поиска по координатам) и «хакерах», атакующих кошельки наркошопов. Квалификация таких деяний как хищения наркотиков сталкивается с вопросом о законности владения предметом хищения. Поскольку наркотики изъяты из гражданского оборота, их похищение у сбытчика через ИТС создает парадоксальную ситуацию, где объектом посягательства является неправомерное владение. Это требует уточнения квалификации действий лиц, использующих ИТ для перераспределения запрещенных веществ внутри теневого рынка.

Проблемы квалификации также затрагивают стадию окончания преступления при передаче НС через тайники-закладки, когда покупатель не находит товар («ненаход»). Существующий правоприменительный подход к данному вопросу характеризуется отсутствием единообразия: дискуссионным остается вопрос, следует ли считать подобные действия завершенным

[1] Хромов Е. В. Проблемы квалификации сбыта наркотических средств, психотропных веществ или их аналогов с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») // Криминалистъ. 2021. № 3(36). С. 32.

преступлением (аргументируя это тем, что продавец полностью исполнил обязательства, передав данные через инфокоммуникационные сети) или же квалифицировать их как покушение (исходя из того, что физический контроль над предметом преступления покупателем фактически не был получен). Применение ИТС в качестве канала для передачи сведений о локации «закладки» превращает данную сложность в системную проблему, так как любые неполадки в работе государственных или частных систем, равно как и умышленные манипуляции со стороны наркокурьера, оказывают прямое воздействие на итоговую юридическую оценку деяния.

Взаимодействие положений уголовного законодательства, регулирующих оборот наркотических средств, с нормами, направленными на защиту общественной безопасности (в частности, ст. 205.2 и 208 УК РФ), при задействовании современных технологий прослеживается в механизмах финансирования террористической деятельности за счет прибыли от незаконного оборота наркотиков. Квалификация подобных многообъектных составов преступлений невозможна без детального доказывания причинно-следственной связи между цифровыми платежами за запрещенные вещества и их последующим использованием для обеспечения экстремистских целей. Трудность заключается в прослеживании всей цепочки перераспределения криптоактивов, что часто приводит к упрощенной квалификации только по «наркотическим» статьям, оставляя без внимания более тяжкие составы преступлений против безопасности государства.

Проблемы квалификации незаконного оборота наркотиков с использованием ИТ в системе норм УК РФ коренятся в дихотомии между материальной природой предмета преступления и виртуальным способом его реализации. Основные сложности сосредоточены вокруг неопределенности момента окончания сбыта при бесконтактном способе, трудностей в доказывании организованных форм соучастия в анонимных сетях и конкуренции норм при квалификации использования криптовалют и специализированного ПО. Для преодоления указанных проблем необходимо на уровне Пленума

Верховного Суда РФ детализировать понятие «использование информационно-телекоммуникационных сетей», признав его не только средством связи, но и способом совершения преступления, обеспечивающим доступ к товару. Также требуется совершенствование норм о легализации преступных доходов и компьютерных преступлениях для обеспечения комплексной квалификации всех аспектов цифровой наркоторговли, включая её финансовую и технологическую инфраструктуру. Только системная интеграция цифровых доказательств в материально-правовые рамки позволит обеспечить единообразие судебной практики и адекватность уголовно-правовой оценки современных форм наркопреступности.

ГЛАВА 2. АНАЛИЗ СУДЕБНОЙ ПРАКТИКИ ПРИМЕНЕНИЯ УГОЛОВНО-ПРАВОВЫХ НОРМ К ПРЕСТУПЛЕНИЯМ, СВЯЗАННЫМ С НЕЗАКОННЫМ ОБОРОТОМ НАРКОТИКОВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Судебная практика по делам о дистанционном сбыте наркотических средств (через сеть Интернет)

Судебная практика по делам о дистанционном сбыте наркотических средств через информационно-телекоммуникационные сети основывается на положениях статьи 228.1 УК РФ и разъяснениях Пленума Верховного Суда РФ № 14. Основной вектор правоприменения направлен на квалификацию действий виновных лиц как оконченного преступления или покушения в зависимости от момента передачи информации о месте нахождения наркотика. Суды исходят из того, что при бесконтактном способе реализации решающее значение имеет выполнение продавцом всех обязательств по доведению товара до потребителя. Если наркотическое средство размещено в тайнике («закладке»), а его координаты, фотографии и описание переданы покупателю или оператору интернет-магазина для последующей перепродажи, деяние квалифицируется как оконченный сбыт. В случаях, когда правоохранительные органы изымают вещество из тайника до момента передачи данных о его локализации конечному потребителю, суды классифицируют действия как покушение на сбыт по части 3 статьи 30 и соответствующей части статьи 228.1 УК РФ.

Квалификация по пункту «б» части 2 статьи 228.1 УК РФ требует доказанности факта использования сети Интернет именно для совершения операций по реализации. Судебная практика относит к таким действиям размещение объявлений на торговых площадках Darknet, использование мессенджеров Telegram, VIPole, Signal для общения с покупателями, применение автоматизированных ботов для приема оплаты и выдачи адресов. Суды отклоняют доводы защиты о том, что использование интернета носило

вспомогательный характер, если установлено, что без цифровых каналов связи совершение преступления в выбранной форме было бы невозможным. При этом суды учитывают, что для вменения данного признака не обязательно наличие прямого контакта между продавцом и покупателем в сети, достаточно подтверждения факта передачи информации через сетевые протоколы.

Важным аспектом судебного разбирательства является оценка доказательств, полученных в ходе исследования электронных носителей информации. В современной судебной практике протоколы осмотра цифровых устройств – от смартфонов до стационарных ПК – признаются надлежащими доказательствами, если они включают в себя переписку, файлы с геопозиционированием и фотофиксацию участков местности с отметками тайников. Ключевым этапом оценки таких доказательств является перекрестный анализ тайминга создания файлов и метаданных изображений с логированием сетевой активности обвиняемого. В ситуациях, когда фигуранты применяют средства шифрования или программное обеспечение для очистки метаданных, суды опираются на выводы экспертов-криминалистов, специализирующихся в области компьютерно-технических исследований. Экспертиза в таких случаях направлена на восстановление деструктивной информации либо на подтверждение факта эксплуатации специализированного софта, предназначенного для сокрытия следов пребывания в сети.

При рассмотрении дел в отношении «закладчиков», у которых изъяты значительные объемы наркотических средств, сформировалась устойчивая судебная позиция по разграничению понятий хранения и сбыта. Обнаружение сопутствующих атрибутов преступной деятельности – измерительного оборудования, расходных материалов (изоленты, фасовочных пакетов), элементов крепления (магнитов), а также выявление в памяти мобильных устройств адресов уже размещенных закладок – трактуется судами как бесспорное доказательство наличия умысла на последующую реализацию наркотиков.

Версия о хранении для личного употребления в таких случаях признается несостоятельной, даже если подсудимый сам страдает наркотической зависимостью. Суды указывают, что фасовка вещества на мелкие дозы и наличие распределенной сети тайников объективно подтверждают цель реализации.

Судебная практика по делам о дистанционном сбыте наркотических средств через информационно-телекоммуникационные сети основывается на положениях статьи 228.1 УК РФ и разъяснениях Пленума Верховного Суда РФ № 14. Основной вектор правоприменения направлен на квалификацию действий виновных лиц как оконченного преступления или покушения в зависимости от момента передачи информации о месте нахождения наркотика. Суды исходят из того, что при бесконтактном способе реализации решающее значение имеет выполнение продавцом всех обязательств по доведению товара до потребителя. Если наркотическое средство размещено в тайнике («закладке»), а его координаты, фотографии и описание переданы покупателю или оператору интернет-магазина для последующей перепродажи, деяние квалифицируется как оконченный сбыт. В случаях, когда правоохранительные органы изымают вещество из тайника до момента передачи данных о его локализации конечному потребителю, суды классифицируют действия как покушение на сбыт по части 3 статьи 30 и соответствующей части статьи 228.1 УК РФ.

Квалификация по пункту «б» части 2 статьи 228.1 УК РФ требует доказанности факта использования сети Интернет именно для совершения операций по реализации. При осуществлении правоприменительной деятельности квалификация действий как совершенных с использованием электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») опирается на конкретные фактические обстоятельства. Судебная практика исходит из того, что создание товарных позиций на площадках теневого сегмента, эксплуатация мессенджеров (таких как Telegram, VIPole, Signal) для коммуникации с клиентами, а также внедрение автоматизированных программных решений (ботов) для проведения транзакций и трансляции координат тайников являются достаточным основанием для инкриминирования

данного признака. Судебная практика показывает, что попытки адвокатов преуменьшить значение цифровых технологий в совершении преступления практически всегда терпят неудачу. Если следствие убедительно доказывает, что без задействования IT-инструментов реализовать задуманную схему было бы невозможно, суды не принимают доводы защиты о «второстепенной» роли интернет-коммуникаций. Ключевым моментом здесь становится не столько факт личного общения преступников, сколько сам процесс передачи данных через сетевые протоколы.

В судебных разбирательствах основное внимание приковано к цифровым следам. Электронные носители информации — смартфоны и компьютеры — выступают главными источниками доказательств. Вердикты базируются на данных, полученных при осмотре такой техники: следствие изучает историю переписки, изучает метаданные (включая геолокацию) и анализирует фотоотчеты, которые преступники делали для маркировки «закладок» с наркотиками.

Когда данных в открытом виде недостаточно, суд прибегает к сопоставлению фактов: например, сверяет время создания файлов с тем, когда именно подсудимый был онлайн. Если злоумышленники пытались замести следы – использовали шифрование или удаляли метаданные, – решающее слово остается за экспертами. Специалисты в области компьютерно-технической экспертизы восстанавливают стертые файлы или подтверждают, что обвиняемый целенаправленно применял софт для маскировки своей деятельности. Именно эти заключения ложатся в основу обвинительного приговора. Судебная практика выработала жесткий подход к разграничению хранения наркотиков и их сбыта при обнаружении крупных партий у «закладчиков». Наличие весов, упаковочного материала (зип-локов, изоленты), магнитов, а также обнаружение в мобильном устройстве адресов уже сделанных закладок интерпретируется судами как однозначное свидетельство умысла на сбыт. Версия о хранении для личного употребления в таких случаях признается несостоятельной, даже если подсудимый сам страдает наркотической

зависимостью. Суды указывают, что фасовка вещества на мелкие дозы и наличие распределенной сети тайников объективно подтверждают цель реализации.

Применение статьи 210 УК РФ (организация преступного сообщества) в делах о дистанционном сбыте через интернет-магазины требует от судов детального анализа структуры организации. Судебная практика выделяет такие роли, как «организатор», «оператор», «склад», «перевозчик», «курьер-закладчик», «трафаретчик». Для квалификации по статье 210 УК РФ суды ищут доказательства стабильности связей, распределения прибыли, наличия системы штрафов и поощрений внутри магазина, а также мер по обеспечению внутренней безопасности (проверка курьеров через залоги или паспортные данные). Отсутствие физического знакомства между участниками цепочки, характерное для цифрового сбыта, не препятствует признанию их членами преступного сообщества, если доказано их осознанное участие в едином технологическом процессе распределения наркотиков.

Проблематика использования криптовалют как средства платежа в судебной практике решается через признание транзакций в Bitcoin, Monero, Litecoin формой оплаты товара. Суды принимают в качестве доказательств выписки из криптокошельков, данные с бирж и обменных сервисов. Если следствию удается доказать цепочку конвертации криптовалюты в фиатные деньги на банковские карты подсудимых или их родственников, действия дополнительно квалифицируются по статье 174.1 УК РФ (легализация денежных средств). Суды подчеркивают, что использование миксеров и анонимных кошельков свидетельствует о профессиональном характере деятельности и умысле на сокрытие преступных доходов.

Особое место в практике занимают дела, связанные с «контрольной закупкой» в цифровой среде. При оценке правомерности оперативно-розыскных мероприятий (ОРМ) арбитры тщательно исследуют вопрос об отсутствии провокации со стороны правоохранительных органов. Основанием для признания доказательств допустимыми служит подтверждение того, что преступный умысел возник у подозреваемого самостоятельно, а не под

воздействием полицейских, и что площадка для сбыта функционировала еще до начала оперативной разработки. Ключевым критерием является наличие у следствия обоснованных сведений о причастности гражданина к незаконному обороту еще до начала активных действий. В делах, связанных с дистанционными продажами, такие данные обычно подтверждаются результатами анализа почтовых отправлений, отслеживанием активности подозрительных профилей или же протоколами допросов лиц, уже привлеченных к ответственности, которые сообщили сведения о конкретном сетевом ресурсе.

В вопросах квалификации объема наркотических средств (определение значительного, крупного или особо крупного размера) при дистанционном способе совершения преступления суды исходят из суммарной массы изъятых веществ, если следствием доказана неразрывная связь между ними и единый преступный план. Например, если курьер-закладчик разместил двадцать отдельных упаковок весом по одному грамму каждая, правоприменитель рассматривает это как единое деяние по сбыту двадцати граммов вещества, а не как совокупность двадцати разрозненных эпизодов, что существенно влияет на тяжесть наказания, переводя деяние в категорию тяжких или особо тяжких преступлений. При этом суды учитывают возможность квалификации через часть 3 статьи 30 УК РФ для тех закладок, информация о которых еще не была передана в «центр» управления магазином.

Использование VPN-сервисов, браузера Tor и прокси-серверов рассматривается судами как обстоятельство, подтверждающее повышенную общественную опасность и стремление виновного избежать ответственности. Хотя формально это не является отягчающим обстоятельством по статье 63 УК РФ, суды учитывают это при назначении наказания в рамках санкции статьи, выбирая более строгие меры. Техническая грамотность подсудимого и использование методов криптографии трактуются как свидетельство глубокой интеграции в преступную деятельность.

В вопросах подсудности суды придерживаются правила о месте совершения основного объема действий. При дистанционном сбыте местом окончания преступления может признаваться как место нахождения сервера, так и место физического размещения наркотика или место нахождения лица, отправившего данные о тайнике. Чаще всего дела рассматриваются по месту обнаружения наркотических средств в тайниках, так как это является материальным последствием преступления. В случае транснациональных групп, где серверы находятся за рубежом, суды опираются на факт наступления последствий на территории РФ.

Судебная практика по делам о сбыте через почтовые отправления (даркнет-посылки) фокусируется на моменте перехода права владения. Сбыт признается оконченным в момент отправки посылки, если она содержит наркотическое средство. Если посылка перехвачена на почте, действия квалифицируются как покушение. Суды детально исследуют квитанции, данные трек-номеров и записи с камер видеонаблюдения в почтовых отделениях для идентификации отправителя.

При вовлечении в сбыт несовершеннолетних через социальные сети суды применяют пункт «в» части 4 статьи 228.1 УК РФ. Важным моментом является доказанность осознания подсудимым возраста вовлекаемого лица. В цифровой среде это доказывается анализом профиля несовершеннолетнего, характером переписки или личным знакомством. Если возраст не был очевиден, суды могут исключить данный признак, однако общая тенденция направлена на усиление ответственности организаторов, использующих молодежь в качестве «бегунков».

Оценка достоверности показаний свидетелей-потребителей в таких делах затруднена анонимностью. Часто свидетели указывают только на никнейм продавца в мессенджере. Суды восполняют этот пробел через идентификацию ID аккаунта, привязанного к номеру телефона или IP-адресу, который в свою очередь сопоставляется с данными провайдера о месте жительства подсудимого. Совокупность косвенных цифровых доказательств (совпадение времени выхода

в сеть, использование конкретных моделей устройств) позволяет судам выносить обвинительные приговоры даже при отсутствии прямых свидетелей визуального контакта.

Судебная практика также сталкивается с проблемой «пустых» закладок (мошенничество в наркобизнесе). Если лицо намеревалось сбыть наркотик, получило деньги, но в тайник положило муляж или ничего не положило, действия квалифицируются как мошенничество по статье 159 УК РФ. Однако, если в составе смеси присутствовало хотя бы незначительное количество психоактивного вещества, суды квалифицируют это как сбыт суррогата по всей массе смеси, что влечет ответственность по статье 228.1 УК РФ.

При назначении наказания суды учитывают роль подсудимого. Операторы и организаторы получают максимально суровые сроки, в то время как для рядовых закладчиков, активно способствующих раскрытию преступления и изобличению других участников, возможно применение статьи 64 УК РФ (назначение наказания ниже низшего предела). Суды детально проверяют объем выданных «адресов», о которых не было известно следствию, как критерий активного сотрудничества.

Вопросы конфискации имущества по делам о дистанционном сбыте включают изъятие не только денежных средств, но и технических средств совершения преступления. Смартфоны, ноутбуки, роутеры признаются орудиями преступления и подлежат обращению в доход государства. В последнее время суды начали практиковать конфискацию эквивалента стоимости криптовалюты, если сами цифровые активы были переведены на недоступные кошельки, но установлена сумма полученного дохода.

Судебная практика по делам о сбыте наркотиков через интернет демонстрирует высокую степень адаптивности к технологическим изменениям. Суды отходят от необходимости фиксации передачи «из рук в руки», заменяя ее анализом цифровых следов и логических цепочек передачи информации. Основной акцент делается на единстве умысла и технологической связанности действий всех участников дистанционной схемы.

Судебная практика по делам о дистанционном сбыте наркотических средств характеризуется приоритетом цифровых доказательств и расширительным толкованием момента окончания преступления через факт передачи информации о тайнике. Ключевой проблемой остается разграничение покушения и оконченного состава при пресечении деятельности на этапе закладки товара, а также сложности в идентификации субъекта в условиях тотальной анонимизации трафика. Эффективность правосудия в данной сфере напрямую зависит от качества компьютерно-технических экспертиз и способности судов правильно интерпретировать данные о движении криптовалют и метаданные электронных документов как подтверждение прямого умысла на сбыт. Требуется дальнейшая унификация подходов к оценке роли ИТ-специалистов в структуре наркошопов для обеспечения соразмерности наказания их вкладу в функционирование системы распределения запрещенных веществ.

§ 2. Особенности применения уголовного закона при выявлении преступлений, совершенных с использованием информационных технологий

Применение уголовного закона при выявлении преступлений, совершенных с использованием информационных технологий (ИТ), требует точного установления места, времени и способа совершения деяния, что в условиях цифровой среды приобретает специфические характеристики. Статья 9 УК РФ определяет время совершения преступления как время совершения общественно опасного действия (бездействия) независимо от времени наступления последствий. В ИТ-преступлениях этот момент часто разрывается во времени с моментом активации вредоносного программного обеспечения (ВПО) или осуществления удаленного доступа. Квалификация требует разграничения этапов подготовки, покушения и оконченного состава, особенно

в случаях использования автоматизированных скриптов, работающих без непосредственного участия человека в момент наступления вреда.

Место совершения преступления (статьи 11, 12 УК РФ) в киберпространстве детерминируется не только физическим нахождением лица, но и местом нахождения сервера, на котором размещена информация, либо местом наступления последствий. При трансграничном характере посягательств возникает проблема экстерриториальности уголовного закона. Если лицо находится вне пределов РФ, но использует ИТ для воздействия на объекты, находящиеся на территории РФ, деяние квалифицируется по российскому законодательству. Особенность заключается в необходимости доказывания того, что цифровое воздействие было направлено именно на защищаемые интересы РФ, что требует анализа сетевых протоколов, IP-адресов и маршрутизации трафика для подтверждения юрисдикции.

Квалификация хищений, совершаемых с использованием ИТ, опирается на разграничение норм статьи 158 (кража), статьи 159.3 (мошенничество с использованием электронных средств платежа) и статьи 159.6 (мошенничество в сфере компьютерной информации). Пункт «г» части 3 статьи 158 УК РФ предусматривает ответственность за кражу с банковского счета или в отношении электронных денежных средств. Ключевым признаком здесь является тайность изъятия, даже если для доступа к счету использовались учетные данные, полученные путем фишинга. Если виновный воздействует непосредственно на программное обеспечение финансовых организаций или модифицирует данные в информационных системах для хищения, деяние подлежит квалификации по статье 159.6 УК РФ. Разграничение проводится по критерию объекта воздействия: при краже объектом является денежная сумма на счете, при компьютерном мошенничестве – процесс обработки и передачи данных.

Статья 159.6 УК РФ требует установления способа совершения преступления: вмешательство в функционирование объектов хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Под вмешательством понимается

несанкционированное изменение данных, ввод ложной информации, удаление или блокирование сведений, приводящее к хищению. Если хищение совершается путем обмана или злоупотребления доверием конкретного лица через мессенджеры или социальные сети без технического воздействия на системы обработки данных, квалификация по статье 159.6 исключается в пользу статьи 159 или 159.3 УК РФ. Судебная практика исходит из того, что использование ИТ как средства связи для введения в заблуждение не образует состава компьютерного мошенничества.

Применение главы 28 УК РФ (преступления в сфере компьютерной информации) при выявлении ИТ-преступлений часто сталкивается с проблемой конкуренции общей и специальной норм. Статья 272 УК РФ предусматривает ответственность за неправомерный доступ к охраняемой законом компьютерной информации. Если такой доступ является этапом совершения хищения, возникает вопрос о необходимости дополнительной квалификации. Согласно позиции Верховного Суда РФ, если неправомерный доступ повлек уничтожение, блокирование, модификацию или копирование информации и был способом совершения другого преступления (например, мошенничества), деяние квалифицируется по совокупности статей 272 и соответствующей части статьи 159.6 или 158 УК РФ. Особенность заключается в том, что информация должна быть «охраняемой законом», что требует подтверждения наличия режима коммерческой, банковской или иной тайны, а также принятия собственником мер по защите данных.

Статья 273 УК РФ наказывает за создание, распространение или использование вредоносных компьютерных программ. При выявлении таких преступлений необходимо проведение компьютерно-технической экспертизы для подтверждения свойств программы: заведомой направленности на несанкционированное уничтожение, блокирование, модификацию или копирование информации. Использование бот-сетей (botnets) для проведения DDoS-атак или массовой рассылки спама с целью вымогательства требует квалификации по совокупности со статьей 273 и статьей 163 УК РФ. При этом

субъективная сторона характеризуется прямым умыслом относительно вредоносных свойств ПО, что отличает данное преступление от неосторожного нарушения правил эксплуатации (статья 274 УК РФ).

Особенности квалификации ИТ-преступлений по статье 274.1 УК РФ связаны с защитой критической информационной инфраструктуры (КИИ) РФ. Субъектом данного преступления могут быть как лица, имеющие доступ к объектам КИИ, так и внешние нарушители. Квалификация зависит от категории значимости объекта КИИ и характера наступивших последствий. Применение данной нормы требует интеграции уголовно-правового анализа с положениями Федерального закона № 187-ФЗ. Если воздействие на КИИ совершено в целях подрыва экономической безопасности или обороноспособности, деяние может переквалифицироваться на диверсию (статья 281 УК РФ), что требует установления специальной цели.

Субъективная сторона ИТ-преступлений характеризуется спецификой формирования умысла. Виновный должен осознавать не только общественную опасность своих действий, но и техническую сущность используемых средств. При использовании удаленного доступа через прокси-серверы, VPN-сервисы или сеть Tor умысел направлен на обеспечение анонимности и сокрытие следов, что в ряде случаев может рассматриваться как свидетельство повышенной общественной опасности и подготовки к преступлению. Определение вины при совершении преступлений с использованием искусственного интеллекта (ИИ) или нейросетей представляет особую сложность. В действующем УК РФ субъектом является только физическое лицо, поэтому квалификация строится на ответственности разработчика или пользователя, задавшего параметры работы ИИ, приведшие к преступному результату.

Формы соучастия в ИТ-преступлениях (статья 35 УК РФ) трансформируются в сторону децентрализованных структур. Организованная группа в цифровой среде может не иметь личного контакта между участниками. Роли распределяются функционально: «кодеры» (разработка ВПО), «дропы» (обналичивание), «администраторы» (координация). Для квалификации по части

4 статьи 158 или части 4 статьи 159.6 УК РФ необходимо доказать устойчивость группы, что подтверждается длительностью связи, использованием специализированных форумов, систем шифрования и распределением доходов. Применение статьи 210 УК РФ к ИТ-сообществам требует доказательства структурированности и цели получения финансовой выгоды, что осложняется анонимностью участников.

Проблема идентификации субъекта при выявлении преступлений, совершенных с использованием ИТ, решается через сопоставление цифровых следов (log-файлы, MAC-адреса, метаданные) с физическими доказательствами (изъятая техника, показания свидетелей). Применение уголовного закона невозможно без привязки виртуальной активности к конкретному лицу. Если устройство использовалось несколькими лицами или было скомпрометировано извне, возникает ситуация неустранимых сомнений в виновности, трактуемых в пользу обвиняемого. Использование «подставных» аккаунтов и арендованных серверов требует проведения оперативно-розыскных мероприятий по деанонимизации, результаты которых должны быть легализованы в рамках УПК РФ для последующей квалификации.

Квалификация незаконного оборота наркотиков с использованием ИТС (пункт «б» части 2 статьи 228.1 УК РФ) основывается на факте использования сетей как инструмента сбыта. Особенность заключается в том, что ИТС используются для поиска покупателей, передачи координат «закладок» и приема оплаты в криптовалюте. Момент окончания преступления связывается с выполнением действий по размещению товара в тайнике и передаче информации покупателю. Если информация не была передана по техническим причинам, деяние квалифицируется как покушение. Использование криптовалют в расчетах за наркотики влечет дополнительную квалификацию по статье 174.1 УК РФ (легализация), если доказана цель придания правомерного вида владению денежными средствами через цепочку транзакций и конвертацию в фиатные деньги.

Легализация (отмывание) денежных средств в ИТ-сфере (статьи 174, 174.1 УК РФ) часто включает использование «миксеров» и «тумблеров» для разрыва связи между преступным источником и конечным получателем. Квалификация требует установления факта совершения финансовых операций с имуществом, приобретенным преступным путем. Использование криптовалюты как предмета легализации признается судебной практикой (Постановление Пленума ВС РФ № 32), при этом стоимостный критерий (крупный и особо крупный размер) определяется на момент совершения операции по курсу соответствующей биржи. Сложность заключается в доказывании цели легализации, которая должна отличаться от простого распоряжения похищенным имуществом.

Применение норм о преступлениях против государственной власти и общественной безопасности (статьи 205.2, 280, 280.1, 282 УК РФ) в ИТ-среде связано с публичностью распространения информации. Использование сети «Интернет» является квалифицирующим признаком, повышающим общественную опасность деяния за счет неограниченного охвата аудитории. Квалификация требует лингвистической экспертизы контента для установления призывов к экстремизму или терроризму. Особенность применения закона здесь заключается в оценке «лайков», «репостов» и «комментариев» как актов распространения информации, что требует установления прямого умысла на доведение запрещенных сведений до третьих лиц.

Квалификация по совокупности со статьей 273 или 138.1 УК РФ (незаконный оборот специальных технических средств) зависит от функционала программного обеспечения. Если программа предназначена для скрытого получения информации и не имеет легального применения, её оборот образует самостоятельный состав. Применение закона требует разграничения между использованием бытовых устройств с функциями записи и специализированных технических средств, предназначенных для негласного получения информации.

Особенности применения уголовного закона при выявлении преступлений, совершенных с использованием ИТ, заключаются в необходимости комплексного анализа технического способа совершения деяния

и его правовой оценки через призму традиционных институтов уголовного права (место, время, субъект, вина). Основная сложность квалификации связана с трансграничностью и анонимностью цифровой среды, что требует адаптации норм о территориальном действии закона и формах соучастия к условиям виртуального пространства. Эффективная квалификация ИТ-преступлений невозможна без интеграции компьютерно-технических знаний в процесс доказывания, особенно при разграничении хищений, компьютерного мошенничества и неправомерного доступа к информации. Дальнейшее развитие уголовного закона должно идти по пути уточнения признаков вмешательства в информационные системы и учета специфики цифровых активов как предметов преступления, что позволит обеспечить адекватную защиту прав личности, общества и государства от высокотехнологичных угроз.

§ 3. Совершенствование уголовно-правовой нормы об ответственности за сбыт с использованием информационных технологий

Трансформация наркопреступности в условиях цифровизации диктует необходимость глубокой ревизии диспозиции статьи 228.1 УК РФ. Действующая редакция пункта «б» части 2 статьи 228.1 УК РФ, предусматривающая ответственность за сбыт наркотических средств с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»), не в полной мере отражает технологическую сложность современных способов совершения данного деяния. Проблема заключается в чрезмерной обобщенности термина «использование сетей», который охватывает как примитивную переписку в мессенджерах, так и функционирование децентрализованных торговых площадок в теневом сегменте интернета (Darknet). Совершенствование нормы требует дифференциации ответственности в зависимости от степени вовлеченности технологического инструментария в процесс распределения наркотиков, а также уточнения момента окончания преступления при бесконтактном способе сбыта.

Существующая правовая конструкция не учитывает специфику использования автоматизированных скриптов и ботов в мессенджерах Telegram, Signal и Element, которые минимизируют участие человека в транзакциях. Уголовно-правовая норма должна быть дополнена указанием на использование программных алгоритмов, обеспечивающих автоматизацию сбыта, что повышает общественную опасность за счет масштабируемости преступной деятельности. Необходимо внедрение квалифицирующего признака, касающегося администрирования информационных ресурсов, специально созданных для реализации запрещенных веществ. Это позволит разграничить рядовых исполнителей («закладчиков») и лиц, обеспечивающих техническую инфраструктуру сбыта (программистов, модераторов, системных администраторов), чья деятельность в текущий момент часто квалифицируется по общим нормам о соучастии, что не всегда соразмерно их вкладу в преступный результат.

Момент окончания сбыта при использовании ИТ нуждается в нормативном уточнении. Постановление Пленума Верховного Суда РФ № 14 указывает, что сбыт признается оконченным с момента выполнения лицом всех действий по передаче товара. Однако в цифровой среде «передача» разбивается на этапы: размещение предложения на витрине Darknet-магазина, получение оплаты в криптовалюте, загрузка координат тайника в базу данных, передача этих координат покупателю. Предлагается закрепить в законе, что при бесконтактном способе сбыт считается оконченным с момента направления покупателю сообщения, содержащего сведения о месте нахождения наркотического средства, при условии предварительного размещения товара в указанном месте. Это устранит неопределенность при разграничении покушения и оконченного состава в случаях, когда покупатель не успел забрать товар по независящим от него обстоятельствам.

Необходимо совершенствование нормы в части ответственности за создание и распространение программного обеспечения, предназначенного исключительно для функционирования наркошопов. Речь идет о CMS-системах

для теневых площадок, специализированных приложениях для курьеров с функцией автоматического удаления метаданных фотографий (EXIF) и шифрования координат. Включение в УК РФ специальной нормы или дополнение статьи 228.1 частью, предусматривающей ответственность за технологическое обеспечение сбыта, позволит привлекать к ответственности «цифровых архитекторов» наркобизнеса, которые в данный момент зачастую остаются вне рамок уголовного преследования из-за отсутствия прямого контакта с наркотиками.

Проблема анонимизации требует введения нового отягчающего обстоятельства – совершение преступления с использованием средств шифрования и сокрытия IP-адреса. Это обосновано тем, что использование таких технологий значительно затрудняет выявление преступления и идентификацию виновного, требуя от правоохранительных органов привлечения дорогостоящих экспертных ресурсов. Повышенная санкция за использование средств анонимизации будет стимулировать отказ от профессиональных методов конспирации и обеспечит превентивное воздействие на технически грамотных участников наркорынка.

Совершенствование уголовно-правовой нормы должно затронуть и вопросы вовлечения несовершеннолетних в сбыт через игровые платформы и социальные сети. Использование игровых механик («геймификация» сбыта) и вербовка через In-game чаты требуют выделения в отдельный квалифицирующий признак. Текущая редакция статьи 150 УК РФ не всегда эффективно работает в цифровой среде, где вербовщик может не осознавать возраст вовлекаемого лица из-за анонимности профиля. Предлагается установить презумпцию осознания возраста при использовании определенных каналов коммуникации, популярных среди молодежи, либо усилить ответственность за сбыт, осуществляемый через платформы с преимущественно подростковой аудиторией.

В контексте международного сотрудничества норма об ИТ-сбыте должна учитывать возможность совершения деяния в составе транснациональных

организованных групп. Цифровая среда позволяет координировать поставки из-за рубежа без физического пересечения границы организаторами. Необходимо синхронизировать диспозицию статьи 228.1 УК РФ с международными конвенциями в части определения «электронных доказательств», чтобы квалификация деяния могла опираться на данные, полученные из серверов, находящихся под иностранной юрисдикцией, если это предусмотрено двусторонними договорами.

Важным аспектом является разграничение сбыта и пропаганды наркотиков в сети (статья 6.13 КоАП РФ). Часто грань между рекламой магазина и предложением конкретной дозы размыта. Уголовный закон должен четко определять, что размещение гиперссылок на ресурсы, осуществляющие сбыт, или QR-кодов с аналогичным содержанием, является формой пособничества в сбыте, а не просто административным правонарушением. Это позволит эффективно пресекать деятельность «трафаретчиков» и лиц, занимающихся агрессивным маркетингом наркотиков в городской среде и интернете.

Интеграция искусственного интеллекта в системы мониторинга и анализа трафика требует правового закрепления возможности использования результатов работы AI при квалификации содеянного. Если система сбыта управляется нейросетью, генерирующей маршруты для курьеров и распределяющей финансы, ответственность должна ложиться на лицо, осуществившее запуск и настройку данной системы. Требуется уточнение понятия «использование информационных технологий» за счет включения в него систем искусственного интеллекта и автономных программных комплексов.

Необходимо пересмотреть подход к конфискации имущества при ИТ-сбыте. Статья 104.1 УК РФ должна быть дополнена положениями, упрощающими изъятие цифровых активов, включая криптовалюты, NFT и права на доменные имена, использовавшиеся в преступных схемах. Без лишения наркоорганизаций их цифровой инфраструктуры и накопленного криптокапитала уголовное наказание в виде лишения свободы отдельных

участников не достигает целей исправления и предупреждения новых преступлений, так как структура легко восстанавливается новыми исполнителями.

Развитие нормы должно идти по пути детализации способов воздействия на потребителя. Использование таргетированной рекламы, алгоритмов рекомендаций в социальных сетях для предложения наркотиков должно рассматриваться как более опасная форма сбыта, чем пассивное ожидание покупателя на торговой площадке. Это обусловлено агрессивным формированием спроса и вовлечением лиц, ранее не имевших намерения приобретать запрещенные вещества. Установление ответственности за «активное цифровое предложение» позволит эффективнее бороться с современными методами наркомаркетинга.

Процессуальное закрепление цифровых следов как основы для материально-правовой квалификации требует внесения изменений в примечания к статье 228.1 УК РФ. Необходимо определить статус «электронного образа наркотического средства» (фотографии товара в месте закладки) как доказательства оконченного сбыта. Сегодня классическое задержание преступника «на месте преступления» становится редкостью. Реалии изменились: теперь фундаментом обвинения становятся не вещественные доказательства в руках, а цифровой след – скриншоты, серверные логи и информация о соединениях (биллинг). Нашему уголовному законодательству необходимо перестроиться и научиться работать с такими уликами так же эффективно, как и с физическими предметами.

Преступления, совершенные через интернет, все чаще пересекаются с угрозами информационной безопасности. Когда наркоторговцы используют взломанные чужие профили или задействуют государственные сервисы, это не просто технический нюанс – это полноценное посягательство на цифровую инфраструктуру. Логичным было бы применять здесь совокупность наказаний: привлекать виновных не только за наркотики, но и за преступления в сфере компьютерной информации (глава 28 УК РФ). Настало время признать, что

использование IT-технологий – это не просто средство коммуникации, а квалифицирующий признак, который прямо указывает на масштабность и опасность содеянного для общества.

Кроме того, преступный мир активно внедряет скрытые методы обмена данными, например, стеганографию, когда координаты тайников прячут внутри обычных фотографий. Если законодатель будет пытаться перечислять в нормах конкретные технические устройства или софт, закон безнадежно устареет еще на этапе принятия. Эффективный подход – отказаться от закрытого перечня инструментов в пользу широкой формулировки. Достаточно закрепить, что любой способ дистанционного взаимодействия, исключающий личную встречу, является способом совершения преступления. Это избавит законодателей от необходимости постоянно «догонять» технический прогресс и править Уголовный кодекс при каждом обновлении протоколов связи.

При определении наказания за наркоторговлю в сети пора учитывать масштаб охвата аудитории. Очевидно, что преступник, выставивший товар на крупной площадке с десятками тысяч посетителей, представляет куда большую угрозу, чем тот, кто просто переписывается в мессенджере с парой знакомых. Если мы закрепим в законе отдельный признак – распространение через общедоступные ресурсы, – это поможет судам различать опасных организаторов масштабных «наркомаркетов» и мелких розничных сбытчиков.

Кроме того, нельзя игнорировать тот факт, что наркотрафик в интернете тесно переплетен с криптоэкономикой, которая часто используется для финансирования экстремизма и терроризма. Статья 228.1 УК РФ нуждается в обновлении: нужно четко прописать механизмы отслеживания транзакций в цифровых валютах. Задача уголовного права здесь – не просто наказать продавца наркотиков, а научиться вычислять цепочки, по которым деньги от «дури» уходят на деструктивную политическую деятельность. По сути, технологии стали тем «мостиком», который соединяет обычный наркобизнес с угрозами национальной безопасности, и законодательство должно этот мостик оперативно перекрывать. Проблема «цифровых посредников» – лиц, оказывающих услуги

по обмену фиатных денег на криптовалюту для покупателей наркотиков (так называемые p2p-обменники), – также нуждается в правовой оценке. Если лицо заведомо осознает, что его услуги используются для обеспечения расчетов в наркобизнесе, его действия должны квалифицироваться как соучастие в сбыте. Уточнение субъективной стороны в норме об ИТ-сбыте позволит привлекать к ответственности лиц, создающих финансовые шлюзы для теневого рынка.

Совершенствование законодательства должно учитывать и возможности облачных технологий. Хранение баз данных покупателей и координат тайников в облачных хранилищах за пределами РФ требует разработки механизмов заочного осуждения и признания таких данных достаточными для квалификации деяния как совершенного организованной группой. Применение уголовного закона в этой части должно быть направлено на разрушение цифрового ядра преступной организации, а не только на задержание низовых звеньев.

Реформирование статьи 228.1 УК РФ в части ИТ-сбыта должно сопровождаться разработкой методических рекомендаций для судей, где будут разъяснены технические термины и критерии оценки цифровых доказательств. Это обеспечит предсказуемость правосудия и исключит ошибки при квалификации сложных многоуровневых схем распространения наркотиков, включающих использование API, SDK и других программных инструментов.

Системный подход к изменению уголовного закона позволит создать эффективный барьер на пути распространения наркоугрозы в цифровом пространстве. Это требует не только ужесточения санкций, но и точной юридической дефиниции новых форм преступного поведения, возникающих на стыке высоких технологий и наркоторговли. Только через детализацию диспозиции и учет технологических особенностей сбыта можно достичь адекватности уголовно-правового воздействия современным вызовам.

Совершенствование уголовно-правовой нормы об ответственности за сбыт наркотиков с использованием информационных технологий требует перехода от формального упоминания «сетей» к детальному описанию технологических способов совершения преступления. Ключевыми направлениями

реформирования являются: закрепление момента окончания бесконтактного сбыта в момент передачи координат товара, введение ответственности за техническое администрирование и программное обеспечение наркоторговли, признание использования криптовалют и средств анонимизации квалифицирующими признаками. Необходимо законодательно разграничить роли участников цифровых наркосообществ, выделив организаторов инфраструктуры в категорию субъектов с повышенной ответственностью. Реализация данных предложений позволит привести уголовный закон в соответствие с фактическим характером общественных отношений в цифровой среде, обеспечит неотвратимость наказания для «высокотехнологичных» звеньев наркобизнеса и создаст правовую базу для эффективного международного противодействия трансграничным кибернаркоугрозам.

ЗАКЛЮЧЕНИЕ

Проведенное исследование уголовно-правовых средств противодействия незаконному обороту наркотических средств, совершаемых с использованием информационных технологий, позволило сформулировать следующие выводы и рекомендации.

Цифровая трансформация наркопреступности привела к переходу от иерархических структур к децентрализованным сетевым моделям. Использование криптографических протоколов, систем анонимизации TOR и I2P, а также мессенджеров Telegram и Signal обеспечивает бесконтактный способ совершения преступлений. Это обуславливает необходимость пересмотра традиционных подходов к определению места и времени совершения деяния, так как преступный умысел реализуется в виртуальном пространстве, не имеющем четких географических границ.

Квалифицирующий признак, предусмотренный пунктом «б» части 2 статьи 228.1 УК РФ, требует уточнения в части используемого инструментария. Современная судебная практика сталкивается с трудностями при разграничении использования сети Интернет как средства связи и как способа автоматизации сбыта. Предлагается закрепить в постановлении Пленума Верховного Суда РФ положение о том, что использование информационных технологий признается способом совершения преступления в случае, если оно направлено на обеспечение анонимности участников, автоматизацию поиска покупателей или сокрытие финансовых потоков.

Проблема квалификации стадий совершения преступления при дистанционном сбыте остается наиболее дискуссионной. Момент окончания преступления по статье 228.1 УК РФ при использовании «закладок» должен быть жестко привязан к моменту передачи покупателю координат или графических данных о месте нахождения вещества. Любые действия, совершенные до этого момента, включая размещение наркотика в тайнике без передачи информации

потребителю, подлежат квалификации как покушение на сбыт по статье 30 УК РФ, что исключает необоснованное вменение оконченного состава.

Доказательственная база по данной категории дел характеризуется спецификой «цифровых следов». Протоколы осмотра электронных носителей информации, логи транзакций в блокчейн-сетях и данные о IP-адресах становятся первичными доказательствами. Существует потребность в унификации методики изъятия виртуальных активов и признания их предметом преступления по статье 174.1 УК РФ. Необходима синхронизация норм уголовного права с законодательством о цифровых финансовых активах для эффективного противодействия легализации доходов, полученных от наркоторговли.

Повышение эффективности противодействия требует введения в УК РФ новых отягчающих обстоятельств, связанных с использованием специализированного программного обеспечения, включая ботов и нейросети, для управления логистикой наркопотоков. Дифференциация ответственности должна учитывать уровень технологической подготовки преступника, что позволит применять более строгие меры наказания к организаторам и администраторам теневых площадок, а не только к рядовым исполнителям-курьерам.

Итогом совершенствования уголовно-правовых средств должно стать создание комплексного механизма, сочетающего оперативное реагирование на появление новых психоактивных веществ и технологическую адаптацию следственных действий. Усиление ответственности за использование средств шифрования при совершении наркопреступлений обеспечит превентивное воздействие на цифровую среду и снизит доступность запрещенных веществ для конечных потребителей.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: принята всенародным голосованием 12 дек. 1993 г. с учетом поправок, внесенных Законами Рос. Федерации о поправках к Конституции Рос. Федерации от 30 дек. 2008 г. № 6-ФКЗ, от 30 дек. 2008 г. № 7-ФКЗ, от 5 февр. 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ, от 4 октября 2022 г. № 5-ФКЗ, от 4 октября 2022 г. № 6-ФКЗ, от 4 октября 2022 г. № 7-ФКЗ, от 4 октября 2022 г. № 8-ФКЗ // Рос. газ. 2020. 4 июля.

2. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая. 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Рос. газ. 1996. 25 июня.

3. Кодекс Российской Федерации об административных правонарушениях: федер. закон Рос. Федерации от 30 декабря 2001 г. № 195-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 20 дек. 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 26 дек. 2001 г. // Рос. газ. 2001. 31 декабря.

4. О наркотических средствах и психотропных веществах: федер. закон Рос. Федерации от 8 января 1998 г. № 3-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 10 дек. 1997 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 24 дек. 1997 г. // Рос. газ. 1998. 15 января.

5. О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами [Электронный ресурс] : постановление Пленума Верховного Суда РФ от 15 июня 2006 № 14. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.10.2025).

6. Об утверждении перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации [Электронный ресурс] : постановление Пленума Верховного Суда РФ от 30 июня

1998 № 681. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.10.2025).

II. Учебная, научная литература и иные материалы

1. Алехин В.П., Мельник Н.А. Особенности уголовно-правового регулирования незаконного оборота наркотических средств, осуществляемого при помощи сети Интернет // Вестник экономики и права. 2020. №38. С. 17-22.

2. Третьяков, Г. М. Информационные технологии в структуре способа совершения преступлений, связанных с незаконным оборотом наркотических средств / Г. М. Третьяков // Вестник Гродненского государственного университета имени Янки Купалы. Серия 4. Правоведение. – 2021. – Т. 11, № 1. – С. 96-103

3. Третьякова, Е. И. Информационные технологии в механизме преступлений, связанных с незаконным оборотом наркотических средств / Е. И. Третьякова // Криминалистика: вчера, сегодня, завтра. – 2022. – № 3(23). – С. 142-150.

4. Самолаева Е.Ю. Проблемы квалификации сбыта наркотических средств и психотропных веществ, совершенных с использованием информационно-телекоммуникационной сети "Интернет" // Эпоха науки. 2017. №11. С. 79-82.

5. Хромов, Е. В. Проблемы квалификации сбыта наркотических средств, психотропных веществ или их аналогов с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») / Е. В. Хромов // Криминалистъ. – 2021. – № 3(36). – С. 32-38.

6. Власов В.А. незаконный оборот наркотических средств и психотропных веществ и их аналогов как одна из важнейших и актуальных проблем обеспечения национальной безопасности России // Право и государство: теория и практика. 2023. №3 (219). С. 211-214.

7. Андрюшенков В.А., Андрюшенкова О.М. Использование информационных технологий как способ совершения преступлений // Закон и право. 2024. №5. С. 208-213.

III. Эмпирические и иные материалы

1. Приговор Симоновского районного суда от 16 декабря 2025 г. по делу № 1-637/2025. URL: https://clck.ru/3S533d (дата обращения: 20.12.2025).

2. Приговор Измайловского районного суда от от 1 октября 2025 г. по делу № 1-407/2025. URL: https://clck.ru/3S53Bh (дата обращения: 20.12.2025).

3. Приговор Измайловского районного суда от от 13 сентября 2025 г. по делу № 01-0453/2024. URL: https://clck.ru/3S53jP (дата обращения: 20.12.2025).

«Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну».

И.А. Гатценбиллер