Дата поступления рукописи в редакцию: 03.10.2026 г.
Дата принятия рукописи в печать: 10.11.2026 г.
DOI: 10.24412/2224-9133-2026-10-568-576

ПЕРЕВОЗНИКОВА Екатерина Юрьевна,
главный советник отдела законодательной деятельности Государственно-правового департамента Правительства Сахалинской области; соискатель кафедры уголовного права Санкт-Петербургского государственного университета,
e-mail: Ekaterinaperevoznikova@rambler.ru

Научный руководитель:
БУРЛАКОВ Владимир Николаевич,
доктор юридических наук, профессор кафедры уголовного права Санкт-Петербургский государственный университет,
e-mail: parus348@mail.ru

ФОРМЫ НЕЗАКОННОГО ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ (ВКЛЮЧАЯ СЕТЬ ИНТЕРНЕТ) ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ И ОСНОВАНИЯ (КРИТЕРИИ) КРИМИНАЛИЗАЦИИ

Аннотация. *Цель исследования. В результате анализа уголовного законодательства и научных публикаций выявлена проблема: технический факт использования информационной технологии нередко смешивается с ее функциональной ролью в механизме преступления и последующим уголовно-правовым значением. Выдвинута гипотеза, согласно которой разделение этих уровней позволяет построить устойчивую классификацию форм незаконного использования информационных технологий и одновременно избежать автоматической криминализации цифрового способа поведения. Методологическую основу составили формально-юридический, системно-структурный и функциональный методы. Гипотеза подтверждена сопоставлением научных позиций об информационно-телекоммуникационных сетях, преступных платформах и цифровых финансовых инструментах. Предложено выделять коммуникационную, координационно-организационную, информационно-дистрибутивную, технологическую, инфраструктурную, финансовую и конспиративную формы. Криминализация должна оцениваться отдельно: ее основанием выступает самостоятельный прирост общественной опасности, обусловленный функцией технологии, а критериями проверки – существенность этой функции, распространенность и типичность поведения, масштаб вреда, недостаточность иных правовых средств, исполнимость запрета и его социальная соразмерность. Намечены направления дальнейшей проверки модели на материале составов УК РФ и судебной практики.*

Highlights:

Анализ выявил смешение технической формы использования ИТ и ее уголовно-правового значения.

Гипотеза о функциональном критерии подтверждена сопоставлением разных моделей цифровой преступной деятельности.

Предложена двухэтапная модель: установление функции технологии и отдельная проверка основания криминализации.

Ключевые слова: *информационные технологии; сеть Интернет; механизм преступления; криминализация; функциональная классификация; общественная опасность.*

Для цитирования: *Перевозникова Е. Ю. Формы незаконного использования информационных технологий (включая сеть интернет) при совершении преступлений и основания (критерии) криминализации // Право и управление. 2026. № 10. С. 568–576.*

PEREVOZNIKOVA Ekaterina Yu.,
Chief Adviser, Legislative Activity Division, State Legal Department, Government of the Sakhalin Region; Applicant, Department of Criminal Law, Saint Petersburg State University

Supervisor:
BURLAKOV Vladimir Nikolaevich,
Doctor of Law, Professor of the Department of Criminal Law, St. Petersburg State University

FORMS OF ILLEGAL USE OF INFORMATION TECHNOLOGIES (INCLUDING THE INTERNET) IN THE COMMISSION OF CRIMES AND GROUNDS (CRITERIA) FOR CRIMINALIZATION

Annotation. *Purpose of the study. The analysis of criminal legislation and legal scholarship revealed a methodological problem: the technical fact of using information technology is often conflated with its functional role in the mechanism of a crime and with its subsequent criminal-law significance. The hypothesis tested in the article is that separating these analytical levels makes it possible to construct a stable classification of forms of illegal use of information technologies while avoiding automatic criminalization of digitally mediated conduct. The study uses formal legal, system-structural and functional methods. The hypothesis is supported by a comparative analysis of scholarly positions on information and telecommunication networks, criminal platforms and digital financial instruments. Seven functional forms are proposed: communicative, coordination-organizational, information-distributive, technological, infrastructural, financial and conspiratorial. Criminalization is assessed separately. Its basis is an independent increase in public danger caused by the technological function; the verification criteria include the significance of that function, prevalence and typicality of conduct, scale of harm, insufficiency of non-criminal remedies, enforceability of the prohibition and social proportionality. Further research should test the model against specific offences in the Russian Criminal Code and judicial practice.*

Key words: *information technologies; Internet; crime mechanism; criminalization; functional classification; public danger.*

For citation: *Perevoznikova E. Yu. Forms of illegal use of information technologies (including the internet) in the commission of crimes and grounds (criteria) for criminalization. Law and administration. 2026; (10):568–576. (In Russ.).*

Highlights:

The analysis revealed a conflation of the technical use of IT with its criminal-law significance.

The functional-criterion hypothesis was supported by comparing different models of digital criminal activity.

A two-stage model is proposed: identify the technological function, then test the basis for criminalization.

Анализ уголовного законодательства, разъяснений высшей судебной инстанции и научных публикаций показывает, что использование информационных технологий при совершении преступлений описывается неоднородно. Законодатель применяет формулы «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет», закрепляет самостоятельные составы преступлений в сфере компьютерной информации и одновременно учитывает цифровой способ в отдельных нормах Особенной части УК РФ. Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 унифицирует понимание электронных и информационно-телекоммуникационных сетей для целей уголовного закона, однако не решает вопрос о том, какое место конкретная технология занимает в механизме преступления и в каких случаях ее использование действительно меняет общественную опасность содеянного [13].

В доктрине накоплен значительный материал о компьютерной и цифровой преступности, информационно-телекоммуникационных сетях, платформах, криптовалютах и иных технологических инструментах. При этом классификационные основания различаются. В одних работах сеть Интернет рассматривается через категории способа и средства совершения преступления, в

других исследование строится вокруг компьютеризированных преступлений, отдельных технологических объектов либо конкретных составов [1; 4; 10; 11]. М.А. Ефремова прямо отмечает, что «понятие преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, в настоящее время в доктрине уголовного права еще не сформировалось» [4, с. 101]. Это наблюдение имеет более широкий смысл: устойчивой системы, позволяющей одинаково описывать функциональную роль информационных технологий в разных преступлениях, также не сложилось.

По результатам анализа выявлена научная проблема. Технический признак использования информационной технологии нередко смешивается с ее уголовно-правовым значением. Из-за этого в одной плоскости оказываются разные явления: технология как средство связи, способ выполнения объективной стороны, среда распространения информации, элемент организации преступной деятельности, платежный инструмент либо средство сокрытия. Такое смешение затрудняет классификацию и создает риск неверного вывода о том, что любое использование сети Интернет само по себе увеличивает общественную опасность деяния и способно служить аргументом для расширения уголовно-правового запрета.

Гипотеза исследования состоит в следующем. Если отделить фактическую функцию информационной технологии в механизме преступной деятельности от ее последующей уголовно-правовой оценки, то формы незаконного использования информационных технологий могут быть систематизированы по единому функциональному критерию. Вопрос о криминализации при этом должен решаться отдельно: не исходя из наименования технологии или факта ее использования, а после установления того, создает ли соответствующая функция самостоятельный прирост общественной опасности и имеется ли действительная потребность в уголовно-правовом запрете.

Цель статьи – проверить эту гипотезу на материале уголовно-правовой доктрины и действующего регулирования, определить основные функциональные формы незаконного использования информационных технологий и предложить критерии оценки их криминализационного значения. При этом криминализация понимается в строгом смысле как признание ранее непреступного вида поведения преступным и уголовно наказуемым. Введение квалифицирующего признака в уже существующий состав относится к дифференциации уголовной ответственности; смешение этих решений методологически нежелательно, хотя оценка общественной опасности цифрового способа необходима в обоих случаях.

Методологическая база проведенного исследования состоит в следующем. Исследование построено как системный уголовно-правовой анализ. Нормативную основу составили положения УК РФ и разъяснения Пленума Верховного Суда Российской Федерации о преступлениях в сфере компьютерной информации и иных деяниях, совершенных с использованием электронных или информационно-телекоммуникационных сетей. Научную основу образовали работы, в которых исследуются значение информационно-телекоммуникационных сетей, платформизация преступной деятельности, цифровые финансовые инструменты, современные тенденции ИКТ-преступности и основания криминализации [1–12, 14].

Формально-юридический метод применялся для разграничения способа, средства, обстановки и иных признаков объективной стороны, а также для отделения криминализации от дифференциации ответственности. Системно-структурный анализ позволил рассматривать технологию не изолированно, а в связи с последовательностью преступных действий и взаимодействием участников. Функциональный метод использован как основной: значение технологии устанавливалось по задаче, которую она фактически выполняет в преступном механизме. Сопоставление доктринальных позиций служило не для механического суммирования существующих классификаций, а для проверки того, объясняет ли функциональный критерий обнаруженные в них расхождения. Для дальнейшего анализа важно разграничить основание криминализации и критерии его установления. Основание выражает объективную общественную потребность в уголовно-правовой охране, возникающую при такой степени общественной опасности поведения, которая не может быть адекватно нейтрализована иными средствами. Критерии представляют собой проверяемые признаки, позволяющие установить наличие или отсутствие этого основания. Такое различение согласуется с современными исследованиями криминализации, где общественная опасность рассматривается в связи с распространенностью деяния, возможностями иных отраслей права, потенциалом уголовно-правового воздействия и состоянием общественного правосознания [2; 6].

Расхождение классификационных оснований и проверка гипотезы состоит в следующем.

Проблема классификации начинается с того, что одна и та же сеть или программа не имеет постоянного уголовно-правового назначения. Мессенджер может использоваться для обычной переписки, передачи координат тайника, распределения ролей в преступной группе, получения платежных реквизитов или удаления сообщений после совершения деяния. В каждом случае технический объект один, но его функция различна.

Поэтому классификация по названию технологии быстро утрачивает объяснительную способность: она фиксирует инструмент, но не показывает его место в преступной деятельности.

Научные позиции подтверждают необходимость такого разграничения. А.И. Антипов, исследуя преступления с признаками призывов, склонения и незаконного оборота предметов и материалов, обращает внимание на массовость цифрового распространения. В изложении М.А. Ефремовой его вывод сформулирован так: использование информационно-телекоммуникационных сетей позволяет «массово и в короткий срок распространять информацию неограниченному кругу лиц» [1, с. 64; 4, с. 103]. Здесь сеть значима не просто как техническое средство передачи данных; она меняет масштаб и адресность распространения. Это позволяет выделить самостоятельную информационно-дистрибутивную функцию.

Иной уровень использования технологии обнаруживается при платформизации преступной деятельности. Р.И. Дремлюга и А.И. Коробеев определяют платформу для осуществления преступной деятельности как «особую форму организации компьютерной информации», структурированную для повышения эффективности взаимодействия заинтересованных в совершении преступлений лиц [3, с. 47]. В данном случае цифровая среда уже не обслуживает единичную операцию. Она организует повторяемое взаимодействие, объединяет участников, правила, информационные потоки и иные элементы преступной инфраструктуры. Такая конструкция не укладывается полностью ни в традиционное понимание средства, ни в характеристику отдельного способа совершения преступления.

Особенно важен вывод М.А. Ефремовой о связи ИТС с общественной опасностью. Автор указывает, что их использование «не всегда повышает общественную опасность деяния» [4, с. 101], а в более поздней работе подчеркивает: использование сетей может быть признаком основного или квалифицированного состава, «однако не всегда усиливает его общественную опасность» [5, с. 22]. Это положение имеет принципиальное значение для проверки выдвинутой гипотезы. Сам факт применения сети не позволяет автоматически перейти от описания способа поведения к выводу о необходимости уголовно-правового запрета или усиления ответственности.

В то же время цифровой компонент способен реально изменить механизм причинения вреда. На примере ИТС Ефремова связывает повышение опасности с упрощением выполнения объективной стороны, дистанционностью, возможностью воздействовать на большое число потерпевших и скрывать следы [4, с. 104]. В финансовой сфере аналогичный эффект возникает не из-за самого существования криптовалюты, а из-за тех свойств, которые востребованы в конкретной преступной модели. А.О. Миронов отмечает, что криптовалюты «способны обеспечить относительную анонимность» [8, с. 144]. Следовательно, один цифровой инструмент может одновременно выполнять финансовую и конспиративную функции, но каждая из них должна оцениваться самостоятельно.

Сопоставление этих позиций подтверждает исходное предположение. Устойчивым классификационным основанием является не технический объект и не отраслевой состав преступления, а функция технологии в механизме преступной деятельности. Технологическое средство становится юридически значимым только через конкретное использование. Отсюда следует и второй вывод: одна форма не равна одному составу преступления, а в одном преступлении могут сочетаться несколько форм.

Необходимо также развести два близких, но не совпадающих объекта классификации. Классификация видов преступлений отвечает на вопрос, какие группы деяний можно объединить по объекту посягательства, законодательной конструкции, характеру вреда или иному уголовно-правовому признаку. Классификация форм использования информационных технологий отвечает на другой вопрос – как именно технология включена в механизм преступной деятельности. Эти классификации пересекаются, но не подменяют друг друга. Например, преступления против собственности и преступления в сфере незаконного оборота наркотиков относятся к различным уголовно-правовым группам, однако в обоих случаях могут одновременно присутствовать коммуникационная, финансовая и конспиративная формы использования цифровых средств. Такое различение позволяет избежать попытки построить универсальную систему «цифровых преступлений» только по признаку наличия Интернета.

Функциональный подход дает возможность учитывать и внутреннюю динамику преступной деятельности. Одна и та же технология способна менять роль по мере развития преступного замысла: на подготовительном этапе обеспечивать связь, в момент совершения деяния – выполнять технологическую операцию, после получения преступного дохода – обслуживать расчет, а затем использоваться для сокрытия следов. Поэтому для анализа важна не только доминирующая функция, но и последовательность функций. Такая конструкция объясняет, почему попытки закрепить за конкретной технологией одно неизменное уголовно-правовое значение приводят к упрощению фактического механизма преступления.

Функциональные формы незаконного использования информационных технологий представляются в следующем.

Коммуникационная форма охватывает передачу преступно значимой информации между участниками: сообщений, инструкций, фотографий, координат, кодов доступа, сведений о потерпевшем, реквизитов и иных данных. Ее признак – обеспечение информационного обмена. Преступное действие может выполняться за пределами самой коммуникации, поэтому наличие переписки еще не раскрывает уголовно-правовое значение технологии. Для оценки существенны содержание передаваемых сведений, роль адресата и связь сообщения с последующим поведением.

Координационно-организационная форма возникает тогда, когда цифровые средства используются для управления совместной деятельностью: распределения ролей, постановки заданий, контроля исполнения, поддержания иерархии или согласования повторяющихся действий. От обычной коммуникации ее отличает управленческая функция. Передача сообщения здесь служит не самостоятельной целью, а элементом организации поведения нескольких лиц. При устойчивом характере такой организации координационная форма может переходить в инфраструктурную.

Информационно-дистрибутивная форма связана с размещением, тиражированием и обеспечением доступа к противоправной информации. Ее содержание раскрывается через масштаб распространения, неопределенность либо множественность адресатов, скорость доведения материала и возможность длительного сохранения доступа. Именно эти свойства объясняют, почему использование сети приобретает особое значение в составах, где общественная опасность зависит от публичности или массового информационного воздействия. Техническая публикация и криминально значимое распространение совпадают не всегда; решающими остаются содержание материала и признаки конкретного состава.

Технологическая форма имеет место, когда информационная технология непосредственно обеспечивает выполнение преступной операции. К ней относятся неправомерное воздействие на компьютерную информацию, применение вредоносного программного обеспечения, автоматизированное выполнение команд, технологическое вмешательство в работу системы и иные действия, где без цифрового инструмента объективная сторона в избранном виде не может быть реализована. Здесь связь между технологией и причинением вреда наиболее тесная. По этой причине технологическая форма чаще других способна иметь самостоятельное уголовно-правовое значение.

Инфраструктурная форма отличается масштабом. Она выражается в создании или использовании цифровой среды, обеспечивающей не единичное действие, а воспроизводимость преступной деятельности: платформы, сервера, системы учетных записей, программно-технического комплекса, распределенной информационной архитектуры. Исследование платформизации показывает, что такая среда может повышать эффективность взаимодействия различных групп участников [3]. В отличие от координации, которая описывает управление лицами, инфраструктура относится к устойчивой технологической основе их деятельности. Именно здесь наиболее отчетливо проявляется возможность появления нового самостоятельного объекта уголовно-правовой оценки.

Финансовая форма включает использование электронных платежных средств, интернет-банкинга, цифровых валют и иных цифровых инструментов для получения, передачи, распределения, конвертации либо сокрытия имущественных ценностей. Ее нельзя сводить к криптовалютам. Определяющей является функция движения стоимости в преступном механизме. Исследования современной наркопреступности показывают, что цифровые валюты включаются в уже существующие криминальные рынки как расчетный инструмент [8; 9; 12]. Правовая оценка поэтому должна зависеть от характера операции и ее связи с основным преступлением, а не от цифровой формы актива как таковой.

Конспиративная форма проявляется в использовании технологических свойств для дистанцирования участников, снижения их идентифицируемости, минимизации прямых контактов, сокрытия информационных следов или затруднения обнаружения преступной деятельности. Она нередко сочетается с коммуникационной и финансовой формами. Ефремова указывает на возможность, «сохраняя анонимность, осуществить воздействие на объект уголовно-правовой охраны дистанционно» и скрыть следы преступления [4, с. 104]. Самостоятельность конспиративной функции не означает, что анонимность должна автоматически криминализироваться: ее значение определяется тем, какую роль она играет в конкретном посягательстве.

Предложенная система не является перечнем видов преступлений. Она описывает устойчивые способы функционального включения технологии в преступную деятельность. Это принципиально: классификация остается применимой при появлении новых программ, сервисов и цифровых активов, поскольку изменение технического инструментария не требует каждый раз создавать новую категорию. Если новый инструмент выполняет уже известную функцию, он включается в

существующую форму; новая форма потребуется лишь тогда, когда возникнет иная устойчивая функция в механизме причинения вреда.

Основания и критерии криминализации цифровых форм поведения состоят в ледующем.Функциональная классификация решает описательную задачу, но не отвечает сама по себе на вопрос о криминализации. Для этого требуется второй уровень анализа. В теории уголовного правотворчества основание криминализации связывается с общественной потребностью в уголовно-правовой охране и с такой общественной опасностью поведения, которая оправдывает применение наиболее строгой формы государственного принуждения [2; 6]. Применительно к цифровой сфере этот тезис требует уточнения: общественную опасность необходимо связывать не с наличием технологии, а с тем изменением механизма посягательства, которое вызвано выполняемой ею функцией.

Поэтому центральным основанием криминализации следует считать самостоятельный прирост общественной опасности, обусловленный функциональным использованием информационной технологии. Такой прирост имеет место, когда цифровая функция позволяет причинять качественно иной или существенно больший вред, создавать устойчивую преступную инфраструктуру, многократно воспроизводить посягательство, охватывать значительно более широкий круг потерпевших либо формировать способ поведения, который не охватывается существующими уголовно-правовыми запретами. Если технология лишь облегчает обычное действие, но не меняет характера и масштаба опасности, основание для новой криминализации не возникает.

Наличие указанного основания должно проверяться по нескольким взаимосвязанным критериям. Существенность функциональной роли показывает, является ли технология необходимым или значимым элементом конкретной модели причинения вреда. Распространенность и типичность позволяют отличить устойчивое общественно опасное явление от единичного криминализационного повода. Важен и характер вреда: его масштаб, число потенциальных потерпевших, повторяемость и возможность дистанционного воздействия. Эти параметры относятся к юридико-криминологическому блоку, который используется и при оценке криминализации преступных платформ [3].

Следующая проверка касается субсидиарности уголовного права. Новая уголовно-правовая норма оправдана лишь при недостаточности гражданско-правовых, административных, информационно-правовых, технических и организационных средств воздействия. М.А. Ефремова, рассматривая возможность дополнения УК РФ признаком использования ИТС, связывает ее не только с повышением возможного вреда, но и с «невозможностью установления иных правовых запретов для устранения возникшей опасности причинения вреда» [4, с. 104]. Для криминализации этот довод еще весомее: уголовный запрет не должен заменять собой регулирование, способное эффективно пресечь менее опасное поведение.

Отдельной оценки требует исполнимость запрета. Цифровая среда не отменяет требований определенности состава, доказуемости признаков и реальной возможности правоприменения. Если граница между правомерным и преступным использованием технологии не может быть сформулирована достаточно точно, криминализация создаст риск расширительного толкования. С этим связан и социально-экономический критерий: затраты уголовной юстиции и ограничения правомерного оборота не должны быть несоразмерны предотвращаемому вреду. Социально-психологический блок дополняет оценку через состояние правосознания и восприятие запрета обществом [6].

Такой подход позволяет по-разному оценивать выделенные формы. Для коммуникационной формы обычно недостаточно самого факта цифрового общения: общественную опасность создает содержание взаимодействия и его связь с преступлением. Информационно-дистрибутивная форма может давать самостоятельный прирост опасности там, где сеть увеличивает масштаб публичного воздействия. Технологическая и инфраструктурная формы обладают наиболее выраженным потенциалом для самостоятельной криминализации, поскольку цифровой компонент способен образовать сам механизм причинения вреда либо устойчивую среду преступной деятельности. Финансовая и конспиративная функции чаще выступают обеспечивающими и требуют особенно осторожного разграничения с правомерными операциями и способами защиты частной жизни.

Иллюстративным является исследование Р.И. Дремлюги и А.И. Коробеева. Авторы не ограничиваются констатацией появления преступных платформ, а проверяют создание и обеспечение их работы через юридико-криминологические, социально-экономические и социально-психологические факторы и приходят к выводу о соответствии такого поведения критериям криминализации [3, с. 47–56]. Тем самым одна конкретная инфраструктурная форма получает обоснование уголовно-правового запрета не потому, что реализуется в цифровой среде, а вследствие совокупности характеристик общественной опасности и возможности уголовно-правового воздействия.

Проведенный анализ подтвердил выдвинутую гипотезу. Научные позиции, которые на первый взгляд используют разные классификационные основания, становятся сопоставимыми, если рассматривать их через фактическую функцию технологии. Средство передачи информации соответствует коммуникационной функции; массовое распространение – информационно-дистрибутивной; цифровая платформа – инфраструктурной; криптовалюта в расчетах – финансовой; анонимизация и дистанцирование – конспиративной. Противоречие между такими подходами во многом снимается, поскольку они описывают разные уровни одного механизма.

Одновременно источники показывают пределы функционального подхода. Форма характеризует фактическое включение технологии, но не предрешает юридический вывод. Позиция о том, что использование ИТС не всегда усиливает общественную опасность [4; 5], исключает автоматический переход от формы к криминализации. С другой стороны, анализ преступных платформ [3] демонстрирует ситуацию, когда инфраструктурная функция приобретает такую самостоятельность и опасность, что вопрос о специальном уголовно-правовом запрете становится обоснованным. Именно различие этих случаев подтверждает необходимость двухэтапной оценки.

Дополнительный аргумент в пользу осторожного подхода дает современная оценка цифровизации уголовного законодательства. Е.А. Русскевич показывает, что технологическая новизна далеко не всегда требует новой уголовно-правовой конструкции: значительная часть цифровых способов поведения может быть охвачена уже существующими моделями составов [11]. Для рассматриваемой темы это означает, что обнаружение новой технологии еще не свидетельствует о пробеле уголовного закона. Пробел следует искать в механизме охраны: остается ли общественно опасная функция за пределами действующего запрета и нельзя ли устранить риск средствами уже существующих норм.

В качестве решения научной проблемы предлагается модель «функция – уголовно-правовая оценка». На первом этапе устанавливается, какую задачу информационная технология выполняет в механизме преступной деятельности и к какой форме относится ее использование. На втором проверяется наличие основания криминализации через критерии прироста общественной опасности, типичности и распространенности, существенности технологической функции, недостаточности иных правовых средств, исполнимости запрета, его социально-экономической соразмерности и приемлемости для правосознания. Такая модель не подменяет традиционную теорию криминализации, а адаптирует ее к цифровой среде и препятствует превращению технического признака в самодостаточный аргумент уголовной политики.

Анализ нормативного и доктринального материала выявил отсутствие единого критерия, который позволял бы последовательно классифицировать формы незаконного использования информационных технологий в различных преступлениях и одновременно определять их уголовно-правовое значение. Причина заключается не столько в недостатке классификаций, сколько в смешении технического, функционального и нормативного уровней анализа.

Проверка гипотезы показала, что наиболее устойчивым основанием систематизации является функция технологии в преступном механизме. С этих позиций обосновано выделение коммуникационной, координационно-организационной, информационно-дистрибутивной, технологической, инфраструктурной, финансовой и конспиративной форм. Их сочетание в одном преступлении допустимо и отражает многофункциональность цифровых инструментов.

Самостоятельного решения требует вопрос о криминализации. Основанием для уголовно-правового запрета является не цифровая форма поведения как таковая, а обусловленный ею прирост общественной опасности при наличии общественной потребности в уголовно-правовой охране. Предложенные критерии позволяют проверить этот вывод и отделить случаи, где технология лишь сопровождает преступление, от ситуаций, в которых она формирует новый или качественно измененный механизм причинения вреда.

В заключении следует учитывать следующее.

Полученный результат задает направление дальнейшего научного поиска. Следующий этап должен быть связан с постатейным анализом УК РФ: необходимо установить, какие из выделенных форм уже отражены в конструкциях составов, где цифровой признак используется как средство дифференциации ответственности и в каких случаях он остается только фактической характеристикой механизма преступления. Отдельного исследования требует судебная практика после принятия постановления Пленума Верховного Суда РФ № 37; ее можно анализировать через кодирование функциональной роли технологии в конкретных делах и сопоставление этой роли с квалификацией. Сравнительно-правовой материал позволит проверить устойчивость предложенной классификации за пределами российского уголовного законодательства. Такая эмпирическая проверка необходима, чтобы перейти от концептуальной модели к рекомендациям по корректировке отдельных уголовно-правовых норм.

Список литературы:

[1] Антипов А.И. Уголовно-правовое значение использования средств массовой информации и информационно-телекоммуникационных сетей при совершении преступлений с признаками призывов, склонения, незаконного оборота предметов и материалов : дис. … канд. юрид. наук : 5.1.4. Санкт-Петербург, 2022. 248 с. EDN: RINWAA.

[2] Боковня А.Ю. Основание криминализации деяний в сфере охраны окружающей среды // Пробелы в российском законодательстве. 2026. Т. 19. № 1. С. 112–117. DOI: 10.33693/2072-3164-2026-19-1-112-117. EDN: UIVBHI.

[3] Дремлюга Р.И., Коробеев А.И. Уголовно-правовая политика в сфере противодействия платформизации преступной деятельности // Всероссийский криминологический журнал. 2022. Т. 16. № 1. С. 47–56. DOI: 10.17150/2500-4255.2022.16(1).47-56. EDN: LOCVWO.

[4] Ефремова М.А. Информационно-телекоммуникационные сети как средство совершения преступлений // Вестник Казанского юридического института МВД России. 2023. Т. 14. № 4 (54). С. 101–106. DOI: 10.37973/KUI.2023.84.83.013. EDN: UBEXPT.

[5] Ефремова М.А. Уголовно-правовое значение использования информационно-телекоммуникационных сетей при совершении преступлений // Российская юстиция. 2024. № 1. С. 22–27. DOI: 10.52433/01316761_2024_01_22. EDN: TQUUIX.

[6] Кравец И.П. Проблемные вопросы системы оснований и принципов криминализации // Пробелы в российском законодательстве. 2024. Т. 17. № 6. С. 158–168. DOI: 10.33693/2072-3164-2024-17-6-169-176. EDN: IOYVPD.

[7] Литвяк Л.Г. К вопросу о понятии электронных или информационно-телекоммуникационных сетей для целей уголовного закона // Гуманитарные, социально-экономические и общественные науки. 2020. № 11. С. 93–96. DOI: 10.23672/77835-4590-1440-s. EDN: TKURAQ.

[8] Миронов А.О. Криптовалюты как средство совершения преступлений в сфере незаконного оборота наркотических средств и психотропных веществ в современных условиях // Криминалистика: вчера, сегодня, завтра. 2024. № 4 (32). С. 144–154. DOI: 10.55001/2587-9820.2024.10.91.015. EDN: XOSVNV.

[9] Репецкая А.Л. Современные тенденции развития преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Baikal Research Journal. 2025. Т. 16. № 3. С. 947–953. DOI: 10.17150/2411-6262.2025.16(3).947-953. EDN: BCJSUO.

[10] Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения : монография. 2-е изд., перераб. и доп. Москва : ИНФРА-М, 2023. 351 с. DOI: 10.12737/1840963. ISBN 978-5-16-017297-2. EDN: MPWWHL.

[11] Русскевич Е.А. Цифровизация уголовного законодательства: непростые последствия простых решений // Вестник Университета имени О.Е. Кутафина (МГЮА). 2025. № 5 (129). С. 26–33. DOI: 10.17803/2311-5998.2025.129.5.026-033. EDN: EZVFAO.

[12] Соловьев О.Г., Князьков А.А. Современное состояние отечественного законодательства в сфере оборота цифровых валют и цифровых активов и вопросы правоприменения в уголовно-правовой сфере // Вестник Ярославского государственного университета им. П.Г. Демидова. Серия Гуманитарные науки. 2024. Т. 18. № 3 (69). С. 440–447. DOI: 10.18255/1996-5648-2024-3-440-447. EDN: MQCEDI.

[13] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет: постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37.

[14] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в действующей редакции).

References:

[1] Antipov A.I. Criminal law significance of the use of mass media and information and telecommunication networks when committing crimes with signs of incitement, inducement, illegal circulation of objects and materials: dis.... cand. jurid. Sciences: 5.1.4. St. Petersburg, 2022. 248 c. EDN: RINWAA.

[2] Bokovnya A.Yu. Basis for criminalization of acts in the field of environmental protection // Gaps in Russian legislation. 2026. VOL. 19. № 1. S. 112-117. DOI: 10.33693/2072-3164-2026-19-1-112-117. EDN: UIVBHI.

[3] Dremlyuga R.I., Korobeev A.I. Criminal law policy in the field of countering the platformization of criminal activity // All-Russian Criminological Journal. 2022. T. 16. № 1. S. 47-56. DOI: 10.17150/2500-4255.2022.16(1).47-56. EDN: LOCVWO.

[4] Efremova M.A. Information and telecommunication networks as a means of committing crimes // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2023. T. 14. № 4 (54). S. 101-106. DOI: 10.37973/KUI.2023.84.83.013. EDN: UBEXPT.

[5] Efremova M.A. Criminal law significance of the use of information and telecommunication networks in the commission of crimes // Russian

justice. 2024. № 1. S. 22-27. DOI: 10.52433/01316761_2024_01_22. EDN: TQUUIX.

[6] Kravets I.P. Problematic issues of the system of grounds and principles of criminalization // Gaps in Russian legislation. 2024. VOL. 17. № 6. S. 158-168. DOI: 10.33693/2072-3164-2024-17-6-169-176. EDN: IOYVPD.

[7] Litvyak L.G. On the concept of electronic or information and telecommunication networks for the purposes of the criminal law // Humanities, socio-economic and social sciences. 2020. № 11. S. 93-96. DOI: 10.23672/77835-4590-1440-s. EDN: TKURAQ.

[8] Mironov A.O. Cryptocurrencies as a means of committing crimes in the field of illicit trafficking in narcotic drugs and psychotropic substances in modern conditions // Forensics: yesterday, today, tomorrow. 2024. № 4 (32). S. 144-154. DOI: 10.55001/2587-9820.2024.10.91.015. EDN: XOSVNV.

[9] Repetskaya A.L. Current trends in the development of crimes committed using information and telecommunication technologies // Baikal Research Journal. 2025. T. 16. № 3. S. 947-953. DOI: 10.17150/2411-6262.2025.16(3).947-953. EDN: BCJSUO.

[10] Russkevich E.A. Criminal law and "digital crime": problems and solutions: monograph. 2nd ed., Revised and add. Moscow: INFRA-M, 2023. 351 pp. DOI: 10.12737/1840963. ISBN 978-5-16-017297-2. EDN: MPWWHL.

[11] Russkevich E.A. Digitalization of criminal legislation: the difficult consequences of simple solutions // Bulletin of the University named after O.E. Kutafin (MSLA). 2025. № 5 (129). S. 26-33. DOI: 10.17803/2311-5998.2025.129.5.026-033. EDN: EZVFAO.

[12] Soloviev O.G., Knyazkov A.A. The current state of domestic legislation in the field of turnover of digital currencies and digital assets and issues of law enforcement in the criminal legal sphere // Bulletin of Yaroslavl State University named after P.G. Demidov. Humanities series. 2024. T. 18. № 3 (69). S. 440-447. DOI: 10.18255/1996-5648-2024-3-440-447. EDN: MQCEDI.

[13] On certain issues of judicial practice in criminal cases of crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet: decision of the Plenum of the Supreme Court of the Russian Federation of 15.12.2022 No. 37.

[14] Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ (as amended).

