Цифровое пространство в системе признаков объективной стороны преступления: теоретико-правовое осмысление

Нурматов Ахаджон Атхамджонович
адъюнкт, Краснодарский университет МВД России,
akhadjon80@gmail.com

Стремительная дематериализация преступных деяний обнажила догматический кризис современного уголовного права. Жесткая географическая привязка вступает в прямое концептуальное противоречие с децентрализованной, экстерриториальной «архитектурой» киберпреступности. Видимо, традиционные физические координаты места и времени необратимо утратили свою универсальность. Они перестали отвечать запросам практики. Цель в статье сводится к формированию обновленной теоретико-правовой парадигмы объективной стороны преступления, где цифровая среда исследуется не как технический фон, а в качестве самостоятельного топологического объекта. Примечательно, что сравнительный срез правоприменения высветил диаметрально разные стратегии адаптации к этим вызовам. Если российский законодатель тяготеет к казуистичному дроблению норм о цифровом мошенничестве, то таджикская практика пытается расширительно толковать классические составы для противодействия транснациональному сетевому экстремизму, однако регулярно упирается в юрисдикционный тупик. На основании отмеченного автор делает вывод о неизбежности перехода к гибридной модели оценки объективных признаков, в которой сочетаются физические и виртуальные критерии. Изложенный материал имеет прикладную ценность для следственных работников, судейского корпуса, исследователей, которые заняты проектированием адекватной уголовной политики в эпоху технологической сингулярности.

Ключевые слова: виртуальная среда, киберпреступность, место совершения преступления, объективная сторона преступления, Республика Таджикистан, Российская Федерация, сравнительное правоведение, цифровое пространство.

Введение

Современная догматика уголовного права объективно нуждается в масштабной и всесторонней ревизии базовых категорий. По сути, интенсивное развитие информационно-коммуникационных технологий привело к формированию качественно новой среды взаимодействия субъектов. Видимо, классические и укоренившиеся подходы к пониманию места, времени, способа совершения преступления постепенно утрачивают свою прежнюю универсальность. Впрочем, это вполне закономерный процесс эволюции правовой материи.

Сегодня цифровое пространство перестает быть сугубо техническим или социологическим термином. Оно приобретает отчетливые юридические контуры. Как представляется, именно в рамках учения об объективной стороне преступных деяний данная категория раскрывает свой истинный научный и прикладной потенциал.

Объективная сторона традиционно выступает в качестве внешнего акта проявления замысла. Между тем, перенос криминальной активности в виртуальную плоскость существенным образом дематериализует этот акт. Действия виновного лица зачастую сводятся к нажатию клавиш, созданию сложного программного кода либо к банальной отправке электронных пакетов данных. Одновременно с этим, наступают вполне реальные, физически осязаемые общественно опасные последствия в виде имущественного ущерба или нарушения работы инфраструктуры. Примечательно, что разрыв во времени и географическом пространстве между совершенным деянием и наступившим результатом становится в киберпреступности скорее правилом, нежели исключением. В связи с этим отметим, что классическая концепция места совершения преступления остро требует концептуальной адаптации к реалиям децентрализованной сетевой архитектуры.

Материалы и методы

Выбор источников для теоретико-правового осмысления темы обоснован необходимостью разностороннего анализа проблемы, в котором интегрируются уголовно-правовая догматика, криминологические характеристики, международно-юрисдикционные аспекты. В проанализированном массиве литературы авторы применяют разнообразие методологических подходов. Так, формально-догматический преобладает в трудах О.С. Капинус [2], В.В. Полякова [6]. Эти авторы сфокусированы на проблемах квалификации деяний, адаптации классических институтов уголовного права. Криминологический и виктимологический ракурсы рассмотрения реализованы в исследованиях А.В. Майорова [5], В.Г. Романовского [8], Е.З. Сидоровой, Е.Г. Усова [9, 10]. При этом дается характеристика детерминантам киберпреступности и профилям ее участников. В свою очередь, компаративистский и международно-институциональный подходы задействуют М.В. Кардашевская [3], В.А. Кислухин [4], А.С. Рахмонов, Д.А. Рахмонзода [7] в целях оценки трансграничного измерения среды. О.Л. Алферов, Е.В. Алферова [1] используют системно-аналитический подход, чтобы обобщить современные ИТ-угрозы. Регионально-компаративный и риск-ориентированный контексты отражены у Ф.А. Асламшозоды, У.Б. Ашурова [11] при оценке опыта стран Центральной Азии (в том числе, Таджикистана) в сфере борьбы с экстремизмом, активно использующим цифровые каналы связи. Международно-институциональный ракурс реализуется К.Д. Давлатзодой [12], детально исследующим межгосударственное правоохранительное взаимодействие в рамках ШОС и ОДКБ по пресечению киберпреступлений. В свою очередь, программно-целевой и макроструктурный подходы применя-

ются Н.А. Кудратовым, Р.Ғ. Назарзодой [13] с целью обоснования модернизации государственной уголовной политики в Республике Таджикистан на среднесрочную перспективу.

По итогам обзора материалов отмечено постепенное смещение научного фокуса от восприятия технологий лишь как инструмента к осмыслению цифрового пространства как самостоятельной среды обитания, которая инициирует новые составы преступлений.

В методологическую основу написания статьи легли формально-юридический, системно-структурный, сравнительно-правовой анализы. Их применение аргументировано необходимостью корректной экстраполяции классических конструкций уголовного права на новые виртуальные реалии, объективного сопоставления полярных доктринальных трактовок, выработки единого теоретического «фундамента» для закрепления статуса цифрового пространства в системе признаков объективной стороны преступления.

Результаты и обсуждение

Объективная сторона преступления образует «фундамент» для правильной уголовно-правовой квалификации. Разумно предположить, что проникновение digital-технологий в преступную деятельность видоизменяет саму структуру объективных признаков. Способ совершения деяний обогащается алгоритмическими инструментами. Орудия и средства приобретают нематериальный характер, трансформируясь во вредоносное программное обеспечение, скрипты, фишинговые ресурсы [2, 8].

В сопоставлении с более ранними подходами, где место совершения преступления рассматривалось, главным образом, как участок физической территории, современная парадигма требует признания виртуальной среды особым топологическим объектом. По своей природе цифровое пространство – это информационно-телекоммуникационная среда, которая не имеет четких государственных границ, но обладает определенной архитектурой (серверы, провайдеры, конечные узлы). При совершении, например, компьютерного мошенничества местом совершения деяния служит не столько физическое нахождение злоумышленника в момент клика, сколько само digital-пространство, где происходят неправомерная модификация информации и движение электронных средств.

В целях обеспечения большей наглядности концептуальных изменений предлагается рассмотреть процесс трансформации признаков в табличном виде (см. таблицу 1).

Таблица 1

Эволюция признаков объективной стороны в условиях цифровизации (составлено на основе [1, 5, 6, 9, 10])

Аспект	Традиционное (физическое) понимание	Интерпретация в контексте цифрового пространства
Общественно опасное деяние	Физическое воздействие на потерпевшего или материальный предмет	Информационное воздействие (ввод, удаление, модификация цифровых данных)
Место совершения	Конкретная географическая локация (адрес, помещение, участок местности и т. д.)	Информационно-телекоммуникационная сеть, IP-адрес, сервер, виртуальная платформа
Время совершения	Хронологический отрезок совершения физических действий	Время инициации алгоритма; момент синхронизации или отложенного запуска вредоносного кода
Орудия, средства	Физические предметы (оружие, инструменты, технические устройства)	Вредоносные программы, эксплойты, ботнеты, социальная инженерия
Способ совершения	Тайное либо открытое изъятие, обман, применение физического насилия	Обход систем защиты, фишинг, подмена данных, DDoS-атаки

Приведенная выше информация показывает, что цифровое пространство выступает не просто в роли фона, а как активная среда. Она задает параметры для всех остальных факультативных признаков, интегрируя их в единый механизм причинения вреда.

Анализ проблемы в межгосударственном контексте представляет особый научный интерес. Россия и Республика Таджикистан тесно сотрудничают в сфере противодействия транснациональной преступности. Оба государства деятельно внедряют информационные технологии в социально-экономические процессы. Системы уголовного права обеих стран имеют общие исторические корни. Однако пути адаптации их законодательства к digital-угрозам характеризуются определенными различиями.

Так, в Российской Федерации наблюдается тенденция к глубокой детализации «цифровых» составов. Уголовный кодекс РФ регулярно пополняется новыми нормами. К примеру, выделено специфическое мошенничество в области компьютерной информации (статья 159.6 УК РФ). Законодатель четко фиксирует использование электронных средств платежа и информационно-телекоммуникационных сетей в качестве квалифицирующих признаков для многих традиционных деяний [1, 6, 9].

Республика Таджикистан также располагает развитым уголовным законодательством в анализируемой сфере. В главе 28 УК РТ закреплена ответственность за преступления против компьютерной информации. Между тем, правоприменительная практика чаще сталкивается с вызовами, которые сопряжены с действием уголовного закона в пространстве. Террористические и экстремистские организации зачастую используют digital-пространство для вербовки граждан Таджикистана, находясь при этом за пределами юрисдикции республики. В связи с этим таджикские правоведы акцентируют внимание на необходимости расширительного толкования «места совершения преступления» с целью защиты национальных интересов от трансграничных сетевых посягательств [3, 4, 7, 11-13] (таблица 2).

Таблица 2

Сравнительный анализ регулирования цифрового пространства в УК РФ и УК РТ (составлено на основе [1, 3, 4, 6, 7, 9, 11-13])

Критерий сопоставления	Российская Федерация (УК РФ)	Республика Таджикистан (УК РТ)
Наличие специализированной главы	Имеется: глава 28	Присутствует: глава 28
Спецификация цифровых хищений	Выделены отдельные статьи (ст. 159.3, 159.6 – компьютерное мошенничество)	Хищения рассматриваются в рамках общих норм с учетом технического способа совершения
Трактовка места преступления	Формируется практика признания местом преступления нахождения сервера или потерпевшего	Доминирует привязка к физическому месту нахождения лица или наступления последствий
Учет транснационального киберэкстремизма	Разветвленная система норм, в которой учитывается использование сети Интернет как отягчающее обстоятельство	Акцент на противодействие вербовке через цифровое пространство (религиозный экстремизм)

Исходя из представленных данных, подытожим, что Россия идет по пути казуистической дифференциации уголовной ответственности за киберпреступления. Таджикистан же отдает предпочтение сохранению стабильности кодекса, адаптируя общие нормы через призму судебного толкования, правоприменения.

Далее предлагается обозначить конкретные рекомендации по усовершенствованию уголовного законодательства и правоприменительной практики.

Так, целесообразно нормативно закрепить в Общей части уголовного законодательства понятие «цифровое место совершения преступления». Назначение описываемой меры состоит в преодолении коллизий при определении территориальной подсудности и юрисдикции. Новизна подхода выражена в отказе от исключительной географической привязки в пользу смешанной модели. Местом совершения киберпреступления должен признаваться не только физический адрес нахождения преступника, но и виртуальная инфраструктура, где произошло вмешательство (целевой сервер, облачное хранилище). В итоге устранится проблема квалификации действий хакеров, которые

используют многоуровневые сети VPN для сокрытия своего действительного местоположения.

Помимо этого, разумно ввести в доктрину категорию «цифровое средство совершения преступления». Использование алгоритмов машинного обучения для подбора паролей либо создания фишинговых текстов не укладывается в классическое понимание орудий. Законодательное закрепление этого термина поможет правоохранительным органам более эффективно производить арест виртуальных активов и вредоносной инфраструктуры, выступающих в роли средств совершения деяния. Характеризуемый шаг нацелен на разрушение экономических основ организованной киберпреступности.

Заключение

Цифровое пространство объективно преобразовалось из технологического явления в самостоятельную уголовно-правовую категорию. Оно оказывает определяющее влияние на систему признаков объективной стороны. Классическая триада «место, время, обстановка» в контексте киберпреступности приобретает принципиально новые, информационно-цифровые характеристики. Это обусловливает потребность в адаптации уголовно-правовой догматики. Дематериализация преступного деяния и пространственно-временной разрыв между посягательством и результатом более не позволяют правоприменителям опираться исключительно на физические критерии объективной реальности.

Проведенный сравнительно-правовой анализ опыта Российской Федерации и Республики Таджикистан помог выделить как общие интеграционные тенденции, так и специфические национальные подходы к уголовно-правовой охране общественных отношений в условиях технологической сингулярности. В то время, как Россия детализирует Особенную часть профильными нормами о мошенничестве, Таджикистан сталкивается со сложными вызовами пространственной юрисдикции при противодействии сетевому экстремизму.

Сформулированные в статье авторские рекомендации, в частности, предложение о легальном закреплении концепции «цифрового места совершения преступления», обладают потенциалом практического применения. Их имплементация в законодательство способна существенно оптимизировать процесс квалификации дистанционных хищений и распределенных сетевых атак, предупреждая юрисдикционные конфликты.

В дальнейшем исследовании проблематики предлагается сосредоточить внимание на вопросах соучастия в digital-среде, а также на разработке унифицированных международных стандартов оценки объективной стороны транснациональных компьютерных деликтов.

Литература

1. Алферов О.Л., Алферова Е.В. Информационные технологии и «цифровая» преступность (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4. Государство и право: реферативный журнал. – 2024. – №. 4. – С. 83-96.

2. Капинус О.С. Цифровизация преступности и уголовное право // Baikal Research Journal. – 2022. – Т. 13. – №. 1. – С. 22-28.

3. Кардашевская М.В. Организация взаимодействия правоохранительных органов России и Таджикистана в борьбе с преступностью // Известия Тульского государственного университета. Экономические и юридические науки. – 2025. – №. 3. – С. 9-17.

4. Кислухин В.А. Проблема трансграничной преступности в сфере высоких технологий и роль органов внутренних дел России, милиции Республики Таджикистан и полиции государств союза БЕНИЛЮКС в борьбе с этим деструктивным явлением // Юридический вестник. – 2022. – № 1 (9). – С. 83-90.

5. Майоров А.В. Виктимология цифровой преступности: концепция научного направления // Виктимология. – 2024. – Т. 11. – №. 1. – С. 7-12.

6. Поляков В.В. Преступления, совершаемые с использованием цифровых технологий: вопросы квалификации // Уголовное право. – 2025. – № 5 (177). – С. 16-26.

7. Рахмонов А.С., Рахмонзода Д.А. Современная информационная политика Республики Таджикистан по противодействию информационным угрозам, киберпреступности и киберугрозам: тенденции и реалии // Стратегические ориентиры развития Центральной Азии: история, тренды и перспективы. Сборник научных статей международного научно-образовательного форума. – Екатеринбург: 2021. – С. 234-241.

8. Романовский В.Г. Цифровая преступность: понятие, криминологические особенности, проблемы противодействия // Известия высших учебных заведений. Поволжский регион. Общественные науки. – 2024. – №. 3 (71). – С. 123-136.

9. Сидорова Е.З. Современные криминологические характеристики цифровой преступности (цифровой преступник и его жертва) // Сибирский юридический вестник. – 2023. – №. 3 (102). – С. 70-78.

10. Сидорова Е.З., Усов Е.Г. Цифровая преступность: понятие, криминологическая характеристика, предупреждение (часть 2) // Сибирский юридический вестник. – 2024. – №. 3 (106). – С. 81-87.

11. Асламшозода Ф.А., Ашуров У.Б. Таҷрибаи милии кишварҳои Осиёи Марказӣ дар самти мубориза бо ифротгароӣ // Международные отношения и безопасность. – 2025. – № 2 (14). – С. 79-96.

12. Давлатзода К.Д. Ҳамкориҳои минтақавии Ҷумҳурии Тоҷикистон дар самти мубориза бо киберҷиноятҳо: дар мисоли Созмони Ҳамкории Шанхай ва Созмони Паймони Амнияти Дастаҷамъӣ // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2023. – № 6. –С. 232-237.

13. Қудратов Н.А., Назарзода Р.Ғ. Зарурияти қабули Барномаи нави давлатии муқовимат ба ҷинояткорӣ дар Ҷумҳурии Тоҷикистон барои солҳои 2026-2030 // Актуальные проблемы современного государства, общества и права. – 2026. – № 1 (9). – С. 6-19.

Digital space in the system of signs of the objective side of the crime: theoretical and legal understanding

Nurmatov A.A.
Krasnodar University of the Ministry of Internal Affairs of Russia

The rapid dematerialization of criminal acts has exposed a dogmatic crisis in modern criminal law. Strict geographical reference comes into direct conceptual contradiction with the decentralized, extraterritorial "architecture" of cybercrime. Apparently, the traditional physical coordinates of place and time have irreversibly lost their universality. They have ceased to meet the demands of practice. The purpose of the article is to form an updated theoretical and legal paradigm of the objective side of the crime, where the digital environment is studied not as a technical background, but as an independent topological object. Notably, a comparative analysis of law enforcement has highlighted diametrically different strategies for adapting to these challenges. If the Russian legislator leans towards a casuistic fragmentation of norms on digital fraud, then Tajik practice attempts to broadly interpret classical compositions to counter transnational network extremism, but regularly runs into a jurisdictional dead end. Based on the above, the author concludes that the transition to a hybrid model for assessing objective signs, combining physical and virtual criteria, is inevitable. The presented material has applied value for investigative workers, the judiciary, and researchers who are engaged in designing adequate criminal policy in the era of technological singularity.

Keywords: virtual environment, cybercrime, place of crime, objective side of crime, Republic of Tajikistan, Russian Federation, comparative law, digital space.

References

1. Alferov O.L., Alferova E.V. Information technologies and "digital" crime (Review) // Social Sciences and Humanities. Domestic and Foreign Literature. Ser. 4. State and Law: Abstract Journal. 2024. No. 4. Pp. 83-96.
2. Kapinus O.S. Digitalization of crime and criminal law // Baikal Research Journal. 2022. Vol. 13. No. 1. Pp. 22-28.
3. Kardashevskaya M.V. Organization of interaction between law enforcement agencies of Russia and Tajikistan in the fight against crime // News of Tula State University. Economic and Legal Sciences. 2025. No. 3. Pp. 9-17.
4. Kislukhin V.A. The problem of cross-border crime in the field of high technologies and the role of the internal affairs bodies of Russia, the police of the Republic of Tajikistan and the police of the BENELUX states in the fight against this destructive phenomenon // Legal Bulletin. 2022. No. 1 (9). Pp. 83-90.
5. Mayorov A.V. Victimology of digital crime: concept of a scientific direction // Victimology. 2024. Vol. 11. No. 1. Pp. 7-12.
6. Polyakov V.V. Crimes committed using digital technologies: issues of qualification // Criminal Law. 2025. No. 5 (177). Pp. 16-26.

7. Rakhmonov A.S., Rakhmonzoda D.A. Modern information policy of the Republic of Tajikistan on countering information threats, cybercrime and cyber threats: trends and realities // Strategic directions for the development of Central Asia: history, trends and prospects. Collection of scientific articles of the international scientific and educational forum. Yekaterinburg: 2021. Pp. 234-241.
8. Romanovsky V.G. Digital crime: concept, criminological features, problems of counteraction // News of Higher Educational Institutions. Volga Region. Social Sciences. 2024. No. 3 (71). Pp. 123-136.
9. Sidorova E.Z. Modern criminological characteristics of digital crime (digital criminal and his victim) // Siberian Legal Bulletin. 2023. No. 3 (102). Pp. 70-78.
10. Sidorova E.Z., Usov E.G. Digital crime: concept, criminological characteristics, prevention (part 2) // Siberian Legal Bulletin. 2024. No. 3 (106). Pp. 81-87.
11. Aslamshozoda F.A., Ashurov U.B. National experience of Central Asian countries in combating extremism // International Relations and Security. – 2025. – No. 2 (14). – Pp. 79-96.
12. Davlatzoda K.D. Regional cooperation of the Republic of Tajikistan in combating cybercrime: the example of the Shanghai Cooperation Organisation and the Collective Security Treaty Organisation // Bulletin of the National University of Tajikistan. Series of Socio-Economic and Social Sciences. – 2023. – No. 6. – Pp. 232-237.
13. Qudratov N.A., Nazarzoda R.G. The necessity of adopting a new state program for combating crime in the Republic of Tajikistan for 2026-2030 // Current Issues of the Modern State, Society and Law. – 2026. – No. 1 (9). – Pp. 6-19.