Танов Нариман Рафикович[1]
Аспирант 2 курса Института аспирантуры и докторантуры
Московского государственного университета
им. О.Е. Кутафина (МГЮА)
tanovs98@mail.ru

УГОЛОВНО-ПРАВОВАЯ ЮРИСДИКЦИЯ В ОТНОШЕНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В КИБЕРПРОСТРАНСТВЕ

Аннотация. Правоохранительная деятельность специализированных органов России становится все более непростой с учетом специфики, которая ежегодно выводит совершаемые преступления на новый уровень — в киберпространство. В этой связи расследование уголовно-наказуемых деяний также усложняется, что наталкивает законодателей и правоведов все чаще на мысль о необходимости реформы взаимодействия правоохранительных органов с целью обеспечения безопасности физических и юридических лиц, а также их собственности и данных в киберпространстве вне зависимости от юрисдикции. Более того, приоритетной задачей становится не только реформирование законодательства, но и обеспечение правоохранительных органов необходимыми навыками, а также специалистами и техникой, которые бы значительно упрощали их деятельность по упреждению, пресечению и расследованию преступлений, совершаемых в киберпространстве, а также с использованием кибертехнологий.

Ключевые слова: правоохранительные органы, преступления, киберпространство, киберправо, уголовно-правовая юрисдикция.

Tanov Nariman Rafikovich
PhD student of the 2nd grade of Institute of PhD and Doctoral Studies
Kutafin Moscow State Law University (MSAL)

CRIMINAL JURISDICTION OVER CRIMES COMMITTED IN CYBERSPACE

Abstract. The law enforcement activities of specialized bodies in Russia are becoming more and more difficult, taking into account the specifics that annually take crimes committed to a new level — into cyberspace. In this regard, the investigation of criminal offenses is also becoming more complicated, which prompts legislators and legal scholars increasingly to think about the need to reform the interaction of law en-

[1] Научный руководитель: Кудинов Владимир Владимирович, профессор кафедры организации судебной и прокурорско-следственной деятельности Московского государственного юридического университета им. О.Е. Кутафина (МГЮА).

forcement agencies in order to ensure the safety of individuals and legal entities, as well as their property and data in cyberspace, regardless of jurisdiction. Moreover, the priority task is not only to reform legislation, but also to provide law enforcement agencies with the necessary skills, as well as specialists and equipment that would significantly simplify their activities in preventing, suppressing and investigating crimes committed in cyberspace, as well as using cyber technologies.

Key words: law enforcement agencies, crime, cyberspace, cyber law, criminal law jurisdiction.

На сегодняшний день проблема киберпреступлений и их юрисдикции на государственном и международном уровнях остаются одной из наиболее насущных. На данный вид преступлений распространяется две формы юрисдикции — предписания и принуждения. В первом варианте государство посредством изданных законов и норм поведения старается не допустить совершения преступлений, но лишь без использования на то принудительных мер. Во втором оно создает специальные правоохранительные и силовые органы, на которые накладывает обязанность по принуждению общества и его отдельных лиц соблюдать установленные им нормы права и поведения. Как справедливо указывают в своей работе Исаенко В.Н. и Ищенко П.П., долгое время данная уголовно-правовая юрисдикция распространялась лишь на всю территорию государства (официальные представительства за рубежом, воздушное пространство, территориальные воды и континентальный шельф, включенные в государственные границы)[1]. Развитие международного права и сотрудничества путем создания организаций глобального значения ООН, ОБСЕ и др., на площадках которых стали разрабатываться и утверждаться международные договоры, в том числе уголовно-правового характера, подразумевающие как совместное участие государств в раскрытии и упреждении преступных деяний, так и утверждение правоохранительных ведомств мирового и регионального масштабов, что решало бы вопросы юрисдикции (Интерпол, Европол, Америпол).

С появлением информационно-коммуникационных технологий, а также сети Интернет, личность, общество, государственные

[1] Правоохранительные органы: учебник для вузов / В.Н. Исаенко, П.П. Ищенко [и др.]. Москва: Изд-во Юрайт, 2024. С 253.

структуры и само государство становятся полноправными субъектами мировой коммуникации. Это порождает появление киберпространства. Термин «киберпространство» в отечественном законодательстве был впервые использован в Проекте Концепции Стратегии кибербезопасности Российской Федерации, опубликованный Советом Федерации в 2013 году. В нем указывалось, что киберпространство является сферой деятельности в информационном пространстве, образованной совокупностью информационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства).

Но киберпространство стало площадкой для киберпреступлений задолго до формулировки данного термина. Со второй половины 90-х годов, киберпространство стало глобальным явлением, участниками которого на сегодняшний день является большинство стран мира, международные организации и транснациональные компании. С этого периода становится невозможным определить, чьим владением является киберпространство, носит ли оно внутри себя границы как в реальном мире, и где начинается юрисдикция одного государства, и заканчивается юрисдикция другого. Данную проблему пытались решить путем подписания Будапештской конвенции, соглашения Таллиннского руководства, а также в рамках Международного союза электросвязи при ООН и Центра Интерпола по инновациям, но ввиду различного рода причин не смогли включить в свое участие значительное количество стран. В данных документах раскрывалось понятие кибератак, а также право государств, на которые они нацелены, принимать ответные меры вне зависимости от локации субъекта преступления и профилактической обороны — упреждающих мер в случае возможного нападения.

Ключевым и сложно разрешимым вопросом остается возможность привлечения к уголовной ответственности лиц, виновных в совершении киберпреступлений. Многие сотрудники органов прокуратуры, а также правоведы, среди которых можно выделить Капинус О.С. полагают, что открытой остается и тема о том, что объ-

ект и субъект преступления, а также его предмет могут никак не соприкасаться в реальной жизни в случае совершения самого преступления в киберпространстве[1]. Вполне вероятно, что их будет объединять лишь обстановка, интернет-пространство, которое не имеет межгосударственных границ, что затрудняет раскрытие киберпреступлений. Этим активно пользуются преступники при совершении противоправных деяний, что подтверждает статистика, согласно которой количество преступлений, в области информационно-коммуникационных технологий растет с каждым годом, а процент раскрытых дел остается на низком уровне. Только в России, по данным Генпрокуратуры РФ, за неполный 2019 год было зарегистрировано 180 153 киберпреступлений, что за последние 6 лет характеризует их десятикратный рост (в 2014 году — 44 000).

Более того, если иностранный гражданин осуществлял свою преступную деятельность вне пределов России и находится на территории РФ, то он может быть выдан иностранному государству для привлечения к уголовной ответственности или отбывания наказания в соответствии с международным договором РФ. Данная позиция соответствует изложенным ст. 11-13 УК РФ принципам действия Уголовного закона России в отношении лиц, совершивших преступление.

Как справедливо отмечает в своей работе С.С. Витвицкая, в поле зрения правоохранительных органов мира также подпадает и проблема существования «даркнета» — теневой сети интернета, в которой заключаются сделки по реализации и совершению преступлений в киберпространстве (незаконная продажа органов, оружия, наркотических средств)[2]. Частью даркнета являются давно известные правоохранительным службам браузеры и порталы TOP, Гидра, Sphere. Невозможность отследить участников преступления происходит ввиду использования ими криптовалюты и анонимай-

[1] Прокурорский надзор. Общая часть: учебник для вузов / О.С. Капинус [и др.]. Москва: Изд-во Юрайт, 2024. С. 82.

[2] Витвицкая С.С., Витвицкий А.А., Исакова Ю.И. Киберпреступления: понятие, классификация, международное противодействие // Правовой порядок и правовые ценности. Право. 2023. Т. 1. № 1. С. 20.

зеров. Криптовалюта по своему предназначению является расчетной единицей в киберпространстве, не зависящей от механизма реально существующих рыночных отношений, посредством которой в виртуальной реальности происходят расчеты между участниками, особенно если это касается преступлений («отмывание» денежных средств, оплата предоставляемых незаконных услуг, мошенничество). Ее существование, а также отсутствие нормативно-правовой базы ее регулирования, за неимением привязки к определенному государству или организации, вызывают споры в законодательной среде. На сегодняшний день отечественной практике уголовного судопроизводства уже известны уголовные дела о преступлениях, в которых криптовалюта фигурировала как средство оплаты или расчета с наркодилерами за предоставленные ими услуги. Подтверждением этому служат вступившие в законную силу следующие судебные решения: приговор Ленинского районного суда г. Челябинска от 06.07.16 (дело номер № 1-311/2016); приговор Йошкар-Олинского городского суда Республики Марий Эл 01.06.17 (дело № 1-233/2017); приговор Вологодского городского суда Вологодской области от 15.05.17 (дело № 1-461/2017). В случае с такого рода преступлениями, где криптовалюта выступает как средство расчета, необходимо на законодательном уровне либо закрепить ее существование, равно как и владение, либо криминализировать пользование ею.

Попытка борьбы с даркнетом будет оставаться невозможной до тех пор, пока он не будет признан всеобщей зоной ответственности. Одним из способов вывода и обнаружения значительного количества противоправных деяний из теневого интернета станет внедрение государствами системы блокчейн. Особенностью данной системы является высокий уровень защиты обладающей ею объекта от вирусных атак, взломов и незаконной разблокировки, ввиду большого количества содержащихся в ее составе частей, блоков, которые имеют свой уникальный код, а также информации о предыдущем блоке, для взлома которых потребуется одновременное воздействия на все блоки, коих является бесчисленное множество, что делает попытку сбоя системы невозможной.

Использование блокчейн-технологии позволит снизить количество совершаемых киберпреступлений: программа полностью защитит ИКТ от хакерских атак и взломов, сделает денежный оборот и переводы прозрачными, позволит избежать мошенничества при финансовых операциях.

В российских реалиях контроль и реализацию системы блокчейн возможно возложить на ведомства с высокой технологической оснащенностью. Так за внедрение системы блокчейн в государственные структуры и электронное правительство может взяться отдел «К» ФСБ, в то время как внедрение этой же системы в финансовые организации и негосударственный сектор отдел «К» МВД, что разграничит сферы деятельности отечественных ведомств в киберпространстве при проведении реформы[1].

Поддерживая мнение Кулагиной О.Н., следует отметить, что с законодательной точки зрения в России необходимо дополнить и Уголовный Кодекс новыми статьями, которые станут частью главы 28 УК РФ, а также углубить по своему смыслу и полноте уже существующие[2]. Требуется ввести уголовную ответственность за создание, распространение и использование вирусных и вредоносных программ, которые могут нанести ущерб государству, обществу и личности. В зависимости от тяжести последствий или общественной опасности предлагается в виде меры наказания ввести штраф, право занимать определенные должности и заниматься определенной деятельностью, лишение свободы с конфискацией имущества. Неуместно предлагать арест, ограничение свободы и различные виды работ ввиду высокой доли вероятности совершения рецидива со стороны преступника. Также надо расширить статью 174 УК РФ об «отмывании» денежных средств и прописать в ней роль криптовалюты в легализации денежных средств как одного из пунктов

[1] Тимофеев А.В., Комолов А.А. Киберпреступность как социальная угроза и объект правового регулирования // Современные философские исследования. Право. 2021. Т. 1, № 1. С. 96.

[2] Кулагина О.Н., Милова К.А. Деятельность органов прокуратуры по противодействию преступности в сети Интернет // Вестник Пензенского государственного университета. Экономика, социология и право. 2021.Т. 2, № 4. С. 75.

статьи. Законотворческую деятельность необходимо возложить на Федеральное Собрание РФ.

Предлагая реформу процессуального права, следует отметить, что часть доказательств в нем предстает в суде в электронном виде (записи с камер наблюдения, документы с электронной подписью или печатью), подделка которых не составит труда заинтересованной в этом одной из сторон конфликта. В связи с этим, ввиду необходимости более строгой оценки доказательств в ходе судебного разбирательства по делу, необходимо ввести дополнительный процессуальный контроль за качеством собранных доказательств, представляющих собой улики информационного происхождения (наделение органов дознания и предварительного расследованию обязанностью по проведению во всех без исключения случаях назначения и проведения по делам криминалистических экспертиз на предмет выяснения вопроса о том, не вносились ли доказательства, имеющие информационное происхождение какие-либо изменения). При этом, оценка допустимости указанного вида доказательств может быть произведена только после экспертного заключения.

Еще одним решением проблемы является передача части полномочий на проведение дознания и следственных действий Росгвардии. Находящиеся в ее сфере деятельности противодействие терроризму и экстремизму, государственный надзор, вневедомственная охрана и создание банка данных дают возможность участвовать в противодействии киберпреступлениям. Ее разветвленная организационная сеть позволит действовать на всех уровнях государственной власти и интересов, что выразится в координации центра своих региональных и местных отделений в проведении следственных мероприятий. Но во избежание проблем юрисдикции с другими ведомствами необходимо законодательно закрепить полномочия Росгвардии в УПК (ст. ст. 40, 151, 157) и федеральных законах.

Таким образом, можно с уверенностью заявить о том, что проблема как киберпреступлений, так и их юрисдикции на государственном и мировом уровне остается открытой, во-первых, из-за технологического прогресса; во-вторых, из-за отсутствия мировой

стандартизации понятия киберпреступления и единого договора о противодействии данному явлению; в-третьих, из-за недостаточной информационной и правовой грамотности самого населения; в-четвертых, из-за политических противоречий и экономических трудностей, тормозящих решение данных вопросов.

СПИСОК ЛИТЕРАТУРЫ

1. Витвицкая С.С., Витвицкий А.А., Исакова Ю.И. Киберпреступления: понятие, классификация, международное противодействие // Правовой порядок и правовые ценности. Право. — 2023. — Т. 1, № 1. — С. 18-27.
2. Евдокимов К.Н., Хобонкова К.В. К проблеме совершенствования международного сотрудничества в сфере противодействия киберпреступности // сибирский юридический вестник. Право. — 2022. — Т. 2, № 3. — С. 90-96.
3. Кулагина О.Н., Милова К.А. Деятельность органов прокуратуры по противодействию преступности в сети Интернет // Вестник Пензенского государственного университета. Экономика, социология и право. — 2021. — Т. 2, № 4. — С. 75-78.
4. Правоохранительные органы: учебник для вузов / В.Н. Исаенко, П.П. Ищенко [и др.]. — Москва: Издательство Юрайт, 2024. — 312 с.
5. Прокурорский надзор. Общая часть: учебник для вузов / О. С. Капинус [и др.]. — Москва: Издательство Юрайт, 2024. — 231 с.
6. Тимофеев А.В., Комолов А.А. Киберпреступность как социальная угроза и объект правового регулирования // Современные философские исследования. Право. — 2021. — Т. 1, № 1. — С. 95-101.

Тарханова Александра Владимировна[1]

Студент 2 курса Института государства и права
Тюменского государственного университета
stud0000274404@study.utmn.ru

ЦИФРОВЫЕ ПРАВА ЧЕЛОВЕКА: ПОДХОДЫ К ПОНИМАНИЮ И РАЗВИТИЮ

Аннотация. На сегодняшний день цифровизация оказывает существенное влияние практически на все сферы человеческой жизни. Современные процессы, которые неуклонно влияют на социальные отношения, приводят к эво-

[1] Научный руководитель: Некрасов Михаил Александрович, доцент кафедры теоретических и публично-правовых дисциплин Тюменского государственного университета.