ZAMONAVIY HUQUQSHUNOSLIKNING AKTUAL MUAMMOLARI

XXIII-RESPUBLIKA ILMIY-AMALIY KONFERENSIYA

YAKUNLARI BO'YICHA ILMIY ISHLAR TO'PLAMI

Issue - 3(2026) Available at www.uznauka.uz

ЮРИСДИКЦИОННЫЕ КОЛЛИЗИИ В ТРАНСНАЦИОНАЛЬНЫХ КИБЕРПРЕСТУПЛЕНИЯХ: ПРОБЛЕМЫ ЭКСТЕРРИТОРИАЛЬНОГО ПРЕСЛЕДОВАНИЯ

Атаханов Ш.
Независимый соискатель

Аннотация: *в статье исследуются юрисдикционные коллизии, возникающие при расследовании и уголовном преследовании транснациональных киберпреступлений. Анализируется трансформация классических принципов уголовной юрисдикции в условиях цифровизации и экстерриториального характера противоправных деяний. Особое внимание уделяется проблемам конкуренции юрисдикций, экстрадиции, двойной криминализации, принципу ne bis in idem, а также вопросам трансграничного доступа к электронным доказательствам и соотношению экстерриториального преследования с принципом государственного суверенитета. Делается вывод о необходимости совершенствования международных механизмов координации и унификации стандартов сотрудничества для предотвращения правовых конфликтов и обеспечения баланса между эффективностью борьбы с киберпреступностью и соблюдением международно-правовых гарантий.*

Ключевые слова: *киберпреступность, транснациональные преступления, уголовная юрисдикция, экстерриториальность, конкуренция юрисдикций, экстрадиция, двойная криминализация, электронные доказательства, государственный суверенитет, международное сотрудничество.*

Юрисдикционные коллизии в транснациональных киберпреступлениях представляют собой одну из наиболее сложных и дискуссионных проблем современного международного права. Развитие цифровых технологий и глобальный характер сетевой инфраструктуры привели к тому, что преступления, совершаемые в киберпространстве, практически всегда выходят за пределы одной государственной территории. Сервер может находиться в одном государстве, потерпевший — в другом, а предполагаемый преступник — в третьем [1]. В результате возникает множественная конкуренция юрисдикций, что ставит под сомнение традиционные территориальные подходы к осуществлению уголовного преследования.

Классические принципы уголовной юрисдикции сформированы на основе территориального суверенитета государства. В соответствии с общепризнанными нормами международного права государство осуществляет уголовную юрисдикцию в пределах своей территории [2]. Однако транснациональные киберпреступления подрывают данную модель, поскольку деяние может быть начато в одной юрисдикции, реализовано через инфраструктуру другой и причинить вред в третьей. В этих условиях государства стремятся расширять основания для осуществления экстерриториальной юрисдикции, опираясь на принципы активной и пассивной персональной юрисдикции, а также принцип защиты национальных интересов [3].

Ситуация осложняется тем, что различные государства по-разному определяют пределы допустимого экстерриториального преследования. Некоторые национальные законодательства предусматривают возможность

привлечения к ответственности лиц, совершивших киберпреступление за рубежом, если его последствия затронули интересы данного государства или его граждан. Другие государства придерживаются более ограничительного подхода, связывая юрисдикцию исключительно с местом совершения деяния. В результате одно и то же поведение может подпадать под уголовную юрисдикцию сразу нескольких стран, что создаёт риск двойного преследования или, напротив, безнаказанности при отсутствии координации [4].

Особое значение в данной сфере имеет Конвенция о киберпреступности, которая закрепляет обязательство государств устанавливать юрисдикцию в случаях, когда преступление совершено на их территории, на борту судна или воздушного судна под их флагом, либо гражданином данного государства. Вместе с тем Конвенция предусматривает необходимость консультаций между государствами в случае совпадения юрисдикций. Однако данный механизм носит координационный, а не императивный характер, что не исключает возникновения конфликтов [5].

Юрисдикционные коллизии усиливаются в контексте применения экстерриториальных мер принуждения, включая запросы о раскрытии электронных доказательств, замораживании цифровых активов или удалённом доступе к серверам, расположенным за пределами территории государства. Подобные действия могут рассматриваться как вмешательство во внутренние дела другого государства и нарушение принципа невмешательства, закреплённого в Уставе Организация Объединённых Наций. Вопрос о допустимости прямого трансграничного доступа к данным

остаётся одним из наиболее дискуссионных как в доктрине, так и в международной практике [6].

Отдельную проблему составляет экстрадиция лиц, обвиняемых в совершении киберпреступлений. Нередко государства отказывают в выдаче своих граждан либо ссылаются на отсутствие двойной криминализации. Различия в национальных составах преступлений, особенно в сфере информационных правонарушений, могут препятствовать реализации международного сотрудничества [7]. Кроме того, в некоторых случаях государства отказывают в экстрадиции, если существует риск нарушения прав человека, включая запрет на пытки или несправедливое судебное разбирательство.

Юрисдикционные коллизии также затрагивают принцип ne bis in idem, предполагающий недопустимость повторного привлечения к ответственности за одно и то же деяние [8]. В условиях отсутствия универсального механизма распределения юрисдикции существует риск параллельных расследований и конкурирующих судебных процессов. Это поднимает вопрос о необходимости более чётких международных процедур координации и определения приоритетной юрисдикции, исходя из таких критериев, как место причинения основного вреда, гражданство обвиняемого или наиболее тесная связь преступления с конкретным государством [9].

Дополнительную сложность создаёт феномен «облачной» инфраструктуры и распределённого хранения данных. В ряде случаев невозможно точно определить территорию, на которой фактически находились данные в момент совершения преступления [10]. Это ставит под

сомнение применимость традиционного территориального принципа и стимулирует развитие доктрины «объективной территориальности», согласно которой государство вправе осуществлять юрисдикцию, если существенные последствия деяния наступили на его территории.

Решение проблемы юрисдикционных коллизий требует комплексного подхода. Необходимы более детализированные международные нормы о координации расследований, прозрачные механизмы обмена информацией и развитие доверия между государствами [11]. Новый универсальный договор ООН по киберпреступности потенциально может сыграть важную роль в формировании таких механизмов, если будет обеспечен баланс между эффективностью уголовного преследования и уважением суверенитета государств.

Таким образом, юрисдикционные коллизии в сфере транснациональных киберпреступлений отражают структурный кризис традиционной территориальной модели уголовной юрисдикции [12]. Экстерриториальное преследование становится неизбежным инструментом борьбы с цифровой преступностью, однако его применение должно быть ограничено принципами международного права, уважением прав человека и координацией между государствами. В противном случае расширение юрисдикции может привести к усилению межгосударственных конфликтов и подрыву международного сотрудничества в цифровой сфере.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. ШИРИНДЖОНОВ, Ф. ТРАНСНАЦИОНАЛЬНЫЕ КИБЕР ПРЕСТУПЛЕНИЯ: ПОНЯТИЕ, ПРИЗНАКИ И ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ. *АКАДЕМИЧЕСКИЙ ЮРИДИЧЕСКИЙ ЖУРНАЛ Учредители: Институт философии, политологии и права им. А. Баховаддинова АН Республики Таджикистан*, (4), 155-161.

2. Джансараева, Р. Е., & Куаныш, А. (2012). Борьба с киберпреступлениями: сравнительный анализ законодательства стран СНГ. *Всероссийский криминологический журнал*, (3), 95-99.

3. Протасевич, А. А., & Зверянская, Л. П. (2011). Борьба с киберпреступностью как актуальная задача современной науки. *Всероссийский криминологический журнал*, (3), 28-33.

4. Протасевич, А. А., & Зверянская, Л. П. (2011). Борьба с киберпреступностью как актуальная задача современной науки. *Всероссийский криминологический журнал*, (3), 28-33.

5. Кириленко, В. П., & Алексеев, Г. В. (2021). Киберпреступность и цифровая трансформация. *Теоретическая и прикладная юриспруденция*, (1), 39-53.

6. Абделькарим, Я. А. (2025). Конвенция Организации Объединенных Наций против киберпреступности: имплементация концепции взаимной правовой помощи в цифровую эпоху. *Journal of Digital Technologies and Law*, *3*(4), 543-569.

7. Филимонов, С. А. (2014). Некоторые особенности борьбы с транснациональным компьютерным мошенничеством. *Вопросы управления*, (5 (11)), 236-243.

8. Клевцов, К. К. (2022). МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В БОРЬБЕС КИБЕРПРЕСТУПНОСТЬЮ В КОНТЕКСТЕ ПРОТИВОДЕЙСТВИЯ НОВЫМ ВЫЗОВАМ И УГРОЗАМ. *Вестник Санкт-Петербургского университета. Право*, *13*(3), 678-695.

9. Горелик, И. Б. (2022). Роль международных организаций в процессе противодействия киберпреступности. *Международное право*, (3), 28-41.

10. Шлюндт, Н. Ю., & Чельдиева, З. М. (2016). О НЕКОТОРЫХ АСПЕКТАХ КИБЕРПРЕСТУПНОСТИ В МЕЖДУНАРОДНОМ ПРАВЕ. In *НАУЧНЫЕ ИССЛЕДОВАНИЯ И РАЗРАБОТКИ В ЭПОХУ ГЛОБАЛИЗАЦИИ* (pp. 217-221).

11. Матчанов, А. А., & Закиров, Б. Э. (2022). Роль Интерпола в координации международного сотрудничества в борьбе с киберпреступностью. *Journal of marketing, business and management*, *1*(4), 1-7.

12. Данилова, Н. А., & Кушниренко, С. П. (2005). Международное сотрудничество в противодействии преступлениям в сфере высоких технологий. *Вестник Санкт-Петербургского университета МВД России*, (4), 175-180.