Секция «44.23 Правовые традиции Китая: международное и национальное измерения»

Актуальные вопросы уголовной ответственности за преступления, совершаемые с использованием сети Darknet, по законодательству Китайской Народной Республики

Научный руководитель – Карпенко Людмила Константиновна

Солоненко Кристина Михайловна

Студент (магистр)

Донецкий государственный университет, Юридический факультет, Донецк, Россия

E-mail: Sol-kriis@mail.ru

Сеть Darknet (от англ. «dark» – «тёмный» и «net» – «сеть»), представляющая собой скрытый сегмент информационно-телекоммуникационной сети Интернет, созданный для обеспечения анонимности пользователей, в Китайской Народной Республике начала развиваться с 2010 года. Одним из первых известных теневых онлайн-рынков в сети Darknet был сайт Silk Road, объединяющий доступ через «Tor» и оплату криптовалютой. После его закрытия в 2013 году, отмечает Х. Т. Луонг, появились новые, более совершенные платформы для осуществления преступной деятельности [4; 5-6]. Несмотря на усиление государственного контроля, использование сети Darknet в целях совершения преступлений продолжает являться серьезной проблемой для Китайская Народная Республика. Так, за февраль 2025 года – февраль 2026 года Китайская Народная Республика заняла одно из первых мест среди стран мира по количеству киберпреступлений, около 30% которых осуществляются через платформы Darknet [1].

Законодательную основу борьбы с преступностью в цифровой среде составляет Закон «О сетевой безопасности Китайской Народной Республики» от 1 июня 2017 года [2]. Документ закрепляет комплексный подход к кибербезопасности, уделяя особое внимание защите суверенитета и критически важной информационной инфраструктуры государства. Статьи 21-30 определяют обязанности сетевых операторов по предотвращению несанкционированного доступа и утечки данных, а статья 24 предусматривает идентификацию пользователей для ограничения анонимности в сети Интернет. В то же время, положения Закона не полностью учитывают специфику преступлений в сегменте Darknet. Несмотря на правовые предписания, предусмотренные статьями 27 и 63 (относительно действий, вредящих кибербезопасности), они не охватывают в полной мере особенности скрытого сегмента сети, с помощью которого совершаются такие преступления, как: торговля людьми, оборот порнографических материалов с участием несовершеннолетних и др.

Дж. На и С. Бинг отмечают увеличение в 2025 году роста преступности в цифровой среде ввиду отсутствия правовых норм, направленных на борьбу с осуществлением незаконной деятельности в скрытом сегменте информационно-телекоммуникационной сети Интернет [5; 2]. Так, статьями 285 и 286 Уголовного кодекса Китайской Народной Республики предусмотрена ответственность за незаконное вторжение в компьютерные информационные системы и совершение в отношении них вредоносных действий [3], однако не охватываются составы преступлений, совершаемых посредством использования сети Darknet. Также, следует отметить, применение норм главы 6 «Преступления против общественного порядка и порядка управления» Уголовного кодекса Китайской Народной Республики к лицам, совершающим преступления через сеть Darknet, в настоящее время осложнено противоречиями судебной практики и уголовного законодательства. В том числе, отсутствие на законодательном уровне определения понятия «сети Darknet» затрудняет привлечение к уголовной ответственности лиц, совершающих преступления с её использованием.

Статья 287.2 Уголовного кодекса Китайской Народной Республики устанавливает ответственность за использование компьютера для мошенничества, хищения, взяточничества, нецелевого использования средств, похищения государственной тайны и совершения других преступлений. Однако, сопоставление данного состава с преступлениями, совершаемыми посредством сети Darknet проблематично, поскольку: а) использование компьютера подразумевает деятельность, связанную с заражением вредоносным программным обеспечением; б) преступления в сети Darknet охватывают более широкий спектр деяний, нежели поражение компьютерных систем: кражу персональных данных, организацию кибертерроризма и др.

Таким образом, представляется целесообразным предложить дополнение главы 6 Уголовного кодекса Китайской Народной Республики статьей 287.1 следующего содержания:

«287.1 Незаконное использование информационно-телекоммуникационной сети Интернет и её скрытого сегмента Darknet с целью совершения таких преступлений, как незаконный оборот наркотиков, распространение незаконных товаров и услуг, кибермошенничество, кража личных данных, кибертерроризм и любые иные действия, угрожающие национальной безопасности и общественному порядку, – наказывается . . . ».

На основании вышеизложенного можно сделать следующие выводы. Действующее законодательство Китайской Народной Республики не в полной мере учитывает специфику преступлений, совершаемых посредством сети Darknet, чем и обуславливаются трудности их расследования. Законодатель предусматривает ответственность исключительно за противоправные деяния, совершаемые в открытом информационно-телекоммуникационном пространстве сети Интернет, в то время как сеть Darknet является теневым сегментом. Следовательно, дополнение главы 6 Уголовного кодекса Китайской Народной Республики статьей 278.1, закрепляющей ответственность за незаконное использование информационно-телекоммуникационной сети Интернет и её скрытого сегмента Darknet в целях совершения преступлений, является необходимым шагом для обеспечения защиты прав граждан и национальной безопасности.

Источники и литература

1) Chinese Cyber Attack // Sci-tech-today. URL: https://www.sci-tech-today.com (дата обращения: 26.02.2026).

2) О сетевой безопасности: Закон Китайской Народной Республики (принят на 24-м заседании Постоянного комитета 12-го Всайского собрания народных представителей 7 ноября 2016 года) // Центральное народное правительство Китайской Народной Республики. – URL: https://www.gov.cn/xinwen (дата обращения: 26.02.2026).

3) Уголовный кодекс Китайской Народной Республики (принят Постоянным комитетом Всайсайского собрания народных представителей 1 июля 1979 года) (ред. от 01.03.2024) // Кооперативная сеть уголовного законодательства. URL: http://xingfa.org (дата обращения: 26.02.2026).

4) Luong H.T. Preliminary Findings of the Trends and Patterns of Darknet-Related Criminals in the Last Decade // Social Science Research Network. 2022. Pp. 1-10.

5) Na J., Bing S. International Collaborative Responses to Transnational Cybercrime: how China Strengthen its Capacity to Combat Transnational Cybercrime // International Journal of Forensic Sciences. 2024. Vol. 9. Pp. 1-10.