

системы. В связи с этим национальные правительства должны включить в свои законы меры по контролю за оборотом и употреблением этих постоянно меняющихся веществ и их запрет.

Увеличение незаконных рынков в «Darknet» и онлайн-платформ для продажи лекарственных средств создает новые вызовы для правоохранительных органов, что требует формирования правовой среды, направленной на со-

трудничество международных правоохранительных структур и контроль за действиями онлайн-продавцов наркотиков и криптовалютными транзакциями.

Реализация стратегий охраны общественного здоровья, снижения вреда и основанных на доказательствах методов лечения позволит перейти к более устойчивому и эффективному комплексному подходу в борьбе с наркотиками и психоактивными веществами.

Мельникова Л.Ю.

Сибирский юридический институт МВД России (г. Красноярск)

Анализ конвенции ООН о киберпреступности: риски и вызовы

Вопрос о разработке международного договора о противодействии использованию информационно-коммуникационных технологий в преступных целях поднимается на международной арене достаточно давно. В 2001 году была принята Европейская конвенция против киберпреступности. По сути, данный документ стал первым глобальным договором, который был направлен на международное сотрудничество против преступлений в киберпространстве. Существенным достижением этого международного соглашения, безусловно, являлось установление глобального стандарта уголовной ответственности за киберпреступления. Однако Конвенция содержит ряд недостатков, один из которых послужил причиной отказа от подписания данного документа Российской Федерацией.

Европейская конвенция часто критикуется за устаревшие формулировки, которые не охватывают современные киберугрозы (атаки искусственного интеллекта, deepfakes, ransomware на критическую инфраструктуру и др.), и за отсутствие новых форм киберпреступлений (IoT, криптовалютные кражи). Многие также к ключевым недостаткам

относят слишком широкие полномочия по сбору данных и трансграничному доступу без строгих гарантий приватности и пропорциональности. Например, слежка (surveillance) без предварительного судебного контроля, что противоречит не только свободе слова, праву на неприкосновенность частной жизни, но и приводит к юридическим коллизиям. Кроме того, проблемы сотрудничества и суверенитета многие государства, в том числе и Россия, видят в положениях статьи 40 Европейской конвенции, которая разрешает трансграничные операции без обязательного согласия государства. Недостаточная унификация определяет нечеткость правил по допустимости электронных доказательств и полномочиям расследований, а зависимость от MLAT (взаимной правовой помощи) существенно замедляет сам процесс расследования.

Также стоит отметить, что хотя к Европейской конвенции на сегодняшний день присоединилось уже 78 стран, однако среди них нет таких важных для глобального влияния участников, как Индия, Китай и Россия.

Поэтому глобальная эффективность Европейской конвенции, несмотря на

роль «золотого стандарта», недостаточно высокая. Она требует модернизации и внедрения обязательного механизма пересмотра положений под новые угрозы (дополнения, которые были внесены двумя протоколами (2003 и 2023 гг.) решают лишь часть проблем).

В связи с этим Россия инициировала создание универсальной Конвенции ООН против киберпреступности, которая должна была бы устранить указанные недостатки. В 2017 г. российские дипломаты указали на неприемлемость информационной гегемонии западных стран, возможности вмешательства зарубежных спецслужб (преимущественно США и их союзников) в работу компьютерных сетей других государств и предложили разработать альтернативу Конвенции Совета Европы о преступности в сфере компьютерной информации 2001 г. – глобальную конвенцию ООН¹. Несмотря на противодействие Запада, Генеральной Ассамблеей ООН резолюцией 74/247 было принято решение о создании Специального комитета для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. В декабре 2019 г. удалось добиться запуска переговоров по данному вопросу в ООН в рамках ее Специального комитета. Инициатива России по созданию универсального механизма привлечения к ответственности за преступления в сфере ИКТ была услышана и проработана.

В феврале 2024 г. завершилась последняя (седьмая по счету) сессия Спецкомитета по обсуждению проекта Конвенции ООН о противодействии киберпреступности. Переговорный процесс пережил несколько кризисов. При этом Россия осталась не совсем удовлетворена результатами работы Спецкоми-

тета. Тем не менее, независимо от итогов работы над проектом, наша сторона достигла поставленной цели – Россия компетентно и громко заявила о создании глобального механизма цифровой безопасности, указала на необходимость кардинального расширения круга киберпреступлений и инициировала разработку правил ответственного поведения в цифровой сфере.

Глобальная Конвенция ООН против киберпреступности была принята Генеральной Ассамблеей ООН 24 декабря 2024 г., открыта для подписания в г. Ханой 25-26 октября 2025 г., и на январь 2026 г. данную Конвенцию подписали 72 государства, в том числе и Российская Федерация.

Конвенция устанавливает базовый минимальный набор преступлений в сфере компьютерных технологий (несанкционированный доступ, вредоносное ПО, компьютерное мошенничество, атаки на данные/системы и др.), а также механизмы международного сотрудничества по обмену электронными доказательствами для борьбы с киберугрозами. Положения Конвенции расширяют процессуальные полномочия органов власти, способствуя разработке специализированных процессуальных инструментов, включая получение журналов сетевой активности, команд удаленного доступа к компьютерным системам, скоординированные процедуры изъятия и сохранения цифровых данных, а также институт срочных предписаний на сохранение информации (preservation orders).

В условиях расширения полномочий по доступу к цифровым следам возрастает и значение системы гарантий, определяющих субъектный состав уполномоченных органов, порядок выдачи разрешений на доступ, а также механизмы обеспечения сохранности и це-

1 Пикалов П.А. Криминалистические подходы в идентификации киберпреступлений в Европейском союзе и Российской Федерации // Актуальные проблемы научных исследований: теоретический и практический аспекты. 2024. С. 140-144.

лостности электронных доказательств. И здесь ярко выявляются риски и недостатки Конвенции, так как отсутствие четко регламентированных процедур судебного контроля, ограничений по объему и периоду доступа, а также обязательного протоколирования действий создает предпосылки для потенциальных злоупотреблений процессуальными полномочиями.

Еще один аспект, который вызывает дискуссии, – это соотношение процессуальных полномочий и гарантий прав человека. Хотя преамбула и отдельные статьи конвенции декларируют приоритет принципов верховенства права и защиты основных прав и свобод, критика со стороны международных правозащитных организаций акцентирует недостаточную детализированность гарантийного аппарата, отнесенного преимущественно к сфере национального законодательства.

Юридически значимым является то обстоятельство, что формальное упоминание прав человека в международном договоре устанавливает лишь минимальный стандарт соотношения полномочий и ограничений. Эффективность защиты прав субъектов данных во многом определяется наличием институциональных механизмов: независимого судебного контроля при выдаче ордеров на доступ к информации, прозрачности процедур обработки данных, возможности постфактумного контроля за законностью действий правоохранительных органов, а также системы компенсаций за необоснованные ограничения.

Еще одним дискуссионным положением Конвенции можно выделить предусмотренные механизмы и комплексы мер технической и методологической поддержки развивающихся государств, включая программы профессиональной подготовки специалистов, трансфер технологий, организацию центров реагирования на компьютерные инци-

денты (CERT/CSIRT) и иные инициативы по повышению готовности к противодействию киберугрозам.

С институциональной позиции данные положения предоставляют государствам с развитыми правоохранительными системами возможности расширения международного сотрудничества, при этом одновременно создавая для менее обеспеченных юрисдикций риски технологической зависимости от стран-доноров и связанных с ними стандартов обработки информации.

Таким образом, несмотря на длительное обсуждение и на активное участие в разработке проекта многих государств, Конвенция оказалась урезана по некоторым основополагающим аспектам, а её положения вызывают ряд сложностей и имеют некоторые недостатки. Среди основных рисков и вызовов Конвенции можно выделить следующие:

- риск злоупотреблений правами человека. Статьи 28-31, 43-45 Конвенции дают слишком широкие полномочия по электронному надзору и сбору данных без достаточных гарантий, что может привести к массовой слежке, цензуре и преследованиям журналистов/активистов. В случае авторитарного режима в государстве, положения данных статей фактически могут привести к легитимации политических репрессий под видом борьбы с «киберпреступлениями».

- проблемы с размытыми определениями и слишком широким охватом. Возможность международной помощи по любым «серьезным преступлениям» (не только «кибер»), что превращает Конвенцию в инструмент глобального надзора. Нечеткость и размытость формулировок преступлений, закрепляемых в Конвенции, допускают неоднозначность толкования, что может привести к неопределенности исполнения, подводя под киберпреступления деятельность журналистов, исследова-

ния в системе кибербезопасности или даже обычную речь;

– практические проблемы и процедурные риски. Здесь можно отметить недостаток фокуса на жертвах киберпреступлений и слабые гарантии прав человека. Недостаточная детализация защиты персональных данных и принцип «пассивной юрисдикции», общие формулировки защиты без принципов законности, необходимости и пропорциональности – это большая зависимость от национального права, что может привести к злоупотреблениям и массовому надзору;

– политические и геополитические вызовы. Основным риском здесь можно выделить несогласованность имплементации, так как страны с разным уровнем демократии могут использовать конвенцию по-разному. Плюс зависимость развивающихся стран от технической помощи (обучение, технологии), что создает уязвимости для влияния доноров.

Таким образом, Конвенция, которая изначально задумывалась как проект для повышения эффективности борьбы с киберпреступлениями, стала по факту компромиссом, где безопасность уступает рискам авторитаризма. Дан-

ный документ формирует современную архитектуру международного процессуального сотрудничества в сфере кибербезопасности, но ее практическая реализация во многом зависит от качества национальных механизмов обеспечения баланса между расширенными полномочиями правоохранительных органов и системой гарантий защиты прав человека. Необходимость разработки детализированных процедур судебного контроля, стандартов трансграничного обмена данными и независимых механизмов мониторинга исполнения обязательств представляет собой ключевое условие предотвращения рисков злоупотреблений положениями конвенции.

В условиях, когда киберпреступления, совершаемые в виртуальной среде, способны порождать реальные деструктивные последствия в физическом мире, юридическое сообщество трансформируется из вспомогательного элемента в фундаментальную составляющую архитектуры глобальной безопасности. А разработка и принятие универсальных международных актов позволит укрепить позиции государств в системном противодействии транснациональной киберпреступности.

Шлегель П.О.,

кандидат юридических наук

Московский университет МВД России имени В.Я. Кикотя

Правовая идеология в условиях цифровой трансформации государства и права

Сегодня цифровая трансформация проникла практически во все элементы современной правовой и государственной системы. В науке и практике уделяется внимание исследованию вызовов, возникающих в связи с цифровизацией и определением места человека в центре права будущего. На наш взгляд, определение и защита цифрового обра-

за личности, общества и государства, а также создание безопасной цифровой среды напрямую зависит от ценностных и идейных основ, создающих фундамент для сохранения гуманистических основ правопорядка.

Право, как и государство, не может существовать вне идеологии. При этом важно, чтобы любые идеи, ценности,