Агафонов Максим Александрович
курсант
ФГКОУ ВО «Московская академия
Следственного комитета Российской Федерации»
г. Москва

СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ КОНВЕНЦИИ ООН ПРОТИВ КИБЕРПРЕСТУПНОСТИ КАК ПЕРВОГО ГЛОБАЛЬНОГО МЕЖДУНАРОДНОГО ДОГОВОРА ПО БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

***Аннотация**: в статье рассмотрены вопросы актуальности Конвенции ООН против киберпреступности, проанализированы основные проблемы применения данной Конвенции на практики, а также произведено сравнение по некоторым моментам с Будапештской Конвенцией 2001 г.*

***Ключевые слова**: киберпреступность, юрисдикция, правоприменение, хищение, подлог.*

Начало 21-го века ознаменовалось всеобщей цифровизацией общества. Особую популярность получили компьютерные устройства, которые есть у каждого, причем не в одном количестве. В настоящее время сложно представить человека, который не имеет выхода в Интернет. Большинство общественных отношений перешло в виртуальный вид. Данная тенденция способствует тому, что все большее количество преступлений совершаются с использованием именно виртуального пространства, с использованием компьютерных устройств. Поскольку Интернет-пространство не имеет границ и юрисдикций, киберпреступность в большинстве своем является трансграничной, тем самым усложняя процесс расследования, или же делая это вовсе невозможным. К примеру, лицо, находясь в государстве А, может путем удаленного доступа совершать преступление в отношении другого лица, находящегося в государстве Б. В таком случае особую важность при расследовании преступлений приобретает правовой институт международного сотрудничества. Зачастую материальные и процессуальные

нормы государств в области киберспреступности могут существенно различаться, а могут отсутствовать и вовсе. Для того чтобы минимизировать данные коллизии и развить международное сотрудничество, необходимо универсальное межнациональное правовое регулирование такого вида преступлений.

Для решения указанной выше проблемы, 24 декабря 2024 года Генеральная Ассамблея ООН одобрила Резолюцию №79/243 о принятии «Конвенции ООН против киберпреступности» [1, с. 1]. Конвенция должна осуществлять глобальную политику в области борьбы с киберпреступностью, путем создания и развития законодательства в области международного сотрудничества в целях повышения эффективности борьбы с киберпреступностью.

Конвенция состоит из Преамбулы, в которой обосновывается необходимость принятия данного нормативно-правового акта, девяти глав и приложения, в котором даны примечания к отдельным статьям Конвенции.

Как отмечает П.А. Литвишко: «Основное содержание Конвенции можно разделить на материальную (криминализация деяний) и процессуальную, а также внутригосударственную и межгосударственную части» [2, с. 1]. Действительно, к процессуальным частям содержания Конвенции ООН можно отнести Главу 1. «Общие положения», которая является необходимым базисом для всех последующих положений указанного международного нормативного правового акта. Если брать разделение, предложенное П. А. Литвишко за основу, то процессуальной и внутригосударственной будут являться третья Глава «Юрисдикция», в которой содержится важная процессуальная информация для каждого Государства-участника относительно определения юрисдикций в отношений преступлений, признанных данной Конвенцией и глава 4. «Процессуальные меры и правоприменение», в содержание которой входят основные требования, условия и гарантии, а также полномочия Государств-участников в сфере применения процессуальных мер. Кроме того, в данной главе находят свое отражение нормы, раскрывающие сущность основных процессуальных и оперативно-розыскных действий, производимых в процессе расследования преступлений, совершенных с использованием информационных технологий: ст. 26 – Опера-

тивное обеспечение сохранности и частичное раскрытие данных о трафике; ст. 27 – Распоряжение о предоставлении информации; ст. 28 – Обыск и изъятие хранимых электронных данных; ст. 29 – Сбор в режиме реального времени данных о трафике; ст. 30 – Перехват данных о содержании; ст. 31 – Замораживание, арест и конфискация доходов от преступлений.

Ст. 1 настоящей Конвенции закрепляет основные цели данного международного нормативно-правового акта. Первоочередной целью является укрепление содействия (международного сотрудничества) между государствами-членами в принятии мер, направленных на повышение эффективности расследования киберпреступлений и их предупреждение. Также целью выступает осуществление технической поддержки развивающихся государств в целях увеличения потенциала по борьбе с кибепреступностью.

Положения Конвенции устанавливают как новые термины, которых не было в международно-правовых актах в области киберпреступности, так и обновляют и дополняют те, которые уже были, например, в «Конвенции о преступности в сфере компьютерной информации ETS №185 (Будапештская Конвенция) [3, с. 1]. Так, ст. 1 «Будапештской Конвенции» содержит понятие «компьютерная система», которое «означает любое устройство или группу взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных». Конвенция ООН против киберпреступности же, в свою очередь, расширяет термин «компьютерная система», указанный выше, до термина «информационно-компьютерная система», которая не только производит автоматизированную обработку данных, но и осуществляет их сбор и хранение.

Несмотря на это, Конвенция ООН также и «дублирует» положения «Будапештской Конвенции». Так, в ст. 1 «Будапештской Конвенции» содержится определение «компьютерные данные», которыми являются «любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные обязать компьютерную систему выполнять ту или иную функцию». Содержание этого термина

находит свое отражение в определении Конвенции ООН «Электронные данные»: любое представление фактов, информации или концепций в форме, пригодной для обработки в информационно-коммуникационной системе, включая соответствующую программу, в результате действия которой информационно-коммуникационная система выполняет ту или иную функцию. Содержание, находящееся в двух представленных статьях, практически идентично, что говорит об отсутствии целесообразности их нахождения в двух международных правовых актов, затрагивающих идентичные вопросы. Похожая ситуация и с понятием «поставщик услуг». В обеих Конвенциях под поставщиком услуг понимается любая государственная или частная структура, которая:

а) обеспечивает пользователям ее услуг возможность обмена информацией посредством использования информационно-коммуникационной системы;

б) осуществляет обработку или хранение электронных данных от имени такого поставщика коммуникационных услуг или пользователей таких услуг.

Сферой применения настоящей Конвенции, в соответствии со ст. 3, является предупреждение, расследование и преследование за преступления, признанные Конвенцией «Киберпреступлениями». Конвенция обязывает государства-участников принимать законодательные меры по признанию таких деяний преступными в соответствии со своим внутренним законодательством. К таким преступлениям относятся.

1. Незаконный доступ (ст.7): умышленное преступление, совершенное с целью получить электронные данные путем нарушения мер безопасности и конфиденциальности. Совершается в отношении информационной системы (либо любой ее части), соединенной с другой такой же информационной системой (либо ее частью). Российский Уголовный закон содержит аналогичную норму, затрагивающую неправомерный доступ к такого рода информации, которая закреплена в ст. 272 УК РФ. Так, преступлением считается неправомерный доступ к охраняемой законом компьютерной информации. Важным условием является то, что доступ должен повлечь уничтожение, блокирование, модификацию либо копирование компьютерной информации.

2. Ст. 10. Воздействие на информационно-коммуникационную систему. Конвенцией определено, что уголовным правонарушением является умышленное и неправомерное деяние, которое препятствовало функционированию электронно-коммуникационной системы путем ввода, передачи, повреждения, удаления, порчи, изменения или блокирования электронных данных. «Аналогом» данной нормы в РФ является ст.274.1 УК РФ: Неправомерное воздействие на критическую информационную инфраструктуру РФ, которая подразумевает умышленные действия по созданию, распространению или использованию компьютерной информации в целях ее уничтожения, блокирования, модификации и копирования.

3. Ст. 12. Подлог с использованием информационно-коммуникационной системы. Считается умышленным деянием, совершенным путем ввода, изменения, удаления либо блокирования электронных данных, приводящих к возникновению ложных данных для придания им правомерного вида и использования в правовых отношениях с целью совершить обман. Уголовный Кодекс Российской Федерации в ст. 292. «Служебный подлог» закрепляет аналогичную норму, однако в статье отсутствует квалифицирующий признак – совершение преступления с использованием информационно-коммуникационных технологий, что зачастую затрудняет процесс квалификации данного преступного деяния.

4. Ст. 13. Хищение или мошенничество с использованием информационно-коммуникационной системы. Российский уголовный закон также содержит в себе статьи, касающиеся хищений и мошенничества с использованием информационных технологий, причем эти самые технологии будут являться квалифицирующим признаком (п. г) ч.3 ст. 158 УК РФ) или квалифицирующим составом преступления (159.3, 159.6 УК РФ).

5. Ст.14 Преступления, связанные с размещением в интернете материалов со сценами сексуальных надругательств над детьми или их сексуальной эксплуатации – российским аналогом будут выступать п. г) ч. 2 ст. 242.1, п. г) ч. 2 ст. 242.2 УК РФ. Статья 242.1 в пункте г) ч. 2 подразумевает изготовление, приобретение, хранение или перемещение через Государственную границу

Российской Федерации в целях распространения, публичной демонстрации или распространение материалов или предметов с порнографическим изображениями несовершеннолетних, совершенные с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет».

6. Ст. 16 Распространение интимных изображений без согласия – по признакам объективной стороны данный состав схож с преступным деянием, закрепленным в ст. 137 УК РФ «Нарушение неприкосновенности частной жизни – незаконное распространение сведений о частной жизни лица без его согласия. Стоит отметить, что ст. 137 УК РФ содержит квалифицирующий признак, закрепленный в ч. 3, который звучит так: незаконное распространение в электронно-телекоммуникационных сетях.

7. Ст. 17. Отмывание доходов от преступлений. Российский уголовный закон предусматривает «разбивает» это преступление на 2 состава: ст. 174 и ст. 174.1 УК РФ. Разделение этих смежных составов осуществляется по субъекту преступления: в первом случае лицо легализует денежные средства или иное имущество, полученное от других лиц преступным путем. Во втором же легализация будет предикатным преступлением, в котором лицо «отмывает» денежные средства, приобретенные путем совершения им преступления.

Исходя из вышесказанного, сделаем вывод, что Конвенция ООН против киберпреступности не является «идеальной». Сфера ее применения не полностью охватывает преступления, совершенные с использованием информационных технологий. Нами предлагается вынести предложение межведомственной рабочей группе по противодействию информационной преступности под эгидой Генеральной прокуратуры о возможности расширения составов преступлений, которые бы в полной мере охватывались данной Конвенцией. В качестве образца предлагаем использовать Перечень №25 преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации, содержащийся в Указании Генпрокуратуры России №462/11, МВД России №2 от 25.06.2024 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, исполь-

зуемых при формировании статистической отчетности» [4, с.1]. Данный перечень, на наш взгляд, содержит исчерпывающий перечень составов преступлений, в которых использование информационно-телекоммуникационных сетей будет являться альтернативным квалифицирующим признаком, местом, способом или средством совершения преступления.

Список литературы

1. Заместитель начальника Главного управления международного правового сотрудничества Генеральной прокуратуры Российской Федерации [Электронный ресурс]. – Режим доступа: https://viennamission.mid.ru/ru/news/statyazamestitelyanachalnikaglavnogoupravleniyamezhdunarodnopravovogosotrudnichestvageneraln/ (дата обращения: 19.05.2025).

2. Конвенция о преступности в сфере компьютерной информации ETS №185 (Будапешт, 23 ноября 2001 г.) [Электронный ресурс]. – Режим доступа: https://www.europarl.europa.eu/meetdocs/20142019/documents/libe/dv/7convbudapest/7convbudapest_en.pdf (дата обращения: 19.05.2025).

3. Организация Объединенных Наций. Резолюция 79/243 [Электронный ресурс]. – Режим доступа: https://www.un.org/ru/documents/treaty/A-RES-79–243 (дата обращения: 19.05.2025).

4. Указание Генпрокуратуры России N 462/11, МВД России №2 от 25.06.2024 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_483902/251f7ac207ca304c6331640eb36b162351c24684/ (дата обращения: 19.05.2025).