Тезисы выступления главы российской делегации по пункту 4 повестки дня первой субстантивной сессии Спецкомитета ООН по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях («Цели и охват конвенции»)

(Нью-Йорк, 2 марта 2022 г.)

Прежде всего хотел отметить, что Россия поддерживает предложения Председателя Спецкомитета о методе работы по пункту 4 повестки дня. Также хотел выразить благодарность госпоже Председателю за подготовленный документ по целям, охвату и структуре конвенции, который может служить хорошим базисом нашей дальнейшей работы.

Российская Федерация считает, что в будущей конвенции должны закрепляться следующие цели:

Во-первых, установление ответственности за противоправные деяния, совершенные с использованием ИКТ, а также продвижение, содействие принятию и укреплению мер, направленных на эффективное предупреждение и борьбу с использованием ИКТ в преступных и иных противоправных целях при одновременной защите пользователей ИКТ, обеспечении соблюдения обязательств в области прав человека, уважении принципа суверенного равенства и территориальной целостности государств и невмешательства во внутренние дела других государств.

Во-вторых, предоставление полномочий, достаточных для эффективной борьбы с использованием ИКТ в преступных и иных противоправных целях, а также предоставление практического инструментария для расширения технической помощи между государствами-членами и наращивание потенциала национальных органов власти в области

борьбы с использованием ИКТ в преступных целях при одновременном поощрении обмена информацией, опытом и передовыми видами практики.

В-третьих, поощрение, стимулирование и поддержка международного сотрудничества в деле предупреждения и борьбы с использованием ИКТ в преступных целях.

Уважаемые коллеги, тема охвата будущей конвенции является одним из ключевых вопросов первой субстантивной сессии Спецкомитета ООН по разработке всеобъемлющей международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях. Я не случайно озвучил полное название Спецкомитета, которое было закреплено в резолюциях Генассамблеи ООН 74/247 и 75/282.

Довольно насыщенные дискуссии в межсессионный период позволили нам обсудить много важных элементов работы Спецкомитета и даже предварительно согласовать некоторые из них. По вопросу охвата у нас уже имеются расхождения. Их традиционно можно разделить на два подхода.

1. Первый заключается в том, что будущая конвенция должна покрывать только так называемую «киберпреступность», которая с подачи ряда стран ограничит охват конвенции преступлениями, совершаемыми с использованием компьютеров, а также небольшим числом компьютерных преступлений, которые существуют благодаря появлению компьютеров. На английском языке это звучит как «computer-dependent and computer-enabled crimes».

Такой подход не соответствует положениям резолюций ГА ООН 74/247 и 75/282. Россия и целый ряд государств обращает внимание, что наша будущая конвенция посвящена не киберпреступности и сугубо компьютерным преступлениям, а более широкому определению – использованию ИКТ в преступных целях. У нас четкое понимание, что ИКТ выходит за рамки компьютеров и покрывает еще целый ряд технологий.

Так называемый «кибер» не учитывает спутниковую, телефонную, радиосвязь, нарушение работы факсов. Для некоторых отдаленных

территорий, островов единственным способом связи являются не компьютерные сети и кабели, а спутники, через которые в том числе обеспечивается связь с интернетом. В развивающихся государствах также широко применяются простые телефоны, в том числе те, которые не подключены к сети Интернет и не имеют операционных систем, свойственных смартфонам. Все это применяется преступниками в своих целях и не может быть нами проигнорировано.

Причем этот феномен характерен не только для развивающихся государств. Хочу сослаться на доклад Европола IOCTA от ноября прошлого года, в котором, помимо указаний на рост чисто компьютерных преступлений, напоминается о драматическое увеличение числа случаев смс-фишинга. Смс-фишинг – это телефоны, а не компьютеры. Следовательно, это не «кибер», а ИКТ.

Также стоит отметить национальные вклады ряда государств в Спецкомитете, в которых отмечается возрастающее взаимодействие хакеров и террористов и необходимость бороться **с использованием ИКТ в террористических целях**. Простой пример. Широко известны случаи, когда активация взрывных устройств происходила через простой устаревший телефон, который не имеет операционную систему, чип внутри и даже подключение к Интернету. Это направление тоже относится к использованию ИКТ в преступных целях и может быть учтено при разработке будущей конвенции.

Поэтому в существующих профильных конвенциях, которые заточены под «киберпреступность», составов преступлений не более 10 и их число не растет вопреки заявленным обновлениям, а в субстантивных вкладах государств в Спецкомитете таких составов предложено уже порядка 30.

2. Будущая конвенция должна носить **всеобъемлющий** характер в соответствии с резолюциями ГА ООН 74/247 и 75/282. То есть она должна по возможности охватывать все составы преступных деяний, совершаемых с использованием ИКТ.

В этой связи совершенно непродуктивно и преждевременно ограничивать охват конвенции. Если мы сделаем это уже сейчас, а в ходе работы над текстом, например, при определении криминализации поймем, что нам надо будет его расширить, чтобы учесть новые виды преступлений, конвенция не будет всеобъемлющей, а значит и эффективной.

3. Опыт разработки антикриминальных конвенций показывает, что вопрос охвата зачастую окончательно согласовывался делегациями лишь на заключительных этапах переговоров. Так было и с рядом конвенций ООН, так и со вторым доппротоколом Будапештской конвенции. Мы также не исключаем, что при обсуждении криминализации, дефиниций и других смежных тем нам придется возвращаться к вопросу охвата.

4. Поэтому важно оставить уже согласованную в рамках резолюций ГА ООН 74/247 и консенсусной 75/282 наиболее оптимальную терминологию к теме охвата – использование ИКТ в преступных целях. Она не ограничивает нас при создании действительно всеобъемлющей конвенции и создает задел на будущее, чтобы учесть возникающие угрозы. Такой подход, на наш взгляд, обеспечит необходимую и выверенную динамику всего переговорного процесса с тем, чтобы в 2024 году у нас были все возможности согласовать и утвердить проект конвенции, как это заложено резолюцией ГА ООН 75/282.

Уважаемые коллеги, ряд делегаций, ссылаясь на резолюцию ГА ООН 74/247, приводили пример такого документа как Конвенция Совета Европы по противодействию компьютерным преступлениям. Хотел обратить внимание уважаемых коллег на то, что это далеко не единственный ныне существующий региональный документ. В соответствии с оперативным параграфом 2 резолюции 74/247 в своей работе Спецкомитет должен в полной мере учитывать существующие региональные инструменты. В этой связи я хотел напомнить о существовании еще по меньшей мере двух международно-правовых инструментов: Конвенции Лиги арабских государств о борьбе с преступлениями в области информационных технологий (2010 г.) и л Соглашении о сотрудничестве государств-участников содружества

независимых государств в борьбе с преступлениями в сфере информационных технологий (2018 г.), это самое свежее соглашение из всех региональных документов. Уверен, что упоминание этих конвенций будет должным образом зафиксировано. Ряд делегаций также высказались в пользу того, чтобы будущая конвенция не противоречила существующим документам. Существующие документы принимались 10-20 лет назад. Виртуальная сфера, в которой действует информпреступность, чрезвычайно динамична. На данном этапе нельзя исключать, что Спецкомитет идентифицирует и примет решение о включении дополнительных международно-правовых возможностей о противодействии информпреступности.

И последний момент. В выступлении некоторых делегаций озвучивалась необходимость определить в универсальной конвенции технологически нейтральный подход и дефиниции. На взгляд России, этот подход требует дополнительной проработки. В ходе неформальных консультаций уже звучали предложения о технологически нейтральных дефинициях. Я задавал коллегам вопросы, просил привести пример таких дефиниций. К сожалению, ответа не получил. Этот вопрос требует дополнительной проработки, поскольку правовая природа технологически нейтральных дефиниций вряд ли может быть четко определена, и нам нужно избежать ситуации, когда отсутствие такого четкого определения правовой природы станет препятствием для практического взаимодействия между правоохранителями наших стран.