24 August 2020
Russian
Original: English

Доклад о работе совещания Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, прошедшего в Вене 27–29 июля 2020 года

I. Введение

1. В резолюции 65/230 Генеральная Ассамблея просила Комиссию по предупреждению преступности и уголовному правосудию учредить в соответствии с пунктом 42 документа «Салвадорская декларация о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире» межправительственную группу экспертов открытого состава для проведения всестороннего исследования проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора, включая обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве, с целью изучения возможных путей укрепления существующих и выработки предложений в отношении новых национальных и международных правовых или иных мер по противодействию киберпреступности.

2. Первое совещание Группы экспертов состоялось в Вене 17–21 января 2011 года. На этом совещании Группа экспертов рассмотрела и утвердила подборку тем для рассмотрения и методологию исследования (E/CN.15/2011/19, приложения I и II).

3. Второе совещание Группы экспертов состоялось в Вене 25–28 февраля 2013 года. На нем Группа экспертов приняла к сведению проект всестороннего исследования проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора, подготовленный Управлением Организации Объединенных Наций по наркотикам и преступности (УНП ООН) под ее руководством во исполнение мандата, предусмотренного в резолюции 65/230 Генеральной Ассамблеи, на основе подборки тем и методологии исследования, утвержденных на первом совещании Группы экспертов.

4. В Дохинской декларации о включении вопросов предупреждения преступности и уголовного правосудия в более широкую повестку дня Организации Объединенных Наций в целях решения социальных и экономических проблем и содействия обеспечению верховенства права на национальном и международном уровнях, а также участию общественности, принятой на тринадцатом Конгрессе Организации Объединенных Наций по предупреждению преступности и уголовному правосудию и одобренной Генеральной Ассамблеей в

резолюции 70/174, государства-члены отметили деятельность Группы экспертов и предложили Комиссии по предупреждению преступности и уголовному правосудию рассмотреть вопрос о том, чтобы рекомендовать Группе экспертов на основе проводимой ею работы продолжать обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве с целью изучения возможных путей укрепления существующих мер и выработки предложений в отношении новых национальных и международных правовых или иных мер по противодействию киберпреступности.

5. Третье совещание Группы экспертов состоялось в Вене 10–13 апреля 2017 года. На этом совещании Группа экспертов, помимо всего прочего, рассмотрела вопрос об утверждении кратких докладов о работе своих первых двух совещаний, подготовленных Докладчиком, а также проект всестороннего исследования проблемы киберпреступности, замечания к нему и вопросы дальнейшей работы над проектом исследования. Она также обменялась информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве.

6. В резолюции 26/4, принятой Комиссией по предупреждению преступности и уголовному правосудию на двадцать шестой сессии в мае 2017 года, Комиссия просила Группу экспертов продолжать свою работу путем проведения периодических совещаний и выступать в качестве платформы для дальнейшего обсуждения вопросов существа, касающихся киберпреступности, внимательно следя за новыми тенденциями, в соответствии с Салвадорской и Дохинской декларациями. В этой же резолюции Комиссия просила Группу экспертов продолжать обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве с целью изучения возможных путей укрепления существующих мер и выработки предложений в отношении новых национальных и международных правовых или иных мер по противодействию киберпреступности.

7. Четвертое совещание Группы экспертов состоялось в Вене 3–5 апреля 2018 года. На этом совещании Группа экспертов сосредоточила внимание на таких темах, как законодательство и правовые основы противодействия киберпреступности и криминализация связанной с ней деятельности. Были обсуждены последние изменения законодательства и политики в области противодействия киберпреступности на национальном и международном уровнях. Группа экспертов также рассмотрела подходы к криминализации киберпреступлений на национальном уровне. На том же совещании Группа экспертов утвердила предложение Председателя по плану своей работы на период 2018–2021 годов (UNODC/CCPCJ/EG.4/2018/CRP.1).

8. Пятое совещание Группы экспертов состоялось в Вене 27–29 марта 2019 года. На этом совещании Группа экспертов сосредоточила внимание на таких темах, как правоохранительная деятельность и расследование киберпреступлений, а также электронные доказательства и уголовное правосудие. На том же совещании Группа экспертов обсудила, в частности, успехи стран в осуществлении правовых и процессуальных мер противодействия киберпреступности и мер по внедрению нового следственного инструментария для сбора и установления подлинности электронных доказательств, которые будут использоваться в целях доказывания в уголовном судопроизводстве. В ходе обсуждения особое внимание было также уделено вопросу о том, как обеспечить баланс между необходимостью принятия правоохранительными органами эффективных мер реагирования на киберпреступность и защитой основных прав человека, в частности права на неприкосновенность частной жизни. Группа экспертов особо отметила необходимость устойчивого наращивания потенциала в целях расширения возможностей, имеющихся на национальном уровне, и создания благоприятных условий для обмена передовой практикой и опытом проведения расследований.

9. В резолюции 74/173 Генеральная Ассамблея признала важность работы Группы экспертов, направленной на продолжение обмена информацией о национальном законодательстве, передовых методах, технической помощи и международном сотрудничестве в целях изучения возможных путей укрепления существующих мер и выработки предложений в отношении новых национальных и международных правовых или иных мер по противодействию киберпреступности; с удовлетворением отметила, что Группа экспертов разработает в соответствии со своим планом работы на период 2018–2021 годов возможные выводы и рекомендации для представления Комиссии по предупреждению преступности и уголовному правосудию; признала, что Группа экспертов является важной платформой для обмена информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве; просила УНП ООН продолжать периодически собирать информацию о новых тенденциях, достигнутом прогрессе и выявленных передовых методах и периодически представлять эту информацию Группе экспертов и Комиссии и предложила Группе экспертов на основе своей работы оказывать УНП ООН консультационную помощь, в том числе в отношении Глобальной программы борьбы с киберпреступностью, в целях содействия, без ущерба для других вопросов, включенных в мандат Группы экспертов, выявлению первоочередных потребностей в области наращивания потенциала и эффективных мер реагирования, без ущерба для статуса Комиссии как руководящего органа программы Управления по борьбе с преступностью.

10. Первоначальные сроки проведения шестого совещания Группы экспертов, с 6 по 8 апреля 2020 года, были утверждены ее расширенным бюро 11 ноября 2019 года согласно процедуре отсутствия возражений. Предварительная повестка дня совещания была согласована расширенным бюро 18 декабря 2019 года по процедуре отсутствия возражений. Двенадцатого марта 2020 года расширенное бюро было проинформировано о том, что совещание придется перенести из-за введения ограничений в связи с пандемией коронавирусной инфекции (COVID-19). Пятнадцатого апреля 2020 года расширенное бюро в соответствии с процедурой отсутствия возражений утвердило новые сроки проведения шестого совещания Группы экспертов — с 27 по 29 июля 2020 года. Двадцать второго июня 2020 года в соответствии с той же процедурой был утвержден смешанный формат проведения шестого совещания под руководством Председателя.

II. Перечень предварительных рекомендаций и выводов, составленный Докладчиком

11. В соответствии с планом работы Группы экспертов на 2019–2021 годы по итогам состоявшихся на совещании обсуждений и прений Докладчик при содействии Секретариата подготовил перечень предварительных выводов и рекомендаций, высказанных государствами-членами; вошедшие в перечень рекомендации имеют четкую формулировку и нацелены на укрепление практических мер противодействия киберпреступности. Согласно плану работы подборка замечаний государств-членов была включена в доклад о работе шестого совещания для дальнейшего обсуждения на итоговом совещании, которое должно состояться не позднее 2021 года.

12. В соответствии с планом работы на итоговом совещании Группа экспертов рассмотрит накопленные предварительные выводы и рекомендации и составит из них сводный перечень утвержденных выводов и рекомендаций для представления Комиссии по предупреждению преступности и уголовному правосудию. Перед итоговым совещанием предварительные выводы и рекомендации государств-членов будут распространены среди всех остальных государств-членов, наблюдателей и других заинтересованных сторон для комментариев, а все полученные до начала совещания комментарии будут размещены онлайн для сведения делегаций.

A. Международное сотрудничество

13. В соответствии с планом работы Группы экспертов в настоящем пункте Докладчиком обобщены замечания, высказанные государствами-членами в ходе совещания по пункту 2 повестки дня «Международное сотрудничество». Нижеизложенные предварительные рекомендации и выводы были высказаны государствами-членами, и их включение в доклад не означает одобрения Группой экспертов, а порядок перечисления не отражает степени важности.

a) Что касается широты определения киберпреступности для целей международного сотрудничества, то странам следует установить уголовную ответственность за достаточно широкий круг киберпреступлений, в который должны входить как собственно компьютерные преступления, так и другие виды преступлений, часто совершаемых с помощью интернета и электронных средств (преступления, совершаемые с помощью кибертехнологий), такие как кибермошенничество, киберворовство, вымогательство, отмывание денег, торговля наркотиками и оружием, детская порнография[1] и террористическая деятельность.

[1] Термин «детская порнография» прочно закреплен в международно-правовых актах, принятых с начала XXI века. В статье 2 Факультативного протокола к Конвенции о правах ребенка, касающегося торговли детьми, детской проституции и детской порнографии, термин «детская порнография» определен как «любое изображение какими бы то ни было средствами ребенка, совершающего реальные или смоделированные откровенно сексуальные действия, или любое изображение половых органов ребенка главным образом в сексуальных целях». В пункте (c) статьи 3 Факультативного протокола предусмотрено требование о том, чтобы государства установили уголовную ответственность за следующие деяния, образующие состав детской порнографии: «производство, распределение, распространение, импорт, экспорт, предложение, продажу или хранение в вышеупомянутых целях детской порнографии, определяемой в статье 2». Термин «детская порнография» упоминается в пункте 2 статьи 9 Конвенции Совета Европы о киберпреступности, где он определен как «порнографические материалы, изображающие: a) участие несовершеннолетнего лица в откровенных сексуальных действиях; b) участие лица, кажущегося несовершеннолетним, в откровенных сексуальных действиях; c) реалистические изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях». В пункте 2 статьи 20 Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений термин «детская порнография» определен как «любые материалы, которые изображают ребенка, совершающего реальные или смоделированные сексуально откровенные действия, или любое изображение половых органов ребенка главным образом в сексуальных целях». Согласно пункту 1 статьи 20 этой Конвенции, стороны должны установить уголовную ответственность за «производство детской порнографии, предложение или предоставление детской порнографии, распространение или передачу детской порнографии, приобретение детской порнографии для себя или другого лица, хранение детской порнографии и преднамеренное получение доступа к детской порнографии при помощи информационно-коммуникационных технологий».
Из этих документов термин «детская порнография» перекочевал в национальное законодательство. Поэтому он продолжает использоваться для определения соответствующего состава преступления во многих странах. Тем не менее со стороны правоохранительных органов и служб защиты детей все чаще звучат сомнения в адекватности этого термина и наблюдается тенденция использовать альтернативную терминологию (см. Interagency Working Group on Sexual Exploitation of Children, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse* (Bangkok, ECPAT International, 2016), cc. 38–40).
Вследствие этого, несмотря на по-прежнему широкое употребление термина «детская порнография», для обозначения откровенных сексуальных изображений детей все чаше используется термин «материалы о сексуальных надругательствах над детьми», исходя из того, что этот термин точнее передает тяжкий характер обозначаемого деяния и не допускает мысли о том, что подобные действия могут совершаться с согласия ребенка. Так, в рамках проекта по борьбе с распространением материалов о надругательствах над детьми в интернете, являющегося частью программы «Комплексное оперативно-стратегическое планирование в интересах органов полиции», активно продвигается мысль, что любые сексуальные изображения детей являются надругательством или эксплуатацией и не могут быть квалифицированы как порнография. Термин «порнография» используется

b) В связи с вопросом о механизмах международного сотрудничества государствам было рекомендовано присоединиться к таким многосторонним договорам, как Конвенция Организации Объединенных Наций против транснациональной организованной преступности и Конвенция Совета Европы о киберпреступности, и пользоваться ими в качестве правовой основы для оказания взаимной правовой помощи в отсутствие соответствующих двусторонних соглашений. В отсутствие международного договора государства могут обращаться к другим государствам с просьбами о сотрудничестве на основе взаимности. Конвенцию Совета Европы о киберпреступности следует использовать во всем мире в качестве стандарта в вопросах наращивания потенциала и технической помощи, в связи с чем было упомянуто о проведении переговоров по второму дополнительному протоколу к конвенции, который будет способствовать дальнейшему расширению трансграничного сотрудничества. Было вновь высказано мнение, что Конвенция Совета Европы о киберпреступности имеет ограниченную сферу применения из-за своего регионального характера и низкого уровня ратификации, отсутствия цельной концепции и в силу того, что она не учитывает современные тенденции киберпреступности и не вполне подходит для развивающихся стран. Было обращено внимание на тот факт, что в резолюции 74/247 Генеральная Ассамблея постановила учредить специальный межправительственный комитет экспертов открытого состава, представляющий все регионы, для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Ряд делегаций выразил мнение, что разработка конвенции под эгидой Организации Объединенных Наций могла бы способствовать повышению эффективности международного сотрудничества в области борьбы с киберпреступностью. Другие делегации выразили точку зрения, что новые правовые режимы или акты по киберпреступности не должны мешать выполнению действующих договоров, ранее взятых обязательств и уже достигнутых соглашений либо вынуждать государства отказываться от их выполнения или отступать от их положений.

c) К расследованию киберпреступлений необходимо привлекать стратегических партнеров, например членов таких организаций, как Организация американских государств (ОАГ), Группа семи и Международная организация уголовной полиции (Интерпол).

d) При проведении расследований и судебных разбирательств необходимо уважать суверенитет и юрисдикцию государств. Направлять коммерческим предприятиям и физическим лицам прямые запросы о поиске данных, хранящихся в другой стране, недопустимо без предварительного согласия властей этой страны.

e) Для повышения эффективности международного сотрудничества следует создать механизмы быстрого рассмотрения просьб о международной помощи и наладить каналы связи между национальными органами через сотрудников по связи и информационные системы с целью облегчения трансграничного сбора доказательств и передачи электронных доказательств в режиме онлайн.

f) Государствам следует и далее расширять сотрудничество в вопросах защиты важнейших объектов инфраструктуры и укреплять взаимодействие

для описания материалов с изображением совершеннолетних, по обоюдному согласию вступающих в половые сношения, такие материалы предназначены для широкой аудитории и легально распространяются в развлекательных целях. Изображения сцен надругательства над детьми к этой категории не относятся. Они изображают детей, которые еще не могут давать согласие и являются жертвами преступления. С юридической точки зрения, материалы о сексуальных надругательствах над детьми являются документальным доказательством сексуальных посягательств или изнасилования (UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (New York, 2015), с. 10).

между центрами реагирования на компьютерные инциденты и инциденты информационной безопасности.

g) Для ускорения обмена информацией, в том числе оперативными данными и доказательствами совершения правонарушений, государствам следует изучить возможность внедрения новых современных процедур в данной области.

h) Всем государствам-членам следует вновь подтвердить приверженность обеспечению безопасности информационно-коммуникационных технологий путем использования их исключительно в мирных целях и активизации международных усилий по борьбе с любой злонамеренной деятельностью в киберпространстве во времена серьезных кризисов глобального, регионального и местного масштаба.

i) Необходимо оптимизировать процедуры международного сотрудничества таким образом, чтобы в пределах законных возможностей обеспечить оказание максимально широкой помощи в выполнении просьб о международном сотрудничестве в обеспечении сохранности электронных доказательств и предоставлении доступа к файлам журнала событий и учетным записям пользователей, не нарушая права человека и основные свободы или имущественные права.

j) Необходимо разработать стандартный порядок действий по сбору и обеспечению сохранности данных на месте преступления, который будет приемлем на международном уровне. Повсеместное применение стандартной международной методики сбора и хранения доказательств и обмена ими имеет огромное значение, особенно для расследования киберпреступлений и преследования правонарушителей.

k) Странам рекомендуется особо внимательно следить за адекватностью действий следственных органов и уважать основные свободы и требования защиты персональных данных, связанные с тайной личной переписки.

l) При осуществлении международного сотрудничества в сфере противодействия киберпреступности необходимо учитывать гендерно-возрастные особенности и потребности уязвимых групп.

m) Государствам следует воздерживаться от незаконных односторонних действий, идущих вразрез с международным правом и Уставом Организации Объединенных Наций.

n) Что касается широты международного сотрудничества, то если оказанием взаимной правовой помощи должны заниматься только национальные власти, то участвовать в сотрудничестве должен не только ограниченный круг государственных ведомств, но и представители частного сектора, в том числе поставщики интернет-услуг. В этой связи было рекомендовано принять положения о допустимости прямого направления просьб о содействии в получении информации об абонентах и обеспечении сохранности данных поставщикам интернет-услуг из других юрисдикций.

o) Любые возможные меры противодействия киберпреступности и защиты населения должны обеспечивать неуклонное соблюдение прав человека и конституционных гарантий и способствовать созданию более свободного, открытого, безопасного, устойчивого к внешним воздействиям и общедоступного киберпространства.

p) Странам рекомендуется наладить более эффективное сотрудничество с отраслью и активизировать взаимодействие между государством и частными поставщиками услуг, в частности в целях решения проблем, связанных с размещением материалов вредоносного и противозаконного содержания в интернете.

q) Частные компании, в первую очередь поставщики интернет-услуг, несут совместную ответственность за предупреждение и расследование киберпреступлений; таким компаниям следует быстрее и активнее реагировать на

просьбы об оказании правовой помощи, предоставлять такую помощь в странах своего нахождения и поддерживать надлежащие каналы связи с местными властями.

r) Необходимо развивать государственно-частные партнерства. Там, где такие партнерства еще не созданы, их нужно создать, а частные компании следует привлекать к участию в рабочих группах (многосторонних форумах) и обсуждению вопроса о совершенствовании методов противодействия киберпреступности.

s) К усилиям по предупреждению и противодействию киберпреступности следует привлекать неправительственные организации и научные круги, ведь их участие позволяет обеспечить максимально широкий, разносторонний и всеобъемлющий взгляд на проблему и, в частности, гарантировать защиту прав человека, свободу слова и неприкосновенность частной жизни.

t) Для обеспечения сохранности допустимых электронных доказательств и обмена ими странам рекомендуется присоединиться к авторизованным сетям специалистов, включая круглосуточные сети, специализированные сети по киберпреступности и сети оперативного полицейского взаимодействия Интерпола, и активнее использовать и развивать их, а также наладить связи со стратегическими партнерами с целью обмена данными по вопросам киберпреступности, оперативного принятия мер реагирования и сведения к минимуму опасности утраты важных доказательств. Прежде чем задействовать каналы взаимной правовой помощи, рекомендуется использовать каналы полицейского взаимодействия и другие методы неофициального сотрудничества.

u) В дополнение к оказанию международной правовой помощи по уголовным делам по традиционным каналам, каждому государству следует создать реально круглосуточный и должным образом оснащенный контактный центр для обеспечения сохранности цифровых данных, взяв за образец успешный пример механизма блокировки данных, предусмотренный Конвенцией Совета Европы о киберпреступности.

v) Государствам-членам следует делиться информацией о национальных подходах к решению проблемы своевременного доступа к цифровым доказательствам с другими государствами-членами, чтобы те могли использовать этот опыт для повышения эффективности собственных процедур.

w) Государствам-членам следует ввести в практику направление и прием просьб о взаимной правовой помощи в электронной форме с целью сокращения задержек, связанных с международной пересылкой документов.

x) Странам следует развивать межведомственное взаимодействие и повышать операционную совместимость путем стандартизации формы информационных запросов и процедур удостоверения подлинности с привлечением широкого круга заинтересованных сторон.

y) Странам следует обеспечить выполнение требований национального законодательства и усилить координацию и взаимодействие на национальном уровне в вопросах сбора информации и доказательств и обмена ими для целей уголовного преследования.

z) Государствам-членам следует создать такой внутренний правовой режим, чтобы обеспечить быстрый и эффективный обмен «сведениями об абонентах» по смыслу пункта 3 статьи 18 Конвенции Совета Европы о киберпреступности.

aa) Государствам следует усилить меры по обмену финансовой или денежно-кредитной информацией, замораживанию счетов и конфискации активов, чтобы лишить преступников возможности пользоваться доходами от незаконной деятельности.

bb) В целях укрепления потенциала правоохранительных органов государствам рекомендуется создавать совместные следственные группы с другими странами на двустороннем, региональном или международном уровнях.

cc) Государствам следует также обеспечить возможность эффективной работы с электронными доказательствами и их допустимость в суде, в том числе в случаях, когда они предназначены для иностранного государства или получены из-за рубежа. В этой связи странам рекомендуется продолжить или начать реформировать законодательство в области противодействия киберпреступности и использования электронных доказательств, ориентируясь на положительные примеры и успешный мировой опыт проведения реформ.

dd) Рекомендуется создать правовую основу для осуществления экстерриториальной юрисдикции в отношении киберпреступлений.

ee) Странам следует совершенствовать механизмы для предупреждения коллизий и преодоления трудностей, связанных с атрибуцией киберпреступлений и созданием необходимого потенциала для расследования соответствующих дел.

ff) Государствам следует работать над стандартизацией и более широким применением каких процессуальных инструментов, как распоряжения о предоставлении данных, оперативном обеспечении их сохранности или предоставлении трансграничного доступа, позволяющих ускорить процесс предоставления данных и осуществления поисковых запросов, с тем чтобы облегчить работу правоохранительных органов и их прямое взаимодействие с поставщиками интернет-услуг и решить проблемы, связанные с отслеживанием электронных доказательств и их надлежащим использованием.

gg) Государствам следует способствовать разработке и стандартизации совместимых технических стандартов для цифровой криминалистической экспертизы и трансграничного поиска электронных доказательств.

hh) Для обеспечения эффективной работы механизмов сотрудничества в области противодействия киберпреступности рекомендуется выделить средства на создание или развитие эффективного центрального органа по вопросам международного сотрудничества в уголовно-правовой сфере. Также рекомендуется создать специализированные подразделения по расследованию киберпреступлений и предусмотреть возможность направления просьб об обеспечении сохранности данных другим государствам по круглосуточной сети (или в определенных обстоятельствах непосредственно поставщику интернет-услуг) с целью скорейшего обеспечения сохранности требуемых данных. Более оперативному получению данных может способствовать наличие четкого понимания того, какая информация необходима для успешного выполнения просьбы об оказании взаимной правовой помощи.

ii) Для обмена информацией об актуальных киберугрозах, способах совершения преступлений, передовом опыте и новейших технологиях расследования киберпреступлений и обеспечения взаимного доступа к данным может быть полезно заключить официальные соглашения с такими организациями, как Европейский центр по борьбе с киберпреступностью Агентства Европейского союза по сотрудничеству правоохранительных органов (Европол), Центр по борьбе с киберпреступностью Соединенных Штатов Америки, Японский центр противодействия киберпреступности и Национальный центр по вопросам кибербезопасности Соединенного Королевства Великобритании и Северной Ирландии.

jj) Для эффективного международного сотрудничества необходимо, чтобы в национальном законодательстве были предусмотрены соответствующие процедуры. Поэтому необходимо обеспечить, чтобы национальное законодательство допускало возможность международного сотрудничества между правоохранительными органами.

kk) Государствам следует эффективно сотрудничать друг с другом в вопросах выдачи. Если запрашиваемое государство намерено отказать в выдаче подозреваемого в киберпреступлении, оно должно по возможности провести консультации с запрашивающим государством, при поступлении от него соответствующей просьбы, чтобы позволить ему изложить свою позицию и предоставить информацию. Запрашиваемое государство должно сообщить запрашивающему государству основания для отказа.

ll) Помимо национального законодательства, международное сотрудничество в борьбе с киберпреступностью может осуществляться на основе формальных договорных механизмов и по традиционным каналам полицейского взаимодействия. При обсуждении нового документа по вопросам противодействия киберпреступности странам важно помнить о том, что он не должен противоречить имеющимся документам, уже позволяющим многим странам осуществлять международное сотрудничество в режиме реального времени. В этой связи странам следует проследить, чтобы любой новый документ по киберпреступности не противоречил уже действующим договорам.

mm) Следует уделять приоритетное внимание и прилагать более активные усилия к устойчивому наращиванию потенциала и оказанию технической помощи в целях расширения возможностей всех оперативных служб и укрепления потенциала национальных органов в области борьбы с киберпреступностью, в том числе путем развития связей, проведения совместных совещаний и тренингов, обмена передовым опытом, учебными материалами и шаблонами документов. Мероприятия по наращиванию потенциала и подготовке кадров должны включать узкоспециализированные учебные курсы для практических работников, направленные, в частности, на привлечение женщин-экспертов, а также учитывать потребность законодателей и ответственных должностных лиц лучше разобраться в вопросах сохранения данных для целей правоохранительной деятельности. Одним из направлений работы по наращиванию потенциала и подготовке кадров должно быть повышение квалификации сотрудников правоохранительных органов, следователей и аналитиков в таких областях, как судебная экспертиза, использование данных из открытых источников при расследовании, порядок передачи и хранения электронных доказательств, сбор электронных доказательств за рубежом и их совместное использование. Другим направлением работы является повышение квалификации судей, прокуроров, сотрудников центральных органов власти и адвокатов в вопросах ведения соответствующих дел и вынесения решений.

nn) Крайне важно разработать адекватные и по возможности единообразные правила и сроки удерживания/хранения данных, чтобы обеспечить возможность получения или обеспечения сохранности электронных доказательств, необходимых для обоснования последующих просьб о взаимной правовой помощи.

oo) Большое значение для сбора и совместного использования электронных доказательств в контексте трансграничных расследований и для оперативного и эффективно реагирования на просьбы о взаимной правовой помощи, связанной с сохранением и получением электронных доказательств, имеет международное сотрудничество. В процессе такого сотрудничества следует соблюдать принципы суверенитета и взаимности.

pp) УНП ООН рекомендуется и далее проводить программы по наращиванию потенциала и подготовке кадров в области борьбы с киберпреступностью для национальных правительственных экспертов в целях повышения их квалификации в области выявления и расследования киберпреступлений. В рамках работы по наращиванию потенциала необходимо учитывать потребности развивающихся стран, уделять особое внимание факторам уязвимости каждой отдельно взятой страны с целью оказания адресной технической помощи и содействовать обмену новейшими знаниями в интересах специалистов-практиков и заинтересованных сторон.

qq) Для содействия сотрудникам органов уголовного правосудия в составлении просьб о взаимной правовой помощи УНП ООН разработало «Программу составления просьб об оказании взаимной правовой помощи». Управление также разработало «Практическое руководство по истребованию электронных доказательств из-за рубежа», которое доступно по запросу сотрудникам государственных органов государств-членов. Эти пособия УНП ООН могут оказаться весьма полезны странам.

rr) Комиссии по предупреждению преступности и уголовному правосудию следует подумать о том, чтобы продлить план работы Группы экспертов на период после 2021 года в качестве площадки для обмена информацией о киберпреступности между специалистами-практиками.

ss) Некоторые выступавшие выразили мнение, что повышению эффективности международного сотрудничества в вопросах борьбы с киберпреступностью будет способствовать разработка и принятие конвенции о противодействии киберпреступности под эгидой Организации Объединенных Наций.

tt) Разработку новой конвенции было рекомендовано доверить экспертам УНП ООН в Вене.

uu) Несколько выступавших рекомендовали Комиссии по предупреждению преступности и уголовному правосудию продлить мандат международной группы экспертов и принять решение о плане работы на период после 2021 года, в который следует включить новые формы киберпреступности и изучение вопросов, связанных с сексуальными надругательствами над детьми и их эксплуатацией в интернете.

vv) Было также высказано мнение, что специальному межправительственному комитету экспертов открытого состава, учрежденному во исполнение резолюции 74/247 Генеральной Ассамблеи для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, не следует приступать к работе, пока Группа экспертов не согласует свои рекомендации и не направит их Комиссии по предупреждению преступности и уголовному правосудию в 2021 году.

ww) Другие ораторы выразили мнение, что в свете принятия резолюции 74/247 Генеральной Ассамблеи в продолжении работы группы экспертов после 2021 года нет необходимости. Это позволит сконцентрировать внимание на выполнении этой резолюции и проведении переговоров по новой конвенции и оптимальным образом использовать имеющиеся финансовые ресурсы.

xx) Представители многих государств-членов в своих выступлениях приветствовали принятие резолюции 74/247 Генеральной Ассамблеи. При этом отмечалось, что разработка новой конвенции согласно этой резолюции должна вестись на всеохватной, прозрачной и консенсусной основе по аналогии с тем, как в прошлом в рамках Организации Объединенных Наций проходил процесс разработки Конвенции об организованной преступности и Конвенции против коррупции.

yy) Всем государствам-членам было рекомендовано принять активное участие в работе специального комитета по разработке новой конвенции.

zz) Вместе с тем другими ораторами было отмечено, что содержание новой конвенции должно учитывать уже действующую нормативно-правовую базу и акты и не должно вступать с ними в противоречие. В новой конвенции было рекомендовано оговорить такие вопросы, как трансграничный сбор доказательств, криминализация и уважение суверенитета.

aaa) Международному сообществу следует уделять первоочередное внимание развитию потенциала и предоставлению других видов помощи для расширения возможностей национальных органов в области противодействия

киберпреступности, особенно связанной с сексуальными надругательствами над детьми и их эксплуатацией в интернете.

bbb) Государствам-членам следует оказывать друг другу максимально возможную взаимную правовую помощь в получении электронных доказательств, в том числе по делам, связанным с использованием информационно-коммуникационных технологий для совершения террористических актов или финансирования терроризма либо для подстрекательства к таким действиям; было также отмечено, что частные структуры обязаны сотрудничать с национальными властями в этой области.

ccc) Государствам-членам следует подумать о выделении средств на создание специальных централизованных подразделений по противодействию киберпреступности и региональных технических подразделений по расследованию уголовных преступлений.

ddd) Государствам-членам следует также рассмотреть возможность создания внутри центральных органов, отвечающих за оказание взаимной правовой помощи, особых отделов по борьбе с киберпреступностью в качестве экспертных центров по вопросам международного сотрудничества в этой сложной области. Такие специальные отделы будут не только полезны в повседневной практике оказания взаимной правовой помощи, но и позволят оказывать целенаправленную помощь в создании потенциала, например в области подготовки кадров для удовлетворения потребностей национальных и иностранных органов власти в быстром и эффективном получении взаимной правовой помощи, связанной с обеспечением электронных доказательств по делам о киберпреступлениях.

eee) Государствам-членам следует задуматься о ведении электронных баз данных для облегчения доступа к статистическим данным по входящим и исходящим запросам о взаимной правовой помощи, связанной с электронными доказательствами, с целью обеспечить возможность оценки эффективности.

fff) Государствам-членам следует напомнить о необходимости действовать через центральные органы при передаче просьб о взаимной правовой помощи и взаимодействии с компетентными органами по вопросам их выполнения с целью соблюдения требований действующих договоров и сокращения задержек в процессе работы.

ggg) Добиваясь получения необходимых данных для расследования киберпреступлений, государствам следует действовать на основе проверенных и испытанных на практике международных документов, поскольку расследование подобных дел носит комплексный характер и требует наличия институциональной базы, доказавшей свою устойчивость и эффективность. В этой связи было особо отмечено, что уже многие годы стандартом в области обеспечения электронных доказательств служит Конвенция Совета Европы о киберпреступности, позволяющая правоохранительным органам всего мира на повседневной основе добиваться реальных результатов. Во избежание правовых коллизий между требованиями законодательства государствам было рекомендовано при издании прямых распоряжений о предоставлении информации руководствоваться положениями законодательства государства местонахождения поставщика интернет-услуг, которому направляется запрос, либо государства, гражданином которого является подозреваемый.

hhh) Было рекомендовано разработать нормативно-правовую базу, в которой было бы ясно указано, что для принятия решения о возбуждении следствия при отсутствии территориальной привязки нужно попытаться установить, какая территория затронута преступлением и в каком месте требуется обеспечить бесперебойную работу автоматизированных сетей, исходя из чего можно будет проводить консультации о подсудности и надлежащем порядке дальнейшего расследования.

iii) Было рекомендовано обеспечить, чтобы в киберпространстве действовало международное право, включая принципы государственного

суверенитета, территориальной целостности и невмешательства во внутренние дела, не допускать использования информационно-коммуникационных технологий в качестве оружия, осудить совершение кибератак при поддержке государств и привлекать к ответственности стоящих за ними лиц.

jjj) При условии соблюдения требований национального законодательства запрашиваемым государствам следует по мере возможности содействовать выполнению просьб о проведении расследования и сборе доказательств, если такие просьбы не связаны с ограничением личной свободы или имущественных прав либо оказывают на них минимальное влияние.

kkk) Государствам следует создать механизм быстрого реагирования и канал связи для оказания судебной помощи и сотрудничества между правоохранительными органами в борьбе с киберпреступностью и рассмотреть возможность обмена правовыми документами и электронными доказательствами в онлайновом режиме при условии их удостоверения электронными подписями и с помощью других технических средств.

lll) Международному сообществу следует унифицировать порядок применения различных методов расследования киберпреступлений и усовершенствовать нормы национального законодательства, регулирующие обязательства поставщиков интернет-услуг по хранению данных файлов журнала событий.

mmm) Государствам следует препятствовать выводу незаконных доходов от киберпреступлений за рубеж и укреплять международное сотрудничество в области возвращения активов, связанных с киберпреступностью.

nnn) Государствам следует уважать суверенитет других государств при установлении своей юрисдикции в отношении киберпреступлений и не следует злоупотреблять правом на осуществление экстерриториальной юрисдикции в отношении киберпреступлений, с которыми у них отсутствует достаточная и реальная связь. В целях разрешения юрисдикционных споров государствам рекомендуется оставаться на связи и консультироваться друг с другом.

ooo) Важно обеспечить, чтобы информационно-коммуникационные технологии можно было безопасно использовать для связи и информирования людей во всем мире, независимо от статуса территорий, на которых проживают пользователи.

B. Предупреждение киберпреступности

14. В соответствии с планом работы Группы экспертов в настоящем пункте Докладчиком обобщены замечания, высказанные государствами-членами в ходе совещания по пункту 3 повестки дня «Предупреждение киберпреступности». Нижеизложенные предварительные рекомендации и выводы были высказаны государствами-членами, и их включение в доклад не означает одобрения Группой экспертов, а порядок перечисления не отражает степени важности.

a) Следует признать, что предупреждение киберпреступности является обязанностью не одного государства, а требует участия всех заинтересованных сторон, включая правоохранительные органы, частный сектор, особенно поставщиков интернет-услуг, неправительственные организации, учебные заведения, научные круги и рядовых граждан.

b) Было рекомендовано обеспечить, чтобы у граждан был доступ к таким инструментам предупреждения киберпреступности, как онлайн-платформы, аудиоклипы и наглядные информационные материалы, изложенные простым и понятным языком, а также платформы для сообщения о нарушениях.

c) Было выражено мнение о необходимости разработки долгосрочных государственных стратегий предупреждения киберпреступности,

предусматривающих проведение информационных кампаний на тему безопасного пользования интернетом.

d) Тему кибербезопасности следует включить в программу начальных, средних и высших учебных заведений для повышения осведомленности учащихся и преподавателей. В идеале такую работу следует проводить в рамках национальной стратегии кибербезопасности. В интересах предупреждения киберпреступности государствам следует делиться друг с другом опытом реализации стратегий кибербезопасности. Кроме того, государствам следует уделять особое внимание проведению профилактической работы с молодежью, в том числе лицами, впервые совершившими правонарушения, ради профилактики рецидивизма.

e) В рамках работы по предупреждению и противодействию киберпреступности государствам следует уделять особое внимание профилактике и пресечению гендерного насилия, в частности насилия в отношении женщин и девочек, и преступлений на почве ненависти.

f) Профилактическая работа должна носить упреждающий, регулярный и непрерывный характер и проводиться с учетом интересов социально уязвимых категорий населения.

g) Пересечение сфер деятельности и взаимодействие структур государственного и частного секторов в области больших данных и центры обработки больших массивов данных могут представлять зону повышенного риска, особенно в сфере здравоохранения, как наглядно показала текущая пандемия, а также в других областях. Государствам следует обратить особое внимание на регулирование законного доступа к таким данным и их защиту от кибератак.

h) В целях предупреждения киберпреступности поставщикам интернет-услуг следует взять на себя больше ответственности за применение профилактических мер безопасности («по умолчанию»); следует также разработать международные стандарты в отношении содержания файлов журнала событий и сроков их хранения поставщиками интернет-услуг. Помимо этого, следует четко определить обязанности поставщиков интернет-услуг по выявлению, предотвращению и пресечению киберпреступлений.

i) Для успешного предупреждения и противодействия киберпреступности необходимо развивать государственно-частные партнерства, в том числе сотрудничество в области обмена информацией с заинтересованными сторонами, занимающимися вопросами кибербезопасности, и крупными технологическими компаниями.

j) Государствам следует организовать учебную подготовку для судей, специализирующихся на делах о киберпреступлениях, и обеспечить следственные органы высокоэффективными средствами для отслеживания операций с криптовалютой и противодействия ее использованию в преступных целях.

k) Государствам следует усовершенствовать стратегии борьбы с использованием цифровых технологий преступными группами для сокрытия своей деятельности и каналов связи.

l) Необходимо разработать решения для обеспечения возможности прямого сотрудничества между национальными органами и поставщиками интернет-услуг при соблюдении принципа верховенства права, прав человека и требований защиты данных.

m) При разработке мер предупреждения киберпреступности государствам следует обеспечивать свободу печати.

n) Было рекомендовано наращивать коллективный потенциал компетентных учреждений и изменить подход к противодействию киберпреступности с реактивного на превентивный; было также рекомендовано создать надежный

механизм для стимулирования и облегчения обмена оперативными данными о возможных способах совершения преступлений.

o) Государствам-членам было рекомендовано продолжать активную профилактическую работу на национальном и международном уровнях и уделять особое внимание таким превентивным мерам, как проведение информационно-разъяснительной работы об опасности киберпреступности и информационных кампаний, посвященных конкретным методам совершения киберпреступлений, включая фишинг и использование вредоносных программ (программ-вымогателей), и ориентированных на разную целевую аудиторию — от молодежи до людей старшего возраста. Государствам-членам было также рекомендовано и далее работать над повышением вероятности привлечения к ответственности и наказания правонарушителей и предупреждением преступности путем выявления и пресечения незаконной деятельности в интернете. Органам полиции и прокуратуры следует прилагать усилия к выявлению киберугроз, оповещению о них и принятию необходимых мер реагирования. Огромную важность имеет развитие государственно-частных партнерств. Подобные профилактические мероприятия не требуют принятия дополнительных законов и нормативных актов.

p) Из-за сохранения «цифрового разрыва» некоторые развивающиеся страны не имеют возможности предупреждать, выявлять и пресекать киберпреступления и поэтому более уязвимы перед создаваемыми ею угрозами.

q) УНП ООН было настоятельно рекомендовано и далее оказывать техническую помощь в области предупреждения и противодействия киберпреступности при поступлении ему соответствующих просьб.

r) Будущие международные инструменты предупреждения киберпреступности должны быть доступны для всех желающих во всем мире независимо от статуса страны или территории, гражданином или резидентом которой является заинтересованное лицо.

s) Необходимо обеспечить повсеместную защиту базовых прав человека и основных свобод, в том числе в цифровой сфере и киберпространстве, независимо от государственных границ и без какого-либо постороннего вмешательства или ограничений.

t) Киберпространство и киберпреступность не привязаны к конкретной территории и не знают государственных границ и преград. Поэтому в борьбе с киберугрозами международному сообществу следует сохранять сплоченность.

u) Киберпространство является уникальным глобальным пространством, и ввиду отсутствия международного кодекса поведения следует прилагать дальнейшие усилия к разработке правил, принципов и норм ответственного поведения государств в этой области. В этом контексте всем государствам-членам следует отказаться от угроз или применения силы против важнейших объектов инфраструктуры других государств.

v) Государствам-членам рекомендуется и далее проводить эффективную профилактическую работу на национальном и международном уровнях, уделяя особое внимание принятию превентивных мер, направленных на повышение осведомленности о рисках, связанных с киберпреступностью, и вероятности привлечения к ответственности и наказания правонарушителей, и прилагая усилия к предупреждению дальнейших преступлений путем выявления и пресечения незаконной деятельности в интернете.

w) Следует проводить различие между мерами обеспечения кибербезопасности и мероприятиями по борьбе с киберпреступностью. Государствам следует разработать как национальную стратегию противодействия киберпреступности, предусматривающую разработку национального законодательства или политики в области предупреждения киберпреступности, так и национальную стратегию кибербезопасности. Национальные стратегии противодействия киберпреступности должны предусматривать такие направления работы, как

предупреждение киберпреступности, развитие государственно-частного партнерства, укрепление потенциала системы уголовного правосудия и повышение осведомленности путем публикации судебных решений.

x) Странам следует вести сбор данных по широкому спектру вопросов для обеспечения лучшего понимания тенденций с целью выработки обоснованной политики и оперативных мер борьбы с киберпреступностью.

y) При разработке стратегий предупреждения киберпреступности надлежит учитывать необходимость защиты прав человека.

z) Одним из направлений национальных стратегий противодействия киберпреступности должно быть развитие потенциала системы уголовного правосудия. Следует уделять приоритетное внимание оказанию помощи развивающимся странам в укрепления потенциала правоохранительных органов в области предупреждения киберпреступности.

aa) Государствам-членам следует пользоваться возможностью получения помощи в наращивании потенциала в рамках Глобальной программы УНП ООН по борьбе с киберпреступностью и других инициатив, включая расширенный проект Глобальной программы действий Совета Европы по борьбе с киберпреступностью.

bb) Государствам следует разрабатывать и развивать программы поддержки жертв киберпреступлений.

cc) Государствам следует проводить опросы для оценки воздействия киберпреступности на бизнес, в том числе для сбора информации о принимаемых мерах, подготовке сотрудников, видах инцидентов в сфере кибербезопасности, с которыми сталкиваются коммерческие предприятия, и расходах на предотвращение подобных инцидентов и устранение их последствий.

dd) Государствам следует оказывать поддержку бизнесу и профессиональным сообществам в повышении осведомленности о рисках киберпреступности, реализации стратегий смягчения последствий кибератак и совершенствовании методов работы в киберпространстве, поскольку подобные мероприятия в дальнейшем оказывают значительный профилактический эффект.

ee) Необходимо внимательно изучать способы совершения киберпреступлений путем анализа оперативных данных и проведения криминологических исследований с целью более эффективного использования имеющихся ресурсов и выявления уязвимостей.

ff) Государствам следует рассмотреть возможность создания координационной платформы для мгновенного обмена данными о выявленных инцидентах и новых тенденциях в сфере киберпреступности. Государствам следует также подумать о создании криминалистических наблюдательных центров для отслеживания угроз и тенденций киберпреступности.

gg) Странам следует задуматься о принятии конкретных и целенаправленных мер для обеспечения безопасности детей в интернете. В рамках такой работы необходимо обеспечить, чтобы национальная нормативно-правовая база, практические договоренности и механизмы международного сотрудничества обеспечивали возможность сообщать о фактах сексуальных надругательств над детьми и эксплуатации детей в интернете, выявлять и расследовать такие факты, осуществлять уголовное преследование в связи с ними и принимать сдерживающие меры.

hh) Важным партнером в предупреждении киберпреступности является отрасль информационных технологий. Странам следует подумать о создании механизмов сотрудничества с отраслью, в том числе в вопросах переадресации сообщений о нарушениях в компетентные национальные органы и удаления из сети материалов вредоносного и противозаконного содержания, в частности

материалов с изображением сцен сексуальной эксплуатации детей и жестокого насилия.

ii) Следует на регулярной основе выпускать бюллетени с информацией о предотвращенных инцидентах и доводить их до сведения пользователей, организаций и других заинтересованных сторон с целью содействия предотвращению инцидентов в сфере кибербезопасности, потенциально способствующих преступной деятельности.

jj) В целях предупреждения киберпреступности необходимо разработать научно обоснованную методику и стандартный порядок обмена информацией в режиме реального времени.

kk) Следует разработать механизм регистрации всех онлайновых услуг и установить минимальные базовые стандарты безопасности путем национального регулирования.

ll) Государствам следует изучить возможность использования искусственного интеллекта для создания систем, которые будут автоматически менять конфигурацию при обнаружении кибератаки.

mm) Было рекомендовано создать глобальную базу данных о нарушениях, связанных с криптовалютой и использованием больших массивов данных в преступных целях, а также согласованно провести глобальный стратегический обзор угроз, создаваемых преступной деятельностью в даркнете.

nn) Следует поощрять региональные и международные инициативы, направленные на укрепление кибербезопасности, в частности обмен информацией о крупномасштабных кибератаках.

oo) Государства могли бы рассмотреть возможность создания международной системы обмена информацией о киберугрозах с целью обмена сведениями и изучения технологий и методов совершения преступлений, создающих новые угрозы в сфере безопасности.

pp) Государствам рекомендуется создать многоуровневую систему кибербезопасности, применять разные технологии информационной безопасности и механизмы управления для разных информационно-коммуникационных систем и обеспечить защиту критических объектов инфраструктуры от кибератак.

qq) Государствам следует активно привлекать женщин-экспертов к работе по предупреждению и расследованию киберпреступлений.

rr) Для обобщения национального и регионального опыта следует создать многосторонний банк данных, который будет способствовать распространению передовой практики, выработанной в разных контекстах.

ss) Следует принимать более активные меры для борьбы с распространением высказываний, направленных на разжигание ненависти и носящих экстремистский и расистский характер.

tt) Следует проводить более активную информационную работу по проблеме киберзапугивания и угроз применения насилия и жестокого обращения в интернете и оказывать помощь нормотворческой деятельности, направленной на борьбу с этими явлениями.

uu) Следует наладить сотрудничество по вопросам наращивания потенциала в области предупреждения киберпреступности с другими региональными структурами и организациями (например, ОАГ), а также с такими многосторонними механизмами, как Глобальный форум по обмену опытом в области компьютерных технологий.

vv) Государствам рекомендуется воспользоваться возможностью разработки новой конвенции о киберпреступности для выработки единообразных норм в области предупреждения преступности, которые будут способствовать принятию более согласованных мер разными странами.

ww) Государствам было рекомендовано выделять средства на развитие кадрового потенциала с целью повышения профессиональной квалификации сотрудников разных секторов системы уголовного правосудия, поскольку такая работа является действенной мерой предупреждения киберпреступности, оказывающей мощный сдерживающий эффект.

xx) УНП ООН следует способствовать обмену успешным передовым опытом в области принятия эффективных мер предупреждения киберпреступности.

III. Резюме обсуждений (резюме Председателя)

15. По итогам совещания Секретариат в тесном сотрудничестве с Председателем подготовил нижеследующее резюме обсуждений в соответствии с предложением по организации работы, которое было распространено среди членов расширенного бюро Группы экспертов 13 июля 2020 года и утверждено Группой при открытии совещания. Резюме не выносилось на обсуждение и утверждение в ходе совещания. По этой причине резюме, представленное в разделах A — C ниже, выходит за авторством Председателя.

A. Международное сотрудничество

16. На 1, 2 и 3-м заседаниях 27 и 28 июля 2020 года Группа экспертов рассмотрела пункт 2 повестки дня «Международное сотрудничество».

17. В обсуждении этого пункта участвовали: Джордж-Мария Тиендезва (Нигерия), Ганцян Чжан (Китай), Аморнчай Лилакаджонджит (Таиланд), Маркко Кюннапу (Эстония), Вадим Сушик (Российская Федерация), Педро Ханисес (Аргентина), Стивен МакГлинн (Австралия) и Шери Л. Шепард-Пратт (Соединенные Штаты).

18. В ходе обсуждения выступавшие отметили стремительный рост масштабов киберпреступности, в том числе под влиянием трудностей, создаваемых пандемией COVID-19, и подчеркнули важность укрепления международного сотрудничества в целях эффективного решения проблемы компьютерных преступлений и преступлений, совершаемых с помощью компьютерных технологий, которые носят транснациональный характер и отличаются большой изощренностью и высокой адаптируемостью к меняющимся обстоятельствам и приоритетам. В этой связи многие выступавшие сообщили о принятии мер и/или проведении реформ на национальном уровне с целью разработки и реализации стратегий и политики в области кибербезопасности, принятии и/или модернизации законодательства о киберпреступности, применении новых следственных методов для сбора электронных доказательств и содействии международному сотрудничеству в борьбе с киберпреступностью путем принятия эффективных мер и развития потенциала и инфраструктуры на внутригосударственном уровне.

19. Выступавшие отмечали, что трудности, возникающие из-за несогласованности положений о криминализации, пробелов в процессуальных полномочиях правоохранительных органов и органов уголовного правосудия и коллизии юрисдикций в вопросах получении электронных доказательств, требуют от государств-членов активизировать усилия по налаживанию эффективного и более тесного регионального и международного сотрудничества в борьбе с киберпреступностью. В этой связи было подчеркнуто, что, хотя международное сотрудничество играет жизненно важную роль в противодействии и предупреждении киберпреступности, оно должно осуществляться с соблюдением принципов уважения государственного суверенитета и национального законодательства и, в отсутствие применимого договора, на основе взаимности, а также с учетом различий в возможностях и ресурсах, имеющихся у государств-членов, особенно развивающихся стран.

20. Было отмечено, что со времени последнего совещания Группы экспертов в работе Третьего комитета Генеральной Ассамблеи произошли изменения, придавшие новый аспект обсуждению темы киберпреступности на международном уровне в связи с принятием Генассамблеей резолюции 74/247, в которой она постановила учредить специальный межправительственный комитет экспертов открытого состава, представляющий все регионы, для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

21. Ряд ораторов высказал мнение, что разработка конвенции о противодействии киберпреступности под эгидой Организации Объединенных Наций будет способствовать повышению эффективности международного сотрудничества в области борьбы с киберпреступностью и будет наиболее адекватным ответом на киберпреступность со стороны международного сообщества. В этой связи они подчеркнули, что разработка нового глобального документа о борьбе с киберпреступностью позволит, в частности, учесть проблемы и интересы всех государств-членов, особенно развивающихся стран, и поможет ликвидировать правовые пробелы в этой области. Несколько других выступавших выразили мнение, что Конвенция Совета Европы о киберпреступности имеет ограниченную сферу применения в силу своего регионального характера и низкого уровня ратификации, отсутствия цельной концепции и ввиду того, что она не учитывает современные тенденции киберпреступности и не вполне подходит для развивающихся стран.

22. Другие выступавшие высказались за то, чтобы эффективнее использовать уже имеющиеся международные документы, рамочные соглашения и механизмы, такие как Конвенция об организованной преступности, Конвенция Совета Европы о киберпреступности и Интерпол. Говоря о Конвенции об организованной преступности, несколько ораторов подчеркнули, что она может служить особенно полезным инструментом международного сотрудничества в борьбе с киберпреступностью. Одна из выступавших подтвердила, что ее страной было направлено и получено большое число просьб о помощи в соответствии с положениями Конвенции как правовым основанием для международного сотрудничества по вопросам, связанным с электронными доказательствами по делам о киберпреступлениях. В пользу применения этого инструмента та же выступавшая отметила, что в рамках большинства значимых дел киберпреступления связаны с той или иной формой организованной преступности, например операциями на подпольных рынках, а за их совершением стоят преступники из разных стран, и что число преступлений с участием организованных преступных групп нередко существенно превосходит количество случаев совершения преступлений хакерами-одиночками.

23. Несколько выступавших выразили мнение, что Конвенция Совета Европы о киберпреступности обеспечивает достаточную основу для разработки надлежащих мер противодействия киберпреступности на внутригосударственном и международном уровнях. Они напомнили, что Конвенция насчитывает 65 государств-участников, из которых 21 не является членом Совета Европы, и успешно используется в качестве основы международного сотрудничества, модели для разработки национального законодательства и стандарта в области наращивания потенциала и технической помощи. По мнению выступавших, в обозримом будущем Конвенция останется наиболее актуальным и перспективным многосторонним соглашением по киберпреступности, доступным для стран, ищущих самый короткий путь к реформированию законодательства о киберпреступности, укреплению потенциала правоохранительных органов и расширению международного сотрудничества, что, однако, не должно мешать обсуждению вопроса о разработке нового документа под эгидой Организации Объединенных Наций в будущем. Вместе с тем один из ораторов также отметил, что одной из проблем Конвенции является ее слабое осуществление в некоторых государствах, поэтому принятие мер на основе ее положений следует рассматривать как постоянно эволюционирующий процесс.

24. Было упомянуто о продолжении переговоров по второму дополнительному протоколу к Конвенции Совета Европы о киберпреступности, в котором будут установлены четкие правила и более эффективные процедуры выполнения положений о налаживании более эффективного и оперативного международного сотрудничества и допустимости прямого сотрудничества с поставщиками услуг в других правовых системах в отношении просьб о предоставлении информации об абонентах, обеспечении сохранности данных и оказании экстренной помощи, заложена основа для применения практических методов, связанных с трансграничным доступом к данным, и предусмотрены надежные гарантии безопасности, включая требования о защите данных.

25. Некоторые выступавшие обратили внимание Группы экспертов на опыт международного сотрудничества, накопленный в рамках таких региональных организаций, как ОАГ, и таких региональных сетей, Американское полицейское сообщество, а один из ораторов упомянул о том, что его страна продолжает тесно взаимодействовать с Африканской организацией полицейского сотрудничества (АФРИПОЛ) в вопросах борьбы с киберпреступностью.

26. В свете ведущихся дискуссий по согласованию плана и порядка дальнейшей работы специального межправительственного комитета экспертов по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях было подчеркнуто, что новая конвенция должна быть нацелена на обеспечение всеохватности и достижение максимально возможного числа ратификаций и/или присоединений по примеру Конвенции об организованной преступности и Конвенции против коррупции. Был выражен призыв к тому, чтобы работа над конвенцией велась на прозрачной, всеохватной и консенсусной основе с учетом выводов и рекомендаций Группы экспертов и прогресса, уже достигнутого международным сообществом в этой области, а также необходимости способствовать развитию свободного, открытого и безопасного интернета и обеспечить защиту прав человека, включая защиту персональных данных и права на неприкосновенность частной жизни, в киберпространстве. Несколько выступавших отметили, что любая новая конвенция должна разрабатываться на основе консенсуса и учитывать положения действующих соглашений и договоров, не дублируя их и не вступая с ними в противоречие, и не должна мешать выполнению ранее взятых обязательств либо вынуждать государства отказываться от их выполнения или отступать от них.

27. Некоторые ораторы отметили, что по мере развития облачных технологий все больше электронных доказательств хранится на серверах, находящихся за пределами территориальной юрисдикции государств-членов. В этой связи было отмечено, что с учетом транснациональной природы и недолговечности электронных доказательств эффективным способом решения срочных вопросов и преодоления трудностей, обусловленных экстренным характером ситуации, является прямое сотрудничество, особенно в области обмена оперативными данными, которое позволяет сократить время, требуемое для задействования каналов взаимной правовой помощи. Было отмечено, что, хотя прямое сотрудничество по-прежнему опирается на взаимное доверие, ему могла бы способствовать стандартизация формы запросов и процедур оперативного обеспечения сохранности данных, а также более активное использование таких уже существующих механизмов, как глобальная полицейская система защищенной связи Интерпола I-24/7 и сети государственных и частных центров реагирования на инциденты информационной безопасности. Для ускорения процесса может также потребоваться разработка новых процедур обмена информацией и доказательствами.

28. Было отмечено, что одним из ключевых моментов при расследовании киберпреступлений и проведении цифровой экспертизы является сохранение целостности электронных доказательств и обеспечение их подлинности и допустимости использования в качестве доказательств в соответствующем уголовном судопроизводстве, в связи с чем принципиальное значение имеют такие

вопросы, как порядок хранения и передачи доказательств и создание криминалистических копий. Исходя из этого было отмечено, что следует уделять первоочередное внимание совершенствованию специальных методов расследования, предназначенных не только для сбора электронных доказательств, в том числе в даркнете, но и для проведения финансовых расследований. В этой связи один из ораторов высказал мнение, что неотъемлемой частью правоохранительной деятельности по противодействию киберпреступности должна быть борьба с отмыванием денег и финансированием терроризма и меры по возвращению активов. Другие выступавшие упомянули о том, что использование криптовалюты усложняет расследование дел о незаконных финансовых потоках, связанных с доходами от преступной деятельности, и осуществление уголовного преследования в связи с ними. Ряд выступавших подчеркнул необходимость и важность изучения вопроса о том, каким образом обеспечить, чтобы работники уголовного правосудия и правоохранительных органов могли по максимуму использовать для борьбы с киберпреступностью такие новейшие технологии, как искусственный интеллект и современные информационно-коммуникационные технологии.

29. Одним из важнейших условий принятия эффективных мер противодействия киберпреступности и другим видам преступлений, в связи с которыми могут требоваться электронные доказательства, было названо оперативное выполнение просьб о взаимной правовой помощи. Некоторые выступавшие упомянули о том, что на эффективность взаимной правовой помощи в области противодействия киберпреступности негативно влияют такие факторы, как различия в требованиях законодательства и подходах к криминализации, затрудняющие выполнение требования об обоюдном признании деяния преступлением, а также отсутствие стандартных требований к содержанию и формату соответствующих запросов.

30. В целях ускорения международного сотрудничества и упорядочения процесса оказания взаимной правовой помощи было предложено установить особый режим регулирования доступа к информации об абонентах. В этой связи было отмечено, что в рамках переговоров по второму дополнительному протоколу к Конвенции Совета Европы о киберпреступности рассматриваются меры, которые должны позволить быстрее получать такую информацию.

31. Один из ораторов упомянул об основных мерах, которые могут быть приняты странами для сокращения сроков выполнения просьб о взаимной правовой помощи; к ним относится повышение квалификации и уровня подготовки персонала путем изучения требований, предъявляемых к просьбам о взаимной правовой помощи отдельными странами, что должно сократить время рассмотрения просьб и облегчить их выполнение без запроса дополнительных сведений; а также использование прямых каналов связи между центральными органами вместо официальных дипломатических каналов.

32. Несколько ораторов подчеркнули необходимость модернизации, упорядочения и ускорения практики взаимной правовой помощи за счет электронной передачи просьб о международном сотрудничестве, которая с недавних пор практикуется некоторыми странами иберо-американского региона. В этой связи была высказана мысль, что центральные и другие компетентные органы могли бы передавать официальные и межведомственные запросы о помощи по электронной почте, а для передачи просьб об обеспечении сохранности данных пользоваться круглосуточными каналами связи.

33. Несколько выступавших коснулись вопроса о трансграничном доступе к хранящимся компьютерным данным, напомнив, что Конвенция Совета Европы о киберпреступности содержит особое положение на этот счет (статья 32), и подчеркнув, что к применению таких мер следует подходить с осторожностью, соблюдая баланс между нуждами следствия и уважением прав человека и государственного суверенитета.

34. Многие выступавшие подчеркнули, что большое значение для укрепления международного сотрудничества в борьбе с киберпреступностью имеет

развитие сетевых связей. Было отмечено, что круглосуточные сети, объединяющие ответственных контактных лиц во всех странах-участницах, играют важную роль в содействии сотрудничеству, особенно в экстренных ситуациях. Такие сети облегчают выполнение просьб об обеспечении сохранности данных, которые впоследствии нередко становятся предметом просьб о взаимной правовой помощи; подобные просьбы обычно выполняются за несколько дней, а то и часов. Многие выступавшие отмечали, что участие в работе круглосуточных сетей и поддержание контактов с сотрудниками по связи имеет огромную важность для предотвращения риска задержек в расследовании киберпреступлений, учитывая то обстоятельство, что доказательства могут быть быстро удалены, а данные утрачены или изменены. По этой причине выступавшие выражали согласие с тем, что центральным и другим компетентным органам следует налаживать отношения и укреплять взаимное доверие посредством прямых контактов и консультаций, а также через региональные и международные сети судебных и правоохранительных органов или специализированные сети по противодействию киберпреступности. В качестве примера были упомянуты недавно созданная сеть сотрудничества судебных органов в Юго-Восточной Азии (сеть SeaJUST); сеть Cybernet Иберо-американской ассоциации государственных прокуроров (ИААГП), объединяющая специализированные контактные пункты, созданные при прокуратурах и министерствах всех государств — членов ИААГП); и Сеть сотрудничества по уголовным делам ИААГП.

35. Некоторые выступавшие выразили мнение, что в составе центральных органов следует создать специализированные структуры или подразделения по противодействию киберпреступности, которые будут выступать в качестве экспертных центров по вопросам международного сотрудничества в этой сложной области. Такие специализированные структуры или подразделения будут располагать необходимыми ресурсами и опытом для поддержки повседневной работы режима взаимной правовой помощи и позволят организовать целенаправленное обучение сотрудников национальных и зарубежных органов по вопросам быстрого и эффективного получения помощи и электронных доказательств в связи с делами о киберпреступлениях.

36. Многие выступавшие отмечали важность поощрения и укрепления сотрудничества между национальными органами власти и частным сектором, в частности поставщиками услуг связи и интернет-услуг, в целях улучшения сохранности данных и доступа к ним и обеспечения своевременного реагирования на киберпреступления, особенно в рамках транснациональных дел. Для содействия одинаковому пониманию требований и процедур всеми сторонами было предложено разработать систему ориентиров и указаний. Была подчеркнута необходимость принятия положений о допустимости непосредственного направления поставщикам интернет-услуг из других правовых систем просьб о содействии в получении информации об абонентах и обеспечении сохранности данных. Была выражена надежда на то, что в обсуждаемом втором дополнительном протоколе к Конвенции Совета Европы о киберпреступности будет предложено более комплексное решение вопросов прямого сотрудничества с субъектами частного сектора.

37. Один из ораторов подчеркнул, что уникальную роль в содействии сотрудничеству между полицейскими службами играет Интерпол благодаря своим национальным центральным бюро, созданным в каждой стране, системе связи I-24/7, уведомлениям и базам данных и что в рамках Глобальной программы Интерпола по противодействию киберпреступности была, в частности, создана аналитическая платформа по киберпреступности и обеспечены возможности для совместной работы с целью содействия обмену знаниями и координации оперативной деятельности.

38. Многие выступавшие говорили о необходимости уделять первостепенное внимание устойчивому наращиванию потенциала национальных правоохранительных систем и систем уголовного правосудия, включая повышение квалификации специалистов-практиков центральных органов, участвующих в

международном сотрудничестве. Было отмечено, что наращивание потенциала имеет огромное значение, особенно для развивающихся стран, как в плане развития людских ресурсов, инфраструктуры и материально-технической базы, так и в плане преодоления цифрового разрыва с развитыми странами.

39. Было выражено широкое согласие с тем, что укрепление потенциала и предоставление технической помощи на основе существующих документов являются ценным и эффективным инструментом борьбы с киберпреступностью, поэтому работу в этом направлении следует расширять и проводить в первоочередном порядке, учитывая приоритеты государств-членов. В этой связи несколько ораторов заявили о поддержке своими странами — как донорами, так и получателями помощи — Глобальной программы УНП ООН по борьбе с киберпреступностью и других программ и механизмов технической помощи, в том числе осуществляемых под эгидой Интерпола, а также Расширенной программы глобальных действий Совета Европы по борьбе с киберпреступностью и программы кибербезопасности, учрежденной в соответствии с Декларацией по региональной безопасности, принятой на Форуме тихоокеанских островов в Боэ.

40. Говоря о роли УНП ООН, многие выступавшие особо отмечали необходимость продолжать работу по подготовке и повышению квалификации профильных специалистов по вопросам противодействия киберпреступности с целью укрепления национального потенциала в области выявления и расследования киберпреступлений и содействия обмену передовым опытом, связанным с принятием эффективных и успешных мер предупреждения киберпреступности. Была, в частности, подчеркнута необходимость организовать учебную подготовку для разных категорий работников системы уголовного правосудия и правоохранительных органов, включая судей, прокуроров и сотрудников служб безопасности, обеспечить создание и адекватную организационную структуру специализированных подразделений по расследованию киберпреступлений и осуществлению уголовного преследования в связи с ними и обеспечить доступ к передовым технологиям для расследования киберпреступлений и проведения цифровой экспертизы. Несколько выступавших отметили, что в рамках работы по наращиванию потенциала необходимо учитывать потребности развивающихся стран, уделять особое внимание факторам уязвимости каждой страны с целью оказания адресной технической помощи и содействовать обмену новейшими знаниями в интересах специалистов-практиков и заинтересованных сторон.

41. Один из ораторов упомянул о важности повышения квалификации сотрудников правоохранительных органов и сообщил о работе, проводимой на курсах противодействия киберпреступности, действующих на базе Агентства Европейского союза по подготовке сотрудников правоохранительных органов и Международной академии правоохранительных органов. Было подчеркнуто, что международное сотрудничество в сфере образования и профессиональной подготовки также имеет большое значение. Несколько ораторов выразили мнение о необходимости организовать подготовку судебных работников и судей, специализирующихся на делах о киберпреступности, и обеспечить следственные органы высокоэффективными техническими средствами для отслеживания криптовалют и борьбы с их использованием в преступных целях.

42. Несколько выступавших упомянули о том, что оптимизации процессов оказания взаимной правовой помощи, в том числе предоставлению электронных доказательств, могут способствовать такие нововведения, как добавление модуля электронных доказательств в переработанную версию Программы составления просьб об оказании взаимной правовой помощи УНП ООН. В связи с вопросом роли УНП ООН в оказании технической помощи государствам-членам было также упомянуто о подготовке *Практического руководства по истребованию электронных доказательств из-за рубежа*.

43. Ряд ораторов подчеркнул, что государствам-членам следует воздерживаться от незаконных односторонних действий, идущих вразрез с

международным правом и Уставом Организации Объединенных Наций и препятствующих всестороннему социально-экономическому развитию населения затрагиваемых стран. Было отмечено, что односторонние принудительные меры препятствуют сотрудничеству с национальными правоохранительными органами в расследовании и уголовном преследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий, а также в передаче технических средств, необходимых для обеспечения сохранности электронных доказательств и проведения цифровой судебной экспертизы.

44. Некоторые ораторы выразили озабоченность по поводу кибератак на жизненно важные объекты инфраструктуры, включая объекты здравоохранения, совершаемых отдельными государствами-членами или поддерживаемыми ими группами, и подчеркнули, что подобные действия подлежат решительному осуждению, а все стоящие за ними лица — привлечению к ответственности. Другой оратор выразил серьезную озабоченность в связи с тем, что пандемия COVID-19 привела к возникновению совершенно новой ситуации в секторе здравоохранения, который в дополнение к колоссальным проблемам в сфере здравоохранения еще и оказался прямой мишенью и косвенной жертвой кибератак.

45. Некоторые выступавшие высказали мнение, что Комиссии по предупреждению преступности и уголовному правосудию следует рассмотреть вопрос о продлении плана работы Группы экспертов на период после 2021 года, с тем чтобы сохранить площадку для обмена информацией о киберпреступности между экспертами и практическими работниками, в том числе с целью изучения возможных подходов к борьбе с сексуальными надругательствами над детьми и их сексуальной эксплуатацией в интернете и другими новыми формами киберпреступности. Другие же ораторы подчеркнули, что после того, как Группа экспертов завершит выполнение своего плана работы на итоговом совещании в 2021 году, нет никаких оснований для продления ее мандата в свете принятия резолюции 74/247 Генеральной Ассамблеи и необходимости сосредоточить внимание на осуществлении этой резолюции и проведении переговоров по новой конвенции и в целях оптимального использования имеющихся ресурсов.

46. Один из ораторов отметил, что, хотя мандат Группы экспертов отличается от предусмотренного резолюцией 74/247 Генеральной Ассамблеи, нужно обратить внимание на имеющиеся у них точки соприкосновения и взаимодополняющие элементы. С учетом этого тему международного сотрудничества и создания потенциала, которой занималась Группа экспертов, следует определить в качестве одного из основных направлений будущей работы специального комитета, который будет заниматься согласованием новой конвенции.

47. Другой оратор подчеркнул, что специальному комитету не следует приступать к работе до тех пор, пока Группа экспертов не завершит подготовку своих рекомендаций и не направит их Комиссии по предупреждению преступности и уголовному правосудию в 2021 году.

B. Предупреждение киберпреступности

48. На 4-м и 5-м заседаниях 28 и 29 июля 2020 года Группа экспертов рассмотрела пункт 3 повестки дня «Предупреждение киберпреступности».

49. В обсуждении этого пункта участвовали: Дестино Педро (Ангола), Лиюн Хань (Китай), Бенджапорн Ватчаравуттичаи (Таиланд), Орасио Ассолин (Аргентина), Клаудио Пегеро (Доминиканская Республика) и Педро Верделью (Португалия).

50. В ходе обсуждения было отмечено, что предупреждение киберпреступности стало важным компонентом национальной политики и стратегий, направленных на предупреждение кибератак и угроз информационной безопасности и противодействие им, уменьшение уязвимости киберинфраструктуры и

обеспечение эффективного управления всеми связанными с этим рисками. Было отмечено, что тему предупреждения киберпреступности следует рассматривать в контексте комплексной концепции противодействия киберпреступности, которая может быть реализована на широкой основе для обеспечения постоянной доступности и повышения безопасности интернета и связанных с ним коммуникационных технологий для пользователей.

51. Ряд ораторов подчеркнул, что по мере разработки государствами-членами широкомасштабных стратегий предупреждения киберпреступности им следует помнить о своих международных обязательствах в области прав человека. Многие ораторы поддержали точку зрения, что выработку стратегий и предложений по вопросам предупреждения киберпреступности необходимо вести на основе комплексной концепции, учитывающей тот факт, что киберпреступность может оказывать разное и ассиметричное воздействие на разные категории населения в пределах одной страны и на разные страны, особенно ввиду цифрового разрыва между развитыми и развивающимися странами и в силу того факта, что некоторые развивающиеся страны не имеют возможностей для предупреждения, выявления и противодействия киберпреступности и более уязвимы перед создаваемыми ею угрозами.

52. Было отмечено, что в некоторых юрисдикциях проводится различие между сотрудничеством в области кибербезопасности и программами расследования киберпреступлений и что, хотя эти два аспекта нередко рассматривают как две стороны одной медали, осуществление стратегий противодействия киберпреступности является исключительной прерогативой государства, а обеспечение кибербезопасности — обязанностью целого ряда государственных и частных структур. В развитие этой темы было отмечено, что государственные и частные организации продолжают способствовать повышению осведомленности бизнеса путем осуществления программ повышения квалификации специалистов по информационным бизнес-технологиям в области кибербезопасности.

53. Многими ораторами было отмечено, что важным профилактическим фактором в борьбе с киберпреступностью является разработка стратегий с участием широкого круга заинтересованных сторон. Было подчеркнуто, что юридические, технические и институциональные проблемы, создаваемые киберпреступностью, имеют далеко идущие последствия и могут быть решены только на основе последовательной и всеохватной стратегии, учитывающей уже имеющиеся инициативы и роль разных заинтересованных сторон. С этой точки зрения была подчеркнута необходимость поощрять и расширять участие всех заинтересованных структур в предупреждении киберпреступности и отмечено, что региональные организации, частный сектор и научные круги могут оказать, в первую очередь развивающимся странам, необходимую поддержку в формировании глобальной культуры кибербезопасности.

54. Многие выступавшие высказали мысль, что для успешного реагирования на разноплановые вызовы, возникающие в процессе борьбы с киберпреступностью, необходимо развивать государственно-частное партнерство между такими государственными институтами, как правоохранительные органы и органы уголовного правосудия, и поставщиками услуг связи. Была подчеркнута важность налаживания эффективных государственно-частных партнерств, особенно в вопросах выявления преступлений и оповещения о них, предоставления информации о местонахождении подозреваемых и потерпевших и предоставления, в необходимых случаях, других данных. В связи с вопросом о перспективных партнерствах было отмечено, что поставщикам услуг необходимо брать на себя больше обязанностей по принятию профилактических мер безопасности с целью предупреждения киберпреступлений. Такие обязанности должны быть четко прописаны. Было также подчеркнуто, что любые будущие решения, направленные на обеспечение возможности прямого сотрудничества между национальными органами и поставщиками интернет-услуг, должны быть основаны на принципе верховенства права и обеспечивать соблюдение прав человека и требований защиты данных.

55. Некоторые ораторы обратили внимание Группы экспертов на то, что ответственность за защиту данных в соответствии с правом на неприкосновенность частной жизни лежит не только на государстве, но и на частных компаниях и других структурах и что этот вопрос имеет центральное значение для предупреждения киберпреступности наряду с правом на свободу слова и свободу печати. Было отмечено, что одним из ключевых партнеров в работе по предупреждению преступности является отрасль информационных технологий, представители которой могут сотрудничать с органами государственной власти в вопросах переадресации сообщений о нарушениях компетентным национальным органам и удаления из сети вредоносных и противозаконных материалов, в частности изображений сцен сексуальных надругательств над детьми и жестокого насилия.

56. Было особо упомянуто о важной роли неправительственных организаций и научных кругов в разработке всеохватных комплексных стратегий предупреждения и расследования киберпреступлений, обеспечивающих защиту прав человека, особенно свободу слова и неприкосновенность частной жизни.

57. Многие ораторы выступали за принятие эффективных превентивных мер на национальном и международном уровнях, включающих уголовное преследование и наказание правонарушителей и предупреждение будущих преступлений путем выявления и пресечения незаконной деятельности в интернете. Этот аспект работы был признан важным компонентом политики предупреждения киберпреступности в силу его сдерживающего эффекта и был обсужден вместе с вопросом о необходимости выделения средств на развитие кадрового потенциала с целью повышения квалификации сотрудников разных секторов системы уголовного правосудия, включая экспертов-женщин, которых следует активно привлекать к работе по предупреждению и расследованию киберпреступлений на национальном уровне.

58. Было отмечено, что важной составляющей стратегий предупреждения киберпреступности являются информационно-просветительские кампании и инициативы, направленные на привлечение внимания к новым угрозам и ориентированные на конкретную целевую аудиторию, включая детей. В этом контексте была подчеркнута необходимость уделять первоочередное внимание формированию «культуры кибербезопасности» с целью повышения всеобщей осведомленности о рисках преступной деятельности и киберугрозах, а также выработки общего понимания необходимых мер безопасности и профилактики.

59. Было подчеркнуто, что тему кибербезопасности и рисков, связанных с киберпреступностью и теневой стороной интернета, следует включить в программу начального, среднего и высшего образования и преподавать как учащимся, так и учителям. При этом было отмечено, что в идеале такую работу следует проводить в рамках национальной стратегии кибербезопасности. Некоторые ораторы особо подчеркнули необходимость предотвращать распространение высказываний, направленных на разжигание ненависти и носящих экстремистский и расистский характер, и также бороться с киберзапугиванием и насилием в сети, в том числе по признаку пола и в отношении уязвимых категорий населения, как с помощью образовательных инициатив, так и путем совершенствования нормативно-правовой базы. Кроме того, один из ораторов выразил мнение, что государствам следует уделять особое внимание проведению профилактической работы с молодежью, в том числе лицами, впервые совершившими правонарушения, с целью профилактики рецидивизма.

60. Один из ораторов отметил необходимость создания инструментов для обеспечения безопасности цифровой торговли и выразил мнение, что эту тему следует включить в общую программу развития стран, которые еще не в полной мере пользуются преимуществами такого способа торговли товарами и услугами.

61. Было отмечено, что важным инструментом предупреждения киберпреступности является анализ оперативных данных и проведение криминологических исследований. Было отмечено, что одним из методов выявления угроз и

факторов уязвимости является анализ больших массивов данных из открытых источников (киберпатрулирование), позволяющий оценивать масштабность и серьезность угроз и принимать быстрые меры реагирования путем публикации оповещений, разработки инструкций и организации обучения.

62. Один из ораторов упомянул о сотрудничестве Интерпола с партнерами из государственного и частного секторов с целью выработки эффективных стратегий предупреждения киберпреступности, в том числе путем проведения глобальных информационных кампаний, направленных на поддержку усилий правоохранительных органов по решению проблем, связанных с борьбой с киберпреступностью и несообщением о киберпреступлениях в компетентные органы.

63. Один из выступавших рассказал о работе, проводимой в рамках проекта «Никакого выкупа», осуществляемого в рамках совместной инициативы правоохранительных органов и компаний из сектора информационно-технической безопасности с целью пресечения деятельности преступных групп, занимающихся распространением программ-вымогателей, и оказания помощи жертвам таких программ в восстановлении зашифрованных данных без выплаты выкупа злоумышленникам. Тот же оратор упомянул об использовании Европейской сети по предупреждению преступности для обмена передовым опытом реализации стратегий кибербезопасности.

C. Прочие вопросы

64. На 6-м заседании 29 июля 2020 года Группа экспертов рассмотрела пункт 4 повестки дня «Прочие вопросы». До сведения Комиссии не было доведено никаких вопросов в рамках данного пункта повестки дня.

IV. Организация работы совещания

A. Открытие совещания

65. Совещание открыл Председатель Группы экспертов Доктор Машабане (Южная Африка), который поручил исполнение обязанностей председателя на совещании своему заместителю Андре Риплу (Бразилия).

B. Утверждение повестки дня и другие организационные вопросы

66. На 1-м заседании 27 июля 2020 года Группа экспертов утвердила следующую предварительную повестку дня:

1. Организационные вопросы:
   a) открытие совещания;
   b) утверждение повестки дня
2. Международное сотрудничество
3. Предупреждение киберпреступности
4. Прочие вопросы
5. Утверждение доклада.

C. Заявления

67. С заявлениями выступили эксперты из следующих государств-членов: Австралии, Австрии, Азербайджана, Алжира, Аргентины, Армении, Бразилии,

Венгрии, Венесуэлы (Боливарианская Республика), Вьетнама, Гватемалы, Германии, Гондураса, Греции, Доминиканской Республики, Египта, Израиля, Индии, Индонезии, Ирака, Ирана (Исламская Республика), Испании, Италии, Канады, Китая, Колумбии, Кубы, Ливана, Малайзии, Мексики, Монголии, Нигерии, Нидерландов, Новой Зеландии, Норвегии, Парагвая, Перу, Польши, Португалии, Российской Федерации, Румынии, Соединенного Королевства, Соединенных Штатов, Таиланда, Филиппин, Франции, Чили, Эквадора, Эстонии, Южной Африки и Японии.

68. С заявлением выступил эксперт от Государства Палестина — государства-наблюдателя, не являющегося членом Организации Объединенных Наций[2].

69. С заявлениями выступили также представители следующих межправительственных организаций: Европейского союза, Интерпола и Совета Европы. С заявлением также выступил наблюдатель от Пекинского педагогического университета.

D. Участники

70. В работе совещания приняли участие представители 93 государств-членов, одного государства-наблюдателя, не являющегося членом Организации Объединенных Наций, института сети программы Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия, межправительственных организаций и частного сектора.

71. На совещании был распространен предварительный список участников (UNODC/CCPCJ/EG.4/2020/INF/1).

E. Документация

72. Помимо замечаний государств-членов, полученных в соответствии с планом работы на период 2018–2021 годов, Группе экспертов была представлена аннотированная предварительная повестка дня (UNODC/CCPCJ/EG.4/2020/1).

V. Утверждение доклада

73. На 6-м заседании 29 июля 2020 года Рабочая группа утвердила настоящий доклад.

[2] Наблюдатель от Государства Палестина также сделал заявление от имени Группы 77 и Китая.