Distr.: Limited
28 March 2019
Russian
Original: English

Группа экспертов для проведения всестороннего исследования проблемы киберпреступности
Вена, 27–29 марта 2019 года

Проект доклада

Добавление

II. Перечень предварительных рекомендаций и выводов

A. Правоохранительная деятельность и расследования (*продолжение*)

1. В соответствии с планом работы настоящий пункт содержит подборку предложений, внесенных государствами-членами на заседании по пункту 2 повестки дня под названием «Правоохранительная деятельность и расследования». Настоящие предварительные рекомендации и выводы были представлены государствами-членами, и их включение не означает их одобрения Группой экспертов и порядок их представления не подразумевает оценку их значения:

a) с одной стороны, было высказано мнение, что государствам-членам следует продолжать принимать новые международные меры борьбы с киберпреступностью посредством рассмотрения вопроса о разработке в рамках Организации Объединенных Наций нового глобального правового документа по киберпреступности, в котором будут приняты во внимание озабоченности и интересы всех государств-членов с учетом, в частности, предлагаемого проекта конвенции о сотрудничестве в борьбе с киберпреступностью, представленного Генеральному секретарю 11 октября 2017 года (A/C.3/72/12, приложение);

b) с другой стороны, было высказано мнение, что для рассмотрения вопроса о новом глобальном договоре нет никакой необходимости или целесообразности, поскольку проблемы, связанные с киберпреступностью и наличием достаточно подготовленных следователей, прокуроров и судей, лучше всего решаются посредством наращивания потенциала, активного диалога и сотрудничества между правоохранительными органами и использования существующих документов, таких как Будапештская конвенция. С учетом этого мнения государствам-членам следует продолжать использовать и/или стать участниками существующих многосторонних правовых документов по киберпреступности, таких как Будапештская конвенция, которую многие государства считают самым надлежащим и конкретным руководящим документом для разработки соответствующего внутреннего законодательства по борьбе с киберпреступностью, как материально-правового, так и процессуального характера, и содействия международному сотрудничеству для борьбы с ней;

c) ввиду транснационального характера киберпреступности и того факта, что подавляющее большинство киберпреступлений в мире совершается организованными группами, государствам-членам следует также шире использовать Конвенцию об организованной преступности с целью содействия обмену информацией и доказательствами в ходе таких уголовных расследований;

d) государствам-членам следует поощрять международное сотрудничество в борьбе с киберпреступностью и участвовать в нем, используя существующие документы, а также заключая двусторонние соглашения на основе принципа взаимности и оказывать поддержку сотрудничеству с УНП ООН, созданию сетей и обмену информацией между судебными и правоохранительными органами на регулярной основе;

e) странам следует повышать квалификацию сотрудников полиции в области расследований киберпреступлений посредством участия в учебных курсах, которые проводятся многими странами, а также УНП ООН и другими региональными партнерами, и направлены на развитие потенциала в области выявления и расследований киберпреступлений и укрепления коллективного потенциала в борьбе с киберпреступностью. Создание потенциала в этой области должно быть направлено, в частности, на удовлетворение потребностей развивающихся стран и решение проблем каждой страны для обеспечения оказания адресной технической помощи, а также содействовать обмену современными знаниями в наилучших интересах получателей такой помощи;

f) странам рекомендуется продолжать предоставлять УНП ООН необходимые мандаты и финансовую поддержку с целью получения ощутимых результатов в осуществлении проектов по наращиванию потенциала в этой области;

g) странам следует выделять средства на подготовку специалистов по расследованию киберпреступлений и налаживание партнерских отношений для использования механизмов сотрудничества в интересах получения важных доказательств;

h) государствам следует продолжать усилия по созданию и поддержке специализированных подразделений, органов или структур по борьбе с киберпреступностью в рамках правоохранительных, прокурорских и судебных органов, обладающих необходимыми знаниями и оборудованием для решения проблем, связанных с киберпреступностью, и сбора и использования электронных доказательств в ходе уголовных разбирательств и обмена ими;

i) с учетом того, что для ликвидации рынков киберпреступности требуются среднесрочные и долгосрочные правоохранительные стратегии, включая сотрудничество с международными партнерами, эти стратегии должны быть упреждающими и предпочтительно ориентированными на борьбу с организованными киберпреступными группами, члены которых могут находиться во многих странах;

j) странам следует продолжать усилия по принятию законодательства материально-правового характера, касающегося новых и возникающих форм преступности в киберпространстве, которое будет содержать технологически нейтральные формулировки для обеспечения учета будущих достижений в области информационно-коммуникационных технологий;

k) внутреннее процессуальное доказательство должно не отставать от технического прогресса, с тем чтобы обеспечить надлежащее оснащение правоохранительных органов для борьбы с преступностью в Интернете. Соответствующее законодательство должно разрабатываться с учетом применимых технических концепций, а также практических потребностей следователей, занимающихся расследованиями киберпреступлений, при условии обеспечения надлежащих процессуальных гарантий, неприкосновенности частной жизни, гражданских свобод и прав человека, а также принципов соразмерности и субсидиарности и гарантий, обеспечивающих судебный надзор. Кроме того, государствам-

членам следует выделять средства на принятие внутреннего законодательства с целью разрешения:

i) просьб об оперативном сохранении компьютерных данных, направляемых лицу, ответственному за осуществление контроля над этими данными, т.е. провайдерам услуг Интернета и связи, с целью сохранения и обеспечения целостности данных в течение определенного периода времени в связи с потенциальной нестабильностью этих данных;

ii) поиска и получения хранящихся на цифровых устройствах данных контента, которые зачастую являются наиболее актуальными доказательствами совершения электронного преступления для аргументирования его состава;

iii) постановлений о подготовке компьютерных данных, которые могут иметь меньшую степень защиты неприкосновенности частной жизни, таких как данные о трафике и абонентские данные;

iv) сбора в режиме реального времени данных о трафике и контенте в соответствующих случаях; и

v) внутренним правоохранительным органам сотрудничать на международном уровне;

l) поскольку расследования киберпреступлений требуют творческого подхода, технической проницательности и совместных усилий прокуратуры и полиции, странам следует поощрять сотрудничество между прокуратурой и полицией на раннем этапе расследования в целях получения достаточных доказательств для предъявления обвинений определенным субъектам;

m) при проведении расследований по делам о киберпреступлениях сотрудники правоохранительных органов должны руководствоваться рекомендациями следователей, с тем чтобы обеспечить соблюдение надлежащих процессуальных норм;

n) национальным правоохранительным органам следует устанавливать контакты и взаимодействовать с национальными провайдерами интернет-услуг и другими частными промышленными группами. Такая информационная работа способствует проведению правоохранительными органами расследований, укрепляя доверие и сотрудничество между заинтересованными сторонами;

o) странам следует руководствоваться гибкими подходами к применимым юрисдикционным основам в области борьбы с киберпреступностью, в том числе, в частности, благодаря более высокой степени зависимости от места предоставления услуг ИКТ и в меньшей степени от места нахождения данных;

p) странам следует вкладывать средства в просвещение общественности и промышленных кругов в целях повышения их осведомленности о киберпреступности, с тем чтобы снизить количество сообщений о киберпреступлениях по сравнению с другими видами преступлений;

q) государствам-членам следует налаживать публично-частное партнерство в области борьбы с киберпреступностью, в том числе посредством принятия законодательства и создания каналов диалога с этой целью, для содействия сотрудничеству между правоохранительными органами и поставщиками коммуникационных услуг, а также научными кругами в целях углубления знаний и повышения эффективности мер борьбы с киберпреступностью.

III. Резюме обсуждения

A. Правоохранительная деятельность и расследования (*продолжение*)

2. Многие выступавшие сообщили о принятии национальных мер по разработке и реализации стратегий и политики в области кибербезопасности; принятию и/или обновлению законодательства о киберпреступности; внедрению нового следственного инструментария для сбора и установления подлинности электронных доказательств, которые будут использоваться в целях доказывания в уголовном судопроизводстве, с учетом гарантий соблюдения прав человека; внедрению институциональных механизмов, призванных обеспечить более эффективное использование ресурсов в борьбе с киберпреступностью; содействию международному сотрудничеству в борьбе с киберпреступностью. Один из выступавших отметил, что различия между кибербезопасностью и киберпреступностью являются главным фактором, который следует учитывать при организации внутригосударственных мер реагирования и определении сфер полномочий в этих вопросах на институциональном уровне.

3. Многие выступавшие поддержали деятельность Группы экспертов как единственного всеохватного и оптимального глобального форума, в рамках которого государства-члены имеют возможность проводить дискуссии и обмениваться мнениями о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве с целью изучения возможных путей совершенствования национальных и международных правовых или иных мер по противодействию киберпреступности. Была также отмечена дополнительная польза Комиссии по предупреждению преступности и уголовному правосудию в этом отношении. Было указано на то, что Группа экспертов обладает уникальным мандатом на выполнение функций форума для обсуждения этих вопросов, однако это не означает, что необходимо отказываться от других инициатив, направленных на создание на международном уровне всеобъемлющей системы «глобального управления» для противодействия киберпреступности.

4. Было упомянуто организованное параллельно с совещанием Группы экспертов мероприятие «Подходы к борьбе с киберпреступностью: взгляды стран Тихоокеанского региона и за его пределами». Это параллельное мероприятие было организовано правительствами Австралии, Вануату, Доминиканской Республики, Самоа и Соединенных Штатов.

5. Было заявлено о поддержке работы УНП ООН по оказанию технической помощи и созданию потенциала для выработки согласованных мер противодействия киберпреступности.

6. Некоторые выступавшие выразили также признательность за выпуск публикации “Practical Guide for Requesting Electronic Evidence Across Borders” («Практическое руководство по запрашиванию электронных доказательств в других странах»). Руководство было совместно подготовлено и выпущено Управлением Организации Объединенных Наций по наркотикам и преступности (УНП ООН), Исполнительным директоратом Контртеррористического комитета (ИДКТК) Организации Объединенных Наций и Международной ассоциацией прокуроров (МАП) и доступ к нему открыт для государств-членов и сотрудников их органов уголовного правосудия на портале ШЕРЛОК УНП ООН. Будучи подготовлено в сотрудничестве с государствами-членами, другими международными и региональными организациями и такими поставщиками коммуникационных услуг, как Facebook, Google, Microsoft и Uber, Практическое руководство содержит информацию, которая помогает определить на национальном уровне необходимые действия по сбору, сохранению и передаче электронных доказательств с общей целью обеспечить эффективность взаимной правовой помощи на практике.

IV. Организация работы совещания

B. Заявления (*продолжение*)

7. С заявлениями выступили эксперты следующих государств: Армении, Грузии, Доминиканской Республики, Испании, Коста-Рики, Малайзии, Марокко, Мексики, Объединенных Арабских Эмиратов, Парагвая, Перу, Словакии, Таиланда, Филиппин и Эстонии.

8. С заявлением выступил также представитель межправительственной организации — Совета Европы.