Distr.: Limited
27 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 (*продолжение*)

A. Правоохранительная деятельность и расследования

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.

III. Резюме обсуждения

A. Правоохранительная деятельность и расследования (*продолжение*)

2. В ходе последующего обсуждения Группа экспертов уделила внимание примерам предполагаемых преступных деяний, совершаемых в цифровой среде и создающих значительные трудности для работников системы уголовного правосудия и следователей при возбуждении или проведении расследований и последующего уголовного преследования. К таким примерам относятся, в частности, мошенничество в режиме онлайн, использование Интернета в террористических целях, использование «темной сети» для совершения противоправных действий, а также сексуальные надругательства над детьми и их сексуальная эксплуатация путем незаконного использования информационно-коммуникационных технологий. Кроме того, Группа экспертов была проинформирована о концептуальной взаимозависимости киберпреступности и кибербезопасности, а также о тенденциях и проблемах, связанных с киберпреступностью, включая атаки с использованием программ-выкупов; тактику социальной инженерии, используемой для совершения мошеннических действий (фишинг, мошенническая рассылка от имени руководства внутри организации, вишинг, смишинг); использование платформы «Cobalt Strike» для атак в отношении банковской системы;

Интернет вещей; майнинг криптовалют и взлом шифрования; и скимминг и связанные с этим преступления.

3. На совещании Группы экспертов была подтверждена необходимость обсуждения вопроса о том, нужен ли новый глобальный всеобъемлющий правовой документ по киберпреступности или же вместо этого государствам следует сосредоточить внимание на эффективном осуществлении существующих документов, включая Конвенцию Совета Европы о киберпреступности (Будапештскую конвенцию). Кроме того, было высказано мнение, что в разработке нового глобального всеобъемлющего правового документа по киберпреступности нет необходимости с учетом того, что Будапештская конвенция обеспечивает достаточную основу для разработки надлежащих внутренних и международных мер по борьбе с киберпреступностью в рамках сотрудничества. Было вновь обращено внимание на тот факт, что число государств-участников, а именно 63 государства, свидетельствует о том, что Будапештская конвенция открыта для присоединения государств, не являющихся членами Совета Европы. Кроме того, было высказано мнение, что Конвенция используется третьими государствами — участниками Конвенции в качестве справочного источника для согласования внутренних законодательных норм как материально-правового, так и процессуального характера. Было также высказано мнение, что понятие «согласование национальных норм» включает не только случаи совпадения и общего определения, но и случаи, когда международные нормы являются «полезными» для разработки национальных правил. Было отмечено, что Будапештская конвенция дополняет другие региональные документы, такие как Конвенция Африканского союза по кибербезопасности и защите персональных данных (2014 год) и Международный кодекс поведения в области информационной безопасности, принятый Шанхайской организацией сотрудничества (ШОС).

4. С другой стороны, было отмечено, что для решения проблем, связанных с быстрым развитием интернет-технологий, которые не охвачены существующими механизмами, участниками которых являются не все государства мира, необходим новый глобальный правовой документ по киберпреступности, разработанный в рамках Организации Объединенных Наций. Было подчеркнуто, что такой документ планируется подготовить в рамках процесса под руководством Организации Объединенных Наций, в ходе которого все государства-члены могут взять на себя ответственность за оптимизацию усилий по борьбе с киберпреступностью с учетом (или на основе) существующих документов, таких как Будапештская конвенция и вышеупомянутая Конвенция Африканского союза. В этой связи была упомянута резолюция 73/187 Генеральной Ассамблеи от 18 декабря 2018 года, посвященная «проблемам, с которыми сталкиваются государства-члены в сфере противодействия использованию информационно-коммуникационных технологий в преступных целях», и изложенное в ней поручение Генеральному секретарю запросить у государств-членов информацию о трудностях, с которыми они сталкиваются в сфере противодействия использованию информационно-коммуникационных технологий в преступных целях, и представить Генеральной Ассамблее доклад, подготовленный на основе этой информации, для рассмотрения на ее семьдесят четвертой сессии. В ходе других выступлений было высказано мнение, что Будапештская конвенция не учитывает обеспокоенность всех государств — членов Организации Объединенных Наций и предусматривает сложные процессы внесения поправок в ее текст, что может иметь отрицательные последствия с учетом постоянно меняющегося характера киберпреступности.

5. Был упомянут текущий процесс согласования, касающийся принятия второго дополнительного протокола к Будапештской конвенции, направленный на установление четких правил и более эффективных процедур по следующим вопросам: положения о более эффективном и оперативном международном сотрудничестве; положения, допускающие прямое сотрудничество с поставщиками услуг в других правовых системах в отношении просьб о предоставлении информации об абонентах, просьб о сохранении данных и срочных просьб;

более четкая структура и более надежные гарантии для существующей практики трансграничного доступа к данным; и гарантии, включая требования, предъявляемые к защите данных.

6. Было также подчеркнуто, что Конвенцию об организованной преступности можно использовать в качестве полезного инструмента для решения проблем, связанных с киберпреступностью, особенно с учетом их транснационального характера. Было внесено предложение рассмотреть вопрос о согласовании дополнительного протокола к Конвенции об организованной преступности, конкретно касающегося киберпреступности.

7. Делегации и участники дискуссионной группы проинформировали Группу экспертов об успешных национальных усилиях по разработке и осуществлению правовых и процессуальных мер по борьбе с киберпреступностью. Для некоторых из них Будапештская конвенция и сопутствующие ей проекты по созданию потенциала являются важнейшими составными элементами в этой области. Был обстоятельно рассмотрен вопрос о законодательных реформах на национальном уровне, в том числе вопрос о масштабах таких реформ. Внимание было обращено на необходимость проведения всеобъемлющих и основанных на широком участии процессов для обеспечения того, чтобы мнения различных заинтересованных сторон были услышаны. Была отмечена необходимость обеспечения правовой определенности и ясности на основе принципа «nullum crimen nulla poena sine lege», а также необходимость использования в новом законодательстве «технологически нейтральных» формулировок, с тем чтобы оно соответствовало быстрому развитию информационно-коммуникационных технологий.

8. Обсуждались также проблемы, возникающие в связи с коллизиями, касающимися правоприменительной юрисдикции, особенно в тех случаях, когда, например, поставщик услуг может иметь штаб-квартиру в одной юрисдикции, а контролер данных находится в другой стране или данные хранятся в другой или нескольких юрисдикциях. Было отмечено, что появление облачных вычислений создает дополнительные практические и правовые проблемы для уголовных расследований. Было также отмечено, что гибкие подходы к применимым юрисдикционным основам могут быть полезными 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.

9. Группа экспертов также уделила особое внимание необходимости наличия соответствующих процессуальных полномочий для получения электронных доказательств, касающихся не только киберпреступности, но и других видов обычной преступности. Такие электронные доказательства могут включать, среди прочего, информацию об абонентах, данные о содержании контента или данные о трафике. Было отмечено, что в связи с развитием новых технологий, таких как анонимизация программного обеспечения, высококачественное шифрование и использование виртуальных валют в тех случаях, когда проводится расследование правонарушений, связанных с электронными доказательствами, следователям, возможно, потребуется принятие новых стратегий и рассмотрение вопроса о том, как специальные методы расследования и дистанционная цифровая криминалистика для сбора таких электронных доказательств могут использоваться при одновременном обеспечении приемлемости и использовании таких доказательств в суде.

10. В ходе обсуждения особое внимание было также уделено вопросу о том, каким образом обеспечить баланс между необходимостью принятия правоохранительными органами эффективных мер реагирования на киберпреступность и защитой основных прав человека, особенно прав на неприкосновенность частной жизни. Общее мнение заключалось в том, что, например, правила сохранения данных могут отражать прагматический подход к обеспечению возможности для поставщиков коммуникационных услуг играть более весомую роль в борьбе с киберпреступностью посредством более широкого сотрудничества с

правоохранительными органами при том условии, что такие законодательные акты осуществляются с соблюдением должных процессуальных гарантий и обеспечением должной защиты личных данных. Был упомянут доклад Комиссара Организации Объединенных Наций по правам человека по вопросу о праве на неприкосновенность частной жизни в цифровую эпоху, который был представлен Совету по правам человека в соответствии с резолюцией 68/167 Генеральной Ассамблеи (A/HRC/27/37).

11. Группа экспертов вновь заявила о важности международного сотрудничества в области трансграничного расследования киберпреступлений и уголовного преследования за их совершение. Было признано, что число просьб об оказании взаимной правовой помощи в получении или сохранении электронных доказательств быстро растет и что нынешние формы сотрудничества, занимающие, в частности, много времени, недостаточны для решения проблем, связанных с быстрым и успешным доступом к данным, которые, ввиду их неустойчивого характера, могут передаваться или удаляться «одним щелчком компьютерной мыши».

12. В качестве примеров были упомянуты различные виды практики для укрепления международного сотрудничества, связанного с электронными доказательствами, особенно на оперативном уровне, в том числе прямая передача просьб об оказании взаимной правовой помощи между компетентными органами сотрудничающих государств; более частое использование специально разработанных инструментов международного сотрудничества для обеспечения целостности электронных доказательств, таких как оперативное сохранение компьютерных данных; совместные расследования (СР); использование электронных средств для передачи просьб об оказании взаимной правовой помощи с уделением особого внимания потенциальной полезности инициативы Интерпола в отношении безопасной электронной передачи сообщений об оказании взаимной правовой помощи (ЭПСВПП); обмен информацией между координаторами сети, работающими круглосуточно и без выходных; и более частое использование возможностей сотрудничества между органами полиции, в том числе при содействии Интерпола, в целях сбора оперативной информации. Был также упомянут Европейский центр по борьбе с киберпреступностью (ЕЦБК), который был создан Европолом в 2013 году в целях укрепления мер реагирования правоохранительных органов ЕС на киберпреступность.

13. Группа экспертов также рассмотрела вопрос о трансграничном доступе к данным. В целом было отмечено, что применяемые государствами виды практики и процедуры, а также условия и гарантии этих процедур значительно различаются в разных государствах-участниках. Кроме того, особое внимание было уделено процессуальным правам подозреваемых, соображениям неприкосновенности частной жизни и защите личных данных в другой юрисдикции, а также уважению национального суверенитета.

14. Группа экспертов подчеркнула важность устойчивого наращивания потенциала для повышения эффективности и квалификации всех компетентных органов на оперативном уровне в целях решения проблем, связанных с киберпреступностью. В этой связи выступавшие отметили полезность обмена информацией об успешных видах практики и опыте между специалистами-практиками не только в рамках государств, но и с другими государствами. Некоторые выступавшие упомянули об активизации подготовки кадров и процесса укрепления потенциала в связи с созданием специализированных структур по борьбе с киберпреступностью или подразделений при прокуратуре и правоохранительных органах. В этой связи было подчеркнуто, что, поскольку электронные доказательства становятся все более распространенными и при проведении расследования обычных преступлений, крайне важно создать специализированные структуры для расследования этих преступлений специалистами, обладающими конкретным опытом, знаниями и оперативными навыками.

15. Группа экспертов обсудила далее вопрос о сотрудничестве национальных органов с частным сектором, особенно с поставщиками коммуникационных услуг (ПКУ), в целях повышения эффективности сохранения данных и расширения доступа к ним. Было подчеркнуто растущее значение такого сотрудничества на национальном уровне, особенно в чрезвычайных обстоятельствах, связанных с тяжкими преступлениями, а также признано, что для обеспечения аналогичного уровня сотрудничества в рассмотрении транснациональных дел необходимо приложить дополнительные усилия. В этой связи был упомянут «риск двойного соблюдения» для ПКУ, а именно порядок балансирования их реагирования с учетом правовых требований соответствующих государств.

IV. Организация работы совещания

B. Заявления (*продолжение*)

16. С заявлениями выступили эксперты следующих государств: Алжира, Буркина-Фасо, Индии, Италии, Канады, Китая, Колумбии, Кувейта, Мавритании, Нидерландов, Норвегии, Франции, Чили, Шри-Ланки и Японии.

17. С заявлением выступил также представитель межправительственной организации — Европейского союза.