27 July 2020
Russian
Original: English

Группа экспертов для проведения всестороннего исследования проблемы киберпреступности
Вена, 27–29 июля 2020 года

Проект доклада

Добавление

II. Перечень предварительных рекомендаций и выводов (*продолжение*)

B. Предупреждение киберпреступности

1. В соответствии с планом работы Группы экспертов в настоящем пункте обобщены предложения, 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 их одобрения Группой экспертов, а порядок их перечисления не отражает степень их важности.

1) Следует признать, что предупреждение киберпреступности является не только обязанностью правительств, но и требует участия всех заинтересованных сторон, включая правоохранительные органы, частный сектор, особенно поставщиков интернет-услуг, неправительственные организации, учебные заведения и научные круги, а также широкую общественность.

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

3) Было выражено мнение о необходимости разработки долгосрочных государственных стратегий предупреждения киберпреступности, включающих разработку информационных кампаний на тему безопасного пользования интернетом.

4) 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. Государствам следует делиться опытом применения стратегий кибербезопасности для предупреждения киберпреступности. Кроме того, государствам следует уделять особое внимание

проведению профилактической работы с молодежью, в том числе лицами, впервые совершившими правонарушения, с целью профилактики рецидивизма.

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

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

7) Пересечение сфер деятельности и взаимодействие государственных и частных структур, располагающих большими массивами данных или мощностями для их обработки, может представлять зону повышенного риска, особенно в сфере здравоохранения ввиду продолжающейся пандемии, а также в других сферах. Государствам следует уделить особое внимание правовому регулированию доступа к таким данным и их защите от кибератак.

8) В профилактических целях поставщикам интернет-услуг следует взять на себя большую ответственность за применение мер предосторожности (которые должны действовать «по умолчанию») и предупреждение киберпреступности, а также разработать международные стандарты в отношении содержания информации, подлежащей занесению в журналы серверов, и сроков ее хранения поставщиками интернет-услуг. Помимо этого, следует четко определить обязанности ПИУ по выявлению, предотвращению и пресечению киберпреступлений.

9) Для предупреждения и противодействия киберпреступности необходимо развивать государственно-частные партнерства, в том числе наладить сотрудничество с заинтересованными участниками из сектора кибербезопасности и крупными технологическими компаниями в области обмена информацией.

10) 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 их использованию в преступных целях.

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

12) 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.

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

14) 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.

15) Государствам-членам было рекомендовано продолжать активную профилактическую работу на национальном и международном уровнях и уделять особое внимание превентивным мерам, таким 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; повышение вероятности привлечения к ответственности

и наказания правонарушителей и предупреждение преступности путем выявления и пресечения незаконной деятельности в интернете. Органам полиции и прокуратуры было рекомендовано вкладывать усилия в выявление киберугроз, оповещение о них и принятие необходимых мер реагирования. В этой связи была также отмечена необходимость развития государственно-частного партнерства. Подобные профилактические мероприятия не требуют принятия дополнительных законов и нормативных актов.

16) Из-за сохранения «цифрового разрыва» некоторые развивающиеся страны не имеют возможности предупреждать, выявлять и пресекать киберпреступления и поэтому более уязвимы перед угрозой киберпреступности.

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