УДК 343

Международное сотрудничество в борьбе с киберпреступностью: отдельные проблемы и пути их решений

Саргсян Ш.М.
студент международно-правового факультета
МГИМО МИД России
(Одинцовский филиал),
143007, Московская обл., г. Одинцово, ул. Ново-Спортивная, д. 3,
info@odin.mgimo.ru

Аннотация: В данной работе рассмотрен институт международного сотрудничества, который стал одним из наиболее актуальных и дискуссионных тем ввиду возникновения и развития киберпреступлений в последнее время; указаны примеры преступлений в IT сфере, в том числе преступления, затрагивающие интересы, целостность и безопасность отдельных государств, подтверждающих необходимость развития международного сотрудничества в данной сфере. Перечислены источники, основные формы международного сотрудничества, а также возможные препятствия, которые могут возникнуть у государств при осуществлении международного сотрудничества. В частности, указаны неточности при осуществления экстрадиции, пробелы в российском законодательстве касающиеся определения правового статуса лица, подлежащего экстрадиции. Рассмотрены основные цели преступников и коллизии, которыми они пользуются чтобы избежать наказания. Автором предложены возможные практические действия для развития международного сотрудничества, основанные на примере уже существующего сотрудничества, с целью предотвратить ситуацию, при котором будет невозможно обеспечить полноценную защиту граждан и государств от киберпреступлений; указано мнение автора относительно предложенных им в статье возможных путей решения возникшей проблемы отставания норм международного сотрудничества от тех отношений, которые они регулируют.

Ключевые слова: киберпреступление, IT-сфера, международное сотрудничество, экстрадиция.

International cooperation against cybercrime: problems and solutions

Sargsyan Sh.M.
Bachelor of international law,
MGIMO-University MFA Russia
(Odintsovo branch),
3 Novo-Sportivnaya, Odintsovo, Moscow region,
143007, Russia,
info@odin.mgimo.ru

Annotation: This article examines the institute of international cooperation, which has become one of the most relevant and controversial topics due to the emergence and development of cybercrimes in recent years; examples of crimes in the IT sphere, including crimes affecting the interests, integrity and security of some states, confirming the need for the development of international cooperation in this area. There are listed the sources, the main forms of international cooperation, as well as possible obstacles that may arise for States in the implementation of international cooperation are listed. In particular, there are inaccuracies in the implementation of extradition, gaps in Russian legislation concerning the determination of the legal status of a person subject to extradition. The main aims of criminals and the conflict that they use to avoid punishment which are considered. The author suggests possible practical actions for the development of international cooperation, based on the example of existing cooperation, in order to prevent a situation in which it will be impossible to ensure full protection of citizens and states from cybercrime; the author's opinion is indicated regarding the possible ways proposed by him in the article to solve the problem of lagging behind the norms of international cooperation from the relations that they regulate.

Keywords: cybercrime, IT-sphere, international cooperation, extradition.

В настоящее время невозможно представить жизнь современного человека без компьютерных технологий. Информационно-технологическая сфера нашей жизни за последнее десятилетие сделало огромный рывок. Но последствия данного рывка не только положительные, но и отрицательные.

Специалисты отмечают, что поступательное и активное развитие интернета открыло широкие возможности для преступников, что послужило причиной значительного роста преступлений в данной сфере. [6, с. 54-61] Это же подтверждают статистические данные МВД РФ, согласно которым за период с января по ноябрь 2020 года наблюдается значительный рост преступлений с использованием IT-технологий. В частности, на 81,6% увеличилось количество краж с использованием телекоммуникационных систем. [3]

Более того, у преступников появилась возможность совершать противоправные деяния, находясь на большом расстоянии от места преступления, что, несомненно, усложняет процесс их поимки. Зачастую киберпреступники действуют на территории чужих государств, рассчитывая на то обстоятельство, что правоохранительные органы государства, на чьей территории совершено преступление, не имеют властных полномочий на территории того государства, где они находятся, и, следовательно, вероятность того, что они останутся безнаказанными, ощутимо увеличивается.

Также, стоит обратить внимание, на то обстоятельство, что немалая часть киберпреступлений ставят под угрозу не только конфиденциальность личной жизни и безопасность обычных граждан, но и суверенитет и безопасность самого государства, на которое направлен преступный умысел. Целями таких преступных деяний является не

только пропаганда идей определенной группы, но также незаконный сбор данных, незаконный доступ в информационную среду органов власти того или иного государства, что впоследствии может подвергнуть опасности жизнь и безопасность большого количества людей и воспрепятствовать полноценному функционированию органов государственной власти. Так, например, в январе 2009 года вирус Conficker заразил военную технику Франции, в следствие чего истребители не функционировали должным образом и не смогли взлететь. [2] В декабре 2013 года хакеры заразили вредоносным программным обеспечением компьютеры участников G20, проходившего в Санкт-Петербурге и получили доступ к секретным данным. [8]

Все это подтверждает актуальность проблемы усиления борьбы с киберпреступлениями и необходимость международного сотрудничества в данной сфере с целью обеспечения безопасности и правопорядка.

Материалы и методы: Методологическую основу исследования составили как общенаучные методы, к которым относятся дедукция, индукция, анализ и синтез, так и специально юридические методы: формально-юридический и догматический методы.

Основная часть: Международному сотрудничеству в сфере уголовного судопроизводства выделена отдельная глава в Уголовно-процессуальном кодексе Российской Федерации. Также, источниками международного сотрудничества, помимо УПК РФ, являются международные договоры России с другими государствами и принцип взаимности.

В настоящий момент можно выделить три основные формы международного сотрудничества в сфере уголовного судопроизводства:

1. Выдача лиц для уголовного преследования или исполнения приговора (экстрадиция)
2. Исполнение запросов (поручений) о производстве следственных и иных процессуальных действий (это может быть, например, производство допросов, обысков и других действий, направленных на собирание доказательств; осуществление задержания; вручение процессуальных документов, вызовов и извещений; и др.).
3. Передача осужденных к лишению свободы лиц для отбывания наказания. [4, с. 1256]

Необходимо отметить, что при осуществлении каждой из вышеназванных форм международного сотрудничества государства сталкиваются с большим количеством факторов, осложняющих, а в ряде случаев, мешающих полноценному сотрудничеству. Я остановлюсь на некоторых из наиболее распространенных коллизиях, с которыми сталкиваются государства.

В частности, в сфере экстрадиции до настоящего времени не определен процессуальный статус лиц, подлежащих выдаче. По нашему мнению, сам по себе термин «выдача преступника» является некорректным, так как он в определенной степени не соотносится с презумпцией невиновности. Как известно, преступником лицо может быть названо лишь после вступления в законную силу обвинительного приговора суда. Для иностранного государства, обращающегося в Российскую Федерацию о выдаче преступника, это лицо находится в статусе обвиняемого или подозреваемого; при этом, экстрадированный может оказаться невиновным в совершении того преступления, в котором его обвиняют.

В уголовно-процессуальном кодексе РФ такой субъект, как «выдаваемое лицо» не упомянут, а значит, не определены его процессуальные права и обязанности. Однако, фактически, данные лица участвуют в уголовном процессе. Из этого правового пробела вытекает много проблем, например, реализация такими лицами права на защиту. [1, с.249-323.]

Не следует также забывать, что киберпреступники могут совершать противоправные деяния, находясь на территории таких государств, в которых за это деяние не предусмотрено уголовного наказания или предусмотрено более мягкое, чем в стране совершения, наказание. К подобным странам относятся Доминиканская Республика, Гаити, Гондурас, где правовая база в сфере IT-технологий и киберпреступлений не развита в должной мере, что позволяет преступникам избегать наказаний за совершенные преступления.

Несомненно, вышеназванные аспекты не являются единственными. Существует множество препятствий для осуществления международного сотрудничества в сфере уголовного судопроизводства, и основной причиной наличия коллизий является тот факт, что развитие информационных технологий значительно опережает развитие международной и национальной нормативно-правовой базы. Я считаю, что в УПК РФ необходимо внести соответствующие дополнения, направленные на усовершенствование процесса международного сотрудничества, иначе есть риск возникновения ситуации, когда быстроразвивающаяся IT сфера выйдет из-под контроля, что приведет к значительному росту преступлений в информационной сфере.

В связи с вышеизложенным, по моему мнению, следует предпринять ряд действий для предупреждения вышеописанной ситуации. А именно:

1. Сформулировать и создать международный правовой акт, к примеру, Декларацию о всеобщих правилах кибербезопасности, которая будет подписана всеми государствами. На основе Декларации можно будет разработать международный договор о правилах кибербезопасности, подписантами которого станут все государства с развитыми IT-технологиями.

2. В рамках правоохранительной системы каждого государства целесообразно создать отдельный специализированный орган, который будет заниматься исключительно киберпреступлениями в сотрудничестве с организациями и учреждениями, которые занимаются обеспечением кибербезопасности. Примером такой деятельности может служить союз «Лаборатории Касперского» с Интерполом. Кроме того, постоянно проводятся тренинги для офицеров Интерпола с целью передачи опыта в вопросах анализа вредоносных программ, обнаружения цифровых следов и улик, а также исследования финансовых угроз. [5, с. 43-48] Полагаю, что ориентируясь на данный опыт, можно создать международный аналог, где организации, занимающиеся кибербезопасностью, будут помогать международным органам борьбы с киберпреступностью.

3. В структуре Интерпола и Европола создать специализированный отдел, оперативно реагирующий на запросы. Данное предложение связано с тем, что преступления в цифровой среде необходимо расследовать как можно быстрее, так как цифровой след меняется и/или исчезает достаточно быстро.

Заключение и выводы: Подводя итог следует сказать, что проблема киберпреступлений стоит наиболее остро в наши дни, из чего следует, что международное сотрудничество как никогда необходимо. Автор сознает, что вышеизложенные предложения по усовершенствованию и развитию международного сотрудничества в сфере преступлений в IT сфере являются дискуссионными, но считает, что они могут в определенной мере способствовать если не сокращению количества преступлений в киберпространстве, то, по крайней мере, повышению эффективности расследования данных преступных деяний, и в целом оказать влияние на повышение кибербезопасности.

Список используемой литературы

1. Жужгина А. А. Международное сотрудничество в сфере уголовного процесса: проблемы экстрадиции киберпреступников // Молодой ученый Международный научный журнал. – 2020. – № 21(311). – С. 249-323.
2. Истребители ВМС Франции не смогли взлететь из-за компьютерного вируса // URL https://xakep.ru/2009/02/09/47082/ (дата обращения 17.01.2021).

3. Краткая характеристика состояния преступности в Российской Федерации за январь - ноябрь 2020 года // URL: https://мвд.рф/reports/item/22501861/ (дата обращения 27.12.2020).
4. Курс уголовного процесса / Под ред. д.ю.н., проф. Л.В. Головко.– 2-е изд., испр. – М.: Статут, 2017.
5. Несмеянов А.А. Основные проблемы борьбы с преступлениями в сфере высоких технологий // Вестник Восточно-Сибирского института МВД России. – 2014. – № 4(71). – С.43-48.
6. Решняк, М.Г. Современные проблемы действия уголовного законодательства Российской Федерации и отдельных зарубежных стран, связанные с цифровизацией преступной деятельности // Безопасность бизнеса. – 2020. – № 6. – С.54-61.
7. Уголовно-процессуальный кодекс Российской Федерации // Собрание законодательства РФ. – 2001. – N 52(ч. I). – Ст. 4921; Российская газета. – 2020. – № 280.
8. 20 самых громких киберпреступлений 21 века // URL https://zen.yandex.ru/media/id/5c9b21d83bbd5d00b356a271/20-samyh-gromkih-kiberprestuplenii-21-veka-5c9b232c5e29d000b387248b (дата обращения 17.01.2021).