УДК 343.98

ВОЗМОЖНОСТИ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА ПРИ ПРОВЕДЕНИИ НАУЧНЫХ ИССЛЕДОВАНИЙ ТРАНСНАЦИОНАЛЬНОЙ КИБЕРПРЕСТУПНОСТИ

Карагодин Валерий Николаевич

Екатеринбургский филиал Московской академии Следственного комитета Российской Федерации имени А.Я. Сухарева, г. Екатеринбург
e-mail: uc.ural@mail.ru

POSSIBILITIES OF INTERNATIONAL COOPERATION IN CONDUCTING SCIENTIFIC RESEARCH ON TRANSNATIONAL CYBERCRIME

Karagodin Valery N.

Sukharev Moscow academy of the Investigative Committee of the Russian Federation, Yekaterinburg

Аннотация: в статье отмечается важность международного сотрудничества в противодействии транснациональной киберпреступности, которое рассматривается как глобальная международная проблема. Соответственно этому высказывается мысль о том, что научно-методическое обеспечение деятельности по раскрытию, пресечению, расследованию и предупреждению транснациональных киберпреступлений представляет собой глобальную научную проблему, требующую объединения усилий ученых разных стран. Отмечается, что наиболее перспективным представляется взаимодействие ученых стран, кооперирующихся в рамках различных политических, социально экономических организаций.

Такими государствами, в частности, являются страны-участницы БРИКС. Усиление социально-экономических связей между этими странами, несомненно, вызовет не только положительную активность в области торговли, производства, образования, культуры и других сферах жизнедеятельности. Не вызывает сомнений, что представители криминогенного контингента также попытаются использовать укрепляющееся сотрудничество для активизации, развертывания преступной деятельности на территориях взаимодействующих государств, участвующих в БРИКС. В этой

Abstract: the article notes the importance of international cooperation in countering transnational cybercrime, which is considered as a global international problem. Accordingly, the idea is expressed that scientific and methodological support for activities to detect, suppress, investigate and prevent transnational cybercrime is a global scientific problem that requires the combined efforts of scientists from different countries. It is noted that the most promising is the interaction of scientists from countries cooperating within the framework of various political, socio-economic organizations.

Such states, in particular, are the BRICS member countries. Strengthening socio-economic ties between these countries will undoubtedly cause not only positive activity in the field of trade, production, education, culture and other spheres of life. There is no doubt that representatives of the criminal contingent will also try to use the strengthening cooperation to intensify and expand criminal activity in the territories of the interacting states participating in BRICS. In this regard, the problem of consolidating the efforts of the BRICS member states in improving the means, methods and techniques for solving and investigating transnational cybercrimes arises. The article notes that in these countries there is a different level of development, prevalence of digital tools, technologies, software products that can be used in committing transnational cybercrimes. The author suggests that the

связи возникает проблема консолидации усилений государств-участников БРИКС в совершенствовании средств, методов, приемов раскрытия и расследования транснациональных киберпреступлений.

В статье отмечается, что в названных странах наблюдается разный уровень развития, распространенности цифровых средств, технологий, продуктов программного обеспечения, которые могут быть использованы при совершении транснациональных киберпреступлений. Автором высказываются предположения, что субъекты киберпреступлений, представляющие разные страны, отличающиеся по уровню образования, опыта и направленности криминальной деятельности, отдают предпочтения повторяющимся способам посягательств. Одним из основных элементов таких способов является использование, конструирование определенных программных средств для достижения конечной цели преступления, сокрытия характера выполняемых действий. Содержание этого элемента в действиях представителей разных стран существенно отличаются, что требуют применения специфических средств, методов и приемов диагностики, идентификации субъектов преступления.

Представители разных этнических групп, участвующие в совершении единого преступления, формируют и используют оригинальные средства коммуникации. Распознавание смысла передаваемой такими субъектами информации также требует применения нестандартных приемов, методик и средств.

Обобщение названных и иных признаков преступлений рассматриваемого вида, конструирование методов раскрытия и расследования таких посягательств, будут более продуктивны в рамках международного научного сотрудничества.

Ключевые слова: транснациональная киберпреступность, научное сотрудничество, способы преступления, раскрытие и расследование киберпреступлений, искусственный интеллект.

subjects of cybercrimes, representing different countries, differing in the level of education, experience and focus of criminal activity, prefer repetitive methods of encroachment. One of the main elements of such methods is the use, design of certain software to achieve the ultimate goal of the crime, conceal the nature of the actions performed. The content of this element in the actions of representatives of different countries differs significantly, which requires the use of specific means, methods and techniques of diagnostics, identification of the subjects of the crime.

Representatives of different ethnic groups participating in the commission of a single crime form and use original means of communication. Recognition of the meaning of the information transmitted by such subjects also requires the use of non-standard techniques, methods and means.

Generalization of the named and other signs of crimes of the type under consideration, construction of methods for solving and investigating such attacks will be more productive within the framework of international scientific cooperation.

Keywords: transnational cybercrime, scientific cooperation, methods of crime, detection and investigation of cybercrimes, artificial intelligence.

Для цитирования: Карагодин В.Н. Возможности международного сотрудничества при проведении научных исследований транснациональной киберпреступности // Проблемы правовой и технической защиты информации. 2024. № 12 С.25-30.

For citation: Karagodin V.N. Possibilities of international cooperation in conducting scientific research on transnational cybercrime // Legal and Technical Problems of Information Security. 2024. No. 12. P.25-30.

Как известно, стремительное развитие цифровых технологий способствовало не только прогрессу в различных отраслях социально полезной деятельности человека, но и появлению нового вида преступности, получившего название киберпреступности. Практически одновременно с появлением этого вида общественно опасного явления оно приобрело транснациональный характер. Таковыми считаются посягательства, нарушающие нормы уголовного права нескольких стран, имеющие трансграничный или транстерриториальный характер, т.е. связанные с выполнением преступных действий на территории нескольких государств [1, с. 18-22].

Использование цифровых технологий позволяет полностью или частично реализовывать способы киберпреступлений без перемещения субъектов через территориальные границы государств, скрывая истинный характер выполняемых операций и участие в них конкретных лиц.

Негативная динамика и размах транснациональной киберпреступности, высокий уровень ее латентности позволяет относить проблемы борьбы с ней к глобальным, международным. Вряд ли можно возразить против слов Нобелевского лауреата, академика П.Л. Капицы, сказанных почти пятьдесят лет назад: «Исследования, направленные на решение этих проблем, нужно решать в международном масштабе» [2, с.464]. Глобальными, этот великий советский ученый, называл проблемы, имеющие значение для всего человечества или для значительной его части. Несомненно, имеются все основания отнесения к таковым и проблем борьбы с транснациональной преступностью. В данном случае во внимание следует принимать не только широту размаха этой противоправной деятельности, но и ее общественную опасность. Этот вид преступности фактически дестабилизирует как отдельные государства, так и международные организации и, в конченом итоге, все мировое сообщество.

Следует отметить, что субъекты транснациональных киберпреступлений гораздо более мобильны и быстрее объединяют усилия в своей криминальной деятельности, чем их оппоненты: внутригосударственные и международные правоохранительные учреждения.

Межгосударственному взаимодействию в этом направлении препятствует сложная международная обстановка, характеризующаяся серьезными политическими и идеологическими противоречиями. Поэтому целесообразно налаживание сотрудничества, в том числе и научного между странами, уже объединившимися в рамках интергосударственных организаций, таких, в частности, как БРИКС. Не исключается конечно же и участие в международном сотрудничестве других стран, не входящих в названную организацию. Однако, усиление социально экономических связей объединившихся стран нередко сопровождается и транснациональными преступными проявлениями на территориях этих стран. Например, тесное социально экономическое сотрудничество между Россией и Китаем, не осталось без внимания представителей транснациональной преступности. По некоторым данным, в определенный период времени в сети Интернет удалось обнаружить около 150 русскоязычных сайтов, предлагающих доставку в Россию наркотических средств из Китая [3, с.37].

Международное научное сотрудничество может налаживаться в различных направлениях, предполагающих

теоретические изыскания разной степени общности.

Наиболее перспективными выглядят совместные исследования в области раскрытия и расследования отдельных видов транснациональных киберпреступлений.

В российской криминалистике предпринималась попытка классификации компьютерных преступлений (киберпреступлений) по способу их совершения. Все такого рода преступления обоснованно классифицировались на связанные и не связанные с удаленным доступом к компьютерной информации [4, с.673]. Представляется, что возможна более широкая трактовка киберпреступлений как любых посягательств, совершаемых с использованием компьютерных технологий. Кроме преступлений уже названных групп возможно выделение таких видов как связанных с манипулированием, осуществляемым с помощью средств компьютерной техники. В отечественной литературе отмечалось, что манипулятивное воздействие используется в компьютерных преступлениях, совершаемых в сфере экономической деятельности, религиозного сектанства и некоторых посягательств против личности [5, с.42]. Как известно, манипуляции представляют собой скрытое воздействие с целью добиться от партнера по общению поступков, которые он бы не совершил, если бы знал истинные цели манипулятора и реальные условия ситуации. Манипуляции широко используются при совершении мошенничеств, экстремистских посягательств, действий сексуального характера в отношении несовершеннолетних и психически неадекватных лиц, понуждение к самоубийству и т.п. Ряд таких преступлений такого рода носят транснациональный характер.

Оказание подобного воздействия требует выбора и реализации средств коммуникации, которые способны стимулировать желаемое поведение жертвы. Это представляет собой достаточно сложную задачу, особенно при совершении преступлений в отношении иностранцев. Идентификационные признаки субъектов таких посягательств транснационального характера, кроме навыка владения речью, координации и артикуляции [6, с.14] дополняются специфическими признаками компьютерной письменной и устной речи. Представляется, что эти дополнительные признаки отличаются у представителей разных этнических групп, лиц, принадлежащих к разным социальным объединениям и т.п.

Исследования подобных признаков возможны в нескольких направлениях. Прежде всего, для разработки методов и средств своевременного выявления подобных видов информации, передаваемых в компьютерных сетях. В настоящее время в практике правоохранительных органов многих стран используются автоматизированные системы выявления признаков экстремизма в пересылаемых, публикуемых в электронных средствах сообщениях, текстах, изображениях, видеоклипах, роликах и т.п.

В публикациях, подготовленных за рубежом и предназначенных для лиц той же национальности, что и авторы текстов, изображений могут отражаться признаки, которые не расшифровываются автоматизированными системами страны, на территории которой распространяются подобные материалы.

Наконец, компьютерные технологии могут использоваться как средства связи и (или) массовой информации, для передачи сведений о возможности приобретения определенной, запрещенной продукции, для обмена данными необходимыми для совершения преступления или об осуществлении преступного плана. Субъекты, названных видов преступлений принимают меры к шифровке смысла передаваемых сообщений в виде специальных изображений, сочетания определенных лексических средств и т.п. Следует заметить, что в разных странах используются разные обозначения. Представляется, что деятельности по подбору подобных обозначений присущи

общие закономерности независимо от национальности субъекта преступления. Например, субъекты сексуальных преступлений в разных странах используют изображения небольших по размеру животных розового и (или) голубого цвета, для обозначения сайтов, через которые можно заказать несовершеннолетних для оказания сексуальных услуг.

Несомненно, отдельную группу составляют преступления, связанные с незаконным доступом к компьютерной информации юридических лиц с целью завладения материальными средствами или причинения морального и (или) материального вреда [7, с.47-48; 8]. В этих случаях используются разные программные средства, которые заимствуются целиком, формируются из нескольких известных, конструируются из опубликованных и самостоятельно разработанных субъектами преступления. Деятельность по созданию такого программного продукта может также носить транснациональный характер. В таких случаях субъекты из разных стран компонуют программные средства на этапе подготовки к совершению преступления транснационального характера. В подобных продуктах кроме индивидуальных признаков субъектов, отражаются и типичные свойства личности представителей разных стран, лиц, получивших определенное образование, имеющих разный опыт совершения подобных посягательств и т.п. Конечно же, подобные исследования требуют сотрудничества ученых разных стран.

Важное значение имеет обобщение методов, приемов и средств раскрытия и расследования преступлений данного вида, применявшихся представителями компетентных органов разных стран. В результате совместных научных изысканий, желательно по единой методике, могут быть выявлены закономерности раскрытия и расследования такого рода посягательств, совершаемых субъектами, характеризующимися сходными свойствами личности.

Особый интерес представляет исследование возможностей искусственного интеллекта в досудебном производстве по фактам совершения подобных деяний. К сожалению, в отечественной практике результативность подобных изысканий невелика. В некоторых из них глубокомысленные рассуждения о преимуществах использования искусственного интеллекта, сводятся к описанию возможностей автоматизированного производства почерковедческой экспертизы подписей [9, с. 33]. В других все возможности ограничиваются производством процессуальных действий с использованием средств электронной техники [10, с.31-39].

В аспекте рассматриваемой темы интерес представляют возможности использования искусственного интеллекта для обобщения и систематизации, собранной при расследовании преступлений рассматриваемого вида, информации в целях формирования фактической базы для выдвижения версий об обстоятельствах и субъектах транснационального преступления.

В оптимальном варианте предпочтительнее выглядит использование компьютерных технологий для построения версий, оценки степени их подтверждения или опровержения. В последнем случае речь идет фактически об оценке ситуации расследования, степени доказанности обстоятельств расследуемого деяния и субъектов их совершения.

Перспективным выглядит и использование средств искусственного интеллекта для планирования расследования на определенном этапе его осуществления, а также производства отдельных следственных действий.

Наверное, возможны и другие направления возможного сотрудничества разных стран, но выделенные представляются наиболее реальными и актуальными.

В ходе осуществления прикладных исследований могут быть выявлены и решены и фундаментальные проблемы наук криминалистики, уголовного процесса и других.

Библиографический список

1. *Астахова Е.А. Криминалистическая классификация транснациональных преступлений и ее использование в расследовании. Автореф. дис. ... канд. юрид. наук; Саратов, 2023. - 34 с.*
2. *Капица П.Л. Эксперимент. Теория. Практика : Статьи, выступления / Капица П.Л., Акад. наук СССР. — 3-е изд., доп. — М. : Наука. Гл. ред. физ.-мат. лит., 1981. — 496 с. : ил.*
3. *Шурухнов Н.Г. Информационные технологии : современное состояние и отдельные данные их использования в совершении преступлений // Электронные носители информации в криминалистике : монография / под ред. док. юрид. наук О.С. Кучина. М., 2017. – С.33-44*
4. *Россинская Е.Р. Избранное. - Москва : Норма, 2019. – 679 с.*
5. *Воробьев В.В. Манипулирование сознанием как часть информационной войны и угроза национальной безопасности Российской Федерации // Российская правовая система в условиях четвертой промышленной революции. XVI Международная научно-практическая конференция (Кутафинские чтения) : материалы конференции : в 3 ч. – Часть 3. – Москва. 2019. – с. 41-45.*
6. *Баранов Ю.Н. Теоретические основы применения лингвистических знаний в криминалистике при производстве фоноскопических и автороведческих экспертиз. Автореф. дис. ... канд. юрид. наук; Челябинск, 2004. – 19 с.*
7. *Благов Е.В., Бражник С.Д. Уголовная ответственность за неправомерное воздействие на критическую информационную структуру РФ // Российская правовая система в условиях четвертой промышленной революции. XVI Международная научно-практическая конференция (Кутафинские чтения) : материалы конференции : в 3 ч. – Часть 3. – Москва. 2019. – с. 45-49.*
8. *Костомаров К.В. Первоначальный этап расследования преступлений, связанных с незаконным доступом к компьютерной информации банков. Автореф. дис. ... канд. юрид. наук; Челябинск, 2012. – 31 с.*
9. *Бахтеев Д.В. Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений. Автореф. дис. ... докт. юрид. наук; Екатеринбург, 2022. – 41 с.*
10. *Соколов Ю.Н. Информационные технологии и оборот цифровых данных в криминалистике : вопросы теории и практики. Автореф. дис. ... докт. юрид. наук; Екатеринбург, 2023. – 44 с.*