УДК 004.056

О НЕКОТОРЫХ АСПЕКТАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ ТРАНСНАЦИОНАЛЬНОЙ КИБЕРПРЕСТУПНОСТИ В СОВРЕМЕННОМ МИРЕ

Мазуров Валерий Анатольевич

Алтайский государственный университет, г. Барнаул
e-mail: mazurov50@list.ru

ON SOME ASPECTS OF ENSURING INFORMATION SECURITY AND COUNTERING TRANSNATIONAL CYBERCRIME IN THE MODERN WORLD

Mazurov Valery A.

Altai State University, Barnaul

Аннотация: Рассматриваются предложения по совершенствованию системы мер, направленных на обеспечение информационной безопасности в странах БРИКС, Российской Федерации, а также на региональном уровне. Анализируются меры, призванные противодействовать транснациональным видам киберпреступности и использованию в преступных целях киберпространство стран БРИКС, отмечаются возникающие угрозы национальной безопасности. Отдельно рассматривается роль научных исследований в реализации указанных мер, обращается внимание на важность развития сотрудничества стран БРИКС.

Ключевые слова: информационная безопасность, киберпреступность, киберпространство, противодействие преступности, сотрудничество БРИКС.

Abstract: Proposals are being considered to improve the system of measures aimed at ensuring information security in the BRICS countries, the Russian Federation, as well as at the regional level. The measures designed to counteract transnational cybercrime and the use of cyberspace of the BRICS countries for criminal purposes are analyzed, and emerging threats to national security are noted. The role of scientific research in the implementation of these measures is considered separately, attention is drawn to the importance of developing cooperation between the BRICS countries.

Keywords: information security, cybercrime, cyberspace, crime prevention, BRICS cooperation.

Для цитирования: Мазуров В.А. О некоторых аспектах обеспечения информационной безопасности и противодействия транснациональной киберпреступности в современном мире // Проблемы правовой и технической защиты информации. 2024. №12. С.48-51.

For citation: Mazurov V.A. On some aspects of ensuring information security and countering transnational cybercrime in the modern world // Legal and Technical Problems of Information Security. 2024. No. 12. P.48-51.

Стремительное развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз миру и безопасности не только отдельным государствам и народам, но и земной цивилизации в целом [1]. Озабоченность сегодня вызывает и работа над созданием искусственного интеллекта, особенно в странах Запада. Возникают вопросы, какие установки он получит, какие последствия от его включения в жизнедеятельность человечества следует ожидать, какие меры уже сегодня нужно принимать, чтобы

избежать или минимизировать возможные угрозы и ряд других вопросов и проблем [2].

Современная международная обстановка оставляет желать лучшего и характеризуется следующими обстоятельствами, которые сегодня реально представляют угрозу миру и безопасности человечества:

– значительное усиление и рост геополитической нестабильности в мире и межгосударственных противоречий, которые сопровождаются угрозой применения военной силы;

– военно-политическое противостояние между странами Востока и Запада, локальные военные конфликты, информационные и экономические войны, пропаганда военной силы, межнациональной и межконфессиональной ненависти, идеологии терроризма и иных деструктивных идеологий [3];

– использование информационно-коммуникационных технологий для вмешательства во внутренние дела государств;

– игнорирование отдельными странами Запада общепризнанных норм и принципов международного права, ослабление и разрушение существующих международных правовых институтов. И ряд других обстоятельств.

Указанные обстоятельства создают серьезные проблемы по формированию системы мер по обеспечению информационной безопасности и противодействию транснациональной киберпреступности на неопределенный период времени [4]. На наш взгляд, обеспечить или значительно снизить угрозы в киберпространстве, возможно путем создания системы коллективной кибербезопасности на межгосударственном уровне. Сегодня, как никогда, возникла необходимость создания такой системы мер в рамках дружественных России государств.

В Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 2 июля 2021 года №400 [5], в качестве приоритетного направления во внешней политике России, указана работа по укреплению сотрудничества Российской Федерации с иностранными партнерами в области обеспечения кибербезопасности. Углубление многопрофильного сотрудничества с иностранными государствами в форматах Шанхайской организации сотрудничества и БРИКС.

В систему мер по обеспечению информационной безопасности и противодействию киберпреступности входят: организационно - правовые, научно-технические меры, иные меры профилактики, в том числе пропаганда и контрпропаганда [6].

Организационно – правовые меры:

– разработка и принятие международных официальных документов, регулирующих вопросы взаимодействия между государствами – участниками соглашений по обеспечению информационной безопасности и противодействию транснациональной киберпреступности в мероприятиях, направленных на её предупреждение;

– разработка нормативных актов, определяющих организацию оперативно-следственной работы, взаимодействие между правоохранительными органами стран-участников соглашений по обеспечению кибербезопасности. Разработка составов преступлений в киберпространстве и включение соответствующих правовых норм в уголовные кодексы стран БРИКС. Предлагается выработать единый подход по отнесению конкретных составов киберпреступлений в национальное уголовное законодательство этих государств. Так, например, в европейских государствах определены составы преступлений, которые необходимо внести в уголовные кодексы этих государств (минимальный список) и составы преступлений, рекомендованные для включения в уголовное законодательство по желанию этих государств.

К организационно-правовым мерам можно отнести создание структуры, на которую бы были возложены функции по

организации, координации и анализу результатов мероприятий по обеспечению информационной безопасности и противодействию транснациональной киберпреступности в странах БРИКС.

Научное исследование проблем обеспечения информационной безопасности и противодействия киберпреступности сегодня является одной из приоритетных задач по организации эффективной работы по обеспечению кибербезопасности как в отдельно взятой стране, так и в содружестве государств БРИКС. На наш взгляд, научные исследования проблем обеспечения кибербезопасности – информационной безопасности и противодействие преступности в киберпространстве, разработку и научное обоснование профилактических мероприятий, целесообразно осуществлять с привлечением к этой деятельности ученых в сфере цифровых технологий и ученых правоведов [7].

Можно констатировать проверенную практикой особенность данной деятельности, которая проявляется в консолидации ученых в сфере цифровых технологий и ученых-правоведов. Так, на сегодняшний день в Алтайском крае, на базе ФГБОУ ВО «Алтайский государственный университет» действует, созданный в 2006 году, Региональный научно-методический центр правовой и технической защиты информации (далее Центр). Инициаторами и активными участниками в работе Центра, являются, главным образом, преподаватели и студенты института цифровых технологий, электроники и физики, и юридического института. Работа в Центре осуществляется на общественных началах.

В этих целях, предлагается рассмотреть возможность, в рамках соглашений по сотрудничеству между странами БРИКС, на федеральном уровне создать Институт (Центр) исследований проблем обеспечения информационной безопасности транснациональной киберпреступности. Так, например, в США, Великобритании и ряде других государств мира, созданы государственные и общественные структуры по научному исследованию проблем кибербезопасности. (Институт компьютерной безопасности в США, Национальный центр по борьбе с преступлениями в сфере высоких технологий в Великобритании).

Создание такого рода структуры, позволит целенаправленно, в плановом порядке, осуществлять научное изучение проблем кибербезопасности в России и странах БРИКС. Проведение ежегодных тематических международных конференций, семинаров и круглых столов. Все это, в конечном итоге, позволит предметно вносить предложения по совершенствованию законотворческой и правоприменительной практики, а также совершенствовать программы по подготовке специалистов для правоохранительных органов, ученых в сфере цифровых технологий и юриспруденции и других практических работников в сфере профилактики киберпреступности.

Предлагается следующая система организации и координации работы по обеспечению кибербезопасности в России. Целесообразно образовать на федеральном уровне Национальный комитет кибербезопасности Российской Федерации (НККБ РФ). В регионах создать комиссии по обеспечению кибербезопасности региональных органах исполнительной власти [8]. В ряде вузов России, располагающих реальными возможностями по исследованию и решению проблем обеспечения информационной безопасности и противодействию киберпреступности, в структуру вузов ввести Научно-исследовательские центры кибербезопасности (НИЦК). Материалы НККБ и НИЦК можно и нужно использовать в профилактических мероприятиях. На наш взгляд, большое профилактическое значение имеет пропаганда правовой грамотности населения, активной гражданской позиции, патриотизма и иных положительных духовно-нравственных качеств, главным образом, направленная на современную молодежь, которая сегодня является

основным объектом внимания спецслужб недружественных государств, деструктивных и откровенно враждебных сил в киберпространстве, а также контрпропаганда этой деятельности.

Таким образом, результативность и эффективность обеспечения кибербезопасности – информационной безопасности и противодействия преступности в киберпространстве, на наш взгляд, во многом зависит от решения следующих задач:

– стремительное развитие цифровых технологий предопределило серьезные угрозы миру и безопасности, как отдельным государствам, так и международному сообществу в целом, что требует консолидации миролюбивых стран в обеспечении кибербезопасности;

– создание в России системы организации, координации, анализа и разработки предложений по обеспечению безопасности в киберпространстве: НККБ РФ – комиссии по кибербезопасности в региональных исполнительных органах власти – НИЦК в вузах;

– научные исследования проблем обеспечения кибербезопасности осуществлять с привлечением ученых в сфере цифровых технологий, ученых-правоведов и специалистов-практиков.

Выводы и предложения, изложенные в данной работе, не носят исчерпывающий характер, не претендуют на исключительность и бесспорность и, главным образом, рассчитаны на привлечение внимания ученых и специалистов в сфере цифровых технологий и права для углубленного изучения проблем обеспечения информационной безопасности и повышение эффективности противодействия киберпреступности и обеспечения информационной безопасности.

Библиографический список

1. *Головин А.В., Исаев А.А., Мазуров В.А., Поляков В.В., Сидоренко Т.В. Уголовно-правовые и криминологические проблемы защиты информации: монография. Алматы: Изд. центр ОФППИ Интерлигал, 2008. - 338 с.*
2. *О развитии искусственного интеллекта в Российской Федерации : указ Президента Российской Федерации от 10 октября 2019 года № 490 // Собрание законодательства Российской Федерации. – 2019. – № 41. – Ст. 5700.*
3. *Градусова М.М., Мазуров В.А., Потапов Д.П., Снесарь В.В., Труфанов А.Ю. Националистический и религиозный векторы в экстремизме и терроризме: уголовно-правовой и криминологический анализ: монография. – Барнаул: Изд-во Алт. ун-та, 2010. – 399 с.*
4. *Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Российской Федерации от 05 декабря 2016 года № 646 // Собрание законодательства Российской Федерации. – 2016. – № 50. – Ст. 7074*
5. *Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 2 июля 2021 г. № 400. – 43 с. http://www.kremlin.ru/acts/bank/47046 (дата обращения: 10.08.2024).*
6. *Мазуров В.А., Поляков В.В. Криминолого-криминалистическое предупреждение преступности в сфере высоких информационных и телекоммуникационных технологий // Известия АлтГУ. – 2009. - № 2. – С. 95-98.*
7. *Поляков Вит.В., В.А. Мазуров. Использование цифровых средств обучения при подготовке специалистов для правоохранительных органов. Сб. статей I Всерос. научно-практ. конф. «Использование цифровых средств обучения и робототехники в общем и профессиональном образовании: опыт, проблемы, перспективы». Барнаул, 5-6 ноября 2013. Барнаул: Изд-во Алт. ун-та, 2013. С. 109-111.*
8. *В.В. Поляков, В.А. Трушин, В.А. Мазуров и др. Региональные аспекты технической и правовой защиты информации: монография. Барнаул: Изд-во Алт. ун-та, 2013. – 194 с.*