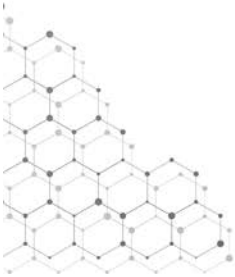
Министерство науки и высшего образования Российской Федерации
Министерство внутренних дел Российской Федерации

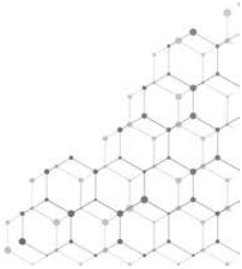
Московский университет Министерства внутренних дел
Российской Федерации имени В.Я. Кикотя

Ю. В. Пузырева, Е. Е. Бардина, Д. Д. Шалягин

НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ МВД РОССИИ ПО ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В РАМКАХ РЕАЛИЗАЦИИ ОСНОВ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аналитический обзор





Москва

Московский университет
МВД России имени В.Я. Кикотя

2023

УДК 341
ББК 67.9
П88

Рецензенты:
заместитель начальника ОМО УМС МВД России **Ю. В. Исаев**;
заместитель начальника 6-го отдела НЦБ Интерпола
МВД России **С. В. Михайлов**

Пузырева, Ю. В.

П88 **Направления деятельности МВД России по повышению эффективности международного сотрудничества в борьбе с преступлениями в сфере информационно-коммуникационных технологий в рамках реализации Основ государственной политики Российской Федерации в области международной информационной безопасности** : аналитический обзор / Ю. В. Пузырева, Е. Е. Бардина, Д. Д. Шалягин. – М. : Московский университет МВД России имени В.Я. Кикотя, 2023. – 258 с.

ISBN 978-5-9694-1390-0

В аналитическом обзоре с предложениями определен вклад МВД России в разработку всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, проанализированы основные направления развития и совершенствования сотрудничества по линии МВД России со стратегическими партнерами Российской Федерации, также изучены проблемы информационного обмена между МВД России и правоохранительными органами иностранных государств в ходе расследования преступлений в сфере компьютерной информации.

По итогам проведенного исследования сформулированы предложения, направленные на повышение эффективности международного сотрудничества в борьбе с преступлениями в рамках реализации Основ государственной политики Российской Федерации в области международной информационной безопасности.

УДК 341
ББК 67.9

ISBN 978-5-9694-1390-0

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В 2022 г. на кафедре прав человека и международного права Московского университета МВД России имени В.Я. Кикотя по заявке УМС МВД России от 27 сентября 2021 г. № 4/11755 осуществлялась разработка научно-исследовательской темы «Направления деятельности МВД России по повышению эффективности международного сотрудничества в борьбе с преступлениями в сфере информационно-коммуникационных технологий в рамках реализации Основ государственной политики Российской Федерации в области международной информационной безопасности».

Результатом научного исследования стал аналитический отчет с предложениями, подготовленный в целях разработки основных направлений деятельности МВД России по реализации государственной политики в области международной информационной безопасности в части совершенствования международного сотрудничества, направленного на противодействие угрозе использования информационно-коммуникационных технологий в преступных целях, и создания необходимого для этого международно-правового режима.

Исследование проводилось по следующим направлениям:

– определение вклада МВД России в разработку всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях;

– формирование основных направлений развития и совершенствования сотрудничества по линии МВД России с государствами – участниками СНГ, ШОС, БРИКС, ОДКБ и иными стратегическими партнерами Российской Федерации по вопросам противодействия угрозе использования информационных технологий в преступных целях;

– анализ проблем информационного обмена между МВД России и правоохранительными органами иностранных государств, а также изучение механизмов обмена информацией в рамках расследования преступлений в сфере компьютерной информации между государствами (использование информационных каналов связи для повышения эффективности взаимодействия между правоохранительными органами; допустимость электронных доказательств, полученных по электронным каналам связи).

ГЛАВА I
Основные характеристики государственной политики Российской Федерации в области международной информационной безопасности

Указом Президента Российской Федерации от 12 апреля 2021 г. № 213 утверждены Основы государственной политики Российской Федерации в области международной информационной безопасности (далее – Основы), которые направлены:

«а) на продвижение на международной арене российских подходов к формированию системы обеспечения международной информационной безопасности и российских инициатив в области международной информационной безопасности;

б) на содействие созданию международно-правовых механизмов предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве;

в) на организацию межведомственного взаимодействия при реализации государственной политики в области международной информационной безопасности»[1].

Основами конкретизируются отдельные положения Стратегии национальной безопасности Российской Федерации[2], Док-

[1] Ключевой документ, формулирующий цель государственной политики – содействие установлению международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности. См.: Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // НПП «Гарант-сервис». URL: https://www.garant.ru/products/ipo/prime/doc/400473497/.

[2] Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_389271/.

трины информационной безопасности Российской Федерации[1], Концепции внешней политики Российской Федерации[2] и других документов стратегического планирования[3].

Содействие установлению международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности (далее – МИБ), призванной оказать противодействие угрозам для стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве, является целью государственной политики Российской Федерации в области МИБ. Эта деятельность неразрывно связана с обеспечением информационной безопасности страны и является стратегически важным направлением обеспечения национальной безопасности Российской Федерации[4].

На международном уровне Российская Федерация – активный и авторитетный участник международного взаимодействия по обеспечению информационной безопасности. В 1998 г. Рос-

---

[1] Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_208191/.

[2] Указ Президента Российской Федерации от 30 ноября 201 г. № 640 «Об утверждении Концепции внешней политики Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_-LAW_207990/.

[3] Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_216363/ ; Указ Президента Российской Федерации от 25 декабря 2014 г. № Пр-2976 «Об утверждении Военной доктрины Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.-consultant.ru/document/cons_doc_LAW_172989/ ; Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации : утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274.

[4] Международная информационная безопасность. Теория и практика : учебник для вузов : в 3 т. Т. 1 / [А. В. Бирюков и др.] ; под общ. ред. А. В. Крутских. М. : Аспект Пресс, 2021. С. 11.

сия впервые инициировала обсуждение проблематики международной информационной безопасности на международном уровне в рамках Организации Объединенных Наций. Следует отметить, что к настоящему времени выработано значительное количество российских инициатив в рассматриваемой области, обсуждение которых проходит на площадке ООН: правила ответственного поведения государств в глобальном информационном пространстве; концепция конвенции ООН об обеспечении международной информационной безопасности; конвенция о сотрудничестве в сфере противодействия информационной преступности; концепция безопасного функционирования и развития сети Интернет.

Кроме того, Россия выступает за развитие сотрудничества в данной области в рамках таких переговорных площадок, как СНГ, ШОС, ОБСЕ, БРИКС, ОДКБ, а также иных региональных организаций.

На уровне государственной политики следует отметить рост инициатив в данной области, связанных, в частности, с разработкой комплексных межведомственных позиций по проекту всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

В настоящее время единой общепризнанной государствами дефиниции в отношении МИБ не выработано. Однако сложилось однозначное понимание трактовки рассматриваемого вида международной безопасности, исходя из характера угроз, присущих данной сфере, к которым традиционно относится использование информационно-коммуникационных технологий (далее – ИКТ) в террористических, преступных и военно-политических целях. Подобный подход к определению угроз

был закреплен в ряде резолюций Генеральной Ассамблеи ООН, посвященных проблематике информационной безопасности[1].

В принятых в Российской Федерации в 2013 г. Основах государственной политики в области международной информационной безопасности на период до 2020 г. К числу угроз была добавлена опасность вмешательства во внутренние дела суверенного государства посредством ИКТ, нарушения общественной стабильности, разжигания межэтнической, межнациональной розни[2]. В принятых в 2021 г. Основах перечень угроз международной информационной безопасности вновь был расширен за счет включения опасности «…использования ИКТ для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру», а также «…использования отдельными государствами технологического доминирования в глобальном информационном пространстве для монополизации рынка информационно-коммуникационных технологий… а также для усиления их технологической зависимости от доминирующих

[1] Резолюции Генеральной Ассамблеи Организации Объединенных Наций от 27 декабря 2013 г. A/RES/68/243, от 2 декабря 2014 г. A/RES/69/28, от 23 декабря 2015 г. A/RES/70/237, от 5 декабря 2016 г. A/RES/71/28, от 5 декабря 2018 г. A/RES/73/27, от 12 декабря 2019 г. A/RES/74/29 и от 31 декабря 2020 г. A/RES/75/240 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» ; Резолюция Генеральной Ассамблеи ООН от 27 декабря 2019 г. № 74/274 «Противодействие использованию информационно-коммуникационных технологий в преступных целях».

[2] Указ Президента Российской Федерации от 24 июля 2013 г. № Пр-1753 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_178634/.

в сфере информатизации государств и информационного неравенства»[1].

В этой связи Российская Федерация выступает за широкий подход к определению содержания понятия «международная информационная безопасность», которое включает в себя как технические аспекты (безопасность информационных сетей и систем), так и обширный круг политико-идеологических аспектов (манипулирование информацией, пропаганда посредством глобальных информационных сетей, информационное воздействие), а также механизмы борьбы с преступностью в данной сфере.

Следует отметить, что страны Запада (прежде всего США) придерживаются узкого подхода, ограничиваясь техническими аспектами, и используют иную терминологию – «кибербезопасность»[2].

Согласно действующим Основам государственной политики Российской Федерации в области международной информационной безопасности, МИБ «представляет собой такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности» (п. 6).

К угрозам МИБ, как было отмечено ранее, относится широкий перечень проблем, среди которых имеются позиции, относящиеся к компетенции МВД России и определяющие активный вклад в развитие эффективной государственной политики в об-

---

[1] Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // НПП «Гарант-сервис». URL: https://www.garant.ru/products/ipo/prime/doc/400473497/.

[2] Зиновьева Е. Информационная безопасность Российской Федерации на современном этапе развития международных отношений // Официальный сайт МГИМО МИД России. URL: https://mgimo.ru/about/news/experts/258416/.

ласти МИБ в части совершенствования международного сотрудничества, направленного на противодействие угрозе использования ИКТ в преступных целях (п. 8, «г»).

В частности, согласно п. 15 Основ, «Основными направлениями реализации государственной политики в области международной информационной безопасности по повышению эффективности международного сотрудничества, направленного на противодействие угрозе использования информационно-коммуникационных технологий в преступных целях, и по созданию необходимого для этого международно-правового режима являются:

а) содействие разработке специальным межправительственным комитетом экспертов открытого состава всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, а также создание условий для последующего принятия государствами – членами ООН данной конвенции;

б) развитие сотрудничества с государствами – участниками СНГ, объединения БРИКС, государствами – членами ОДКБ, ШОС, АСЕАН, Группы двадцати, другими государствами и международными организациями по вопросам противодействия угрозе использования информационно-коммуникационных технологий в преступных целях;

в) повышение эффективности информационного обмена между правоохранительными органами государств в ходе расследования преступлений в сфере компьютерной информации, а также случаев мошенничества с использованием информационно-коммуникационных технологий;

г) совершенствование механизма обмена информацией о методиках расследования преступлений в сфере компьютерной информации, случаев мошенничества с использованием информационно-коммуникационных технологий, а также о судебной практике рассмотрения уголовных дел о таких преступлениях;

д) организация международных конференций и семинаров по вопросам противодействия использованию информационно-коммуникационных технологий в преступных целях».

В Основах закреплено, что «…достижение цели государственной политики в области МИБ осуществляется путем решения задач по развитию на глобальном, региональном, многостороннем и двустороннем уровнях сотрудничества Российской Федерации с иностранными государствами по вопросам формирования системы обеспечения международной информационной безопасности, а также противодействия основным угрозам международной информационной безопасности» (п. 10). Данный глобальный аспект определяет основные направления развития и совершенствования сотрудничества МВД России со стратегическими партнерами Российской Федерации по вопросам противодействия угрозе использования ИКТ в преступных целях.

Подготовка предложений по формированию, совершенствованию и реализации государственной политики в области МИБ, а также контроль за исполнением органами государственной власти решений по вопросам координации деятельности в указанной сфере осуществляется органами Совета Безопасности Российской Федерации.

МИД России во взаимодействии с федеральными органами исполнительной власти участвует в разработке и реализации основных направлений государственной политики в области МИБ, осуществляет координацию деятельности федеральных органов исполнительной власти по реализации указанной политики, а также продвижение на международной арене позиции Российской Федерации по вопросу обеспечения данной сферы.

Федеральные органы исполнительной власти, включая МВД России, реализуют государственную политику в области МИБ в соответствии с их компетенциями, в том числе на основе государственно-частного партнерства.

ГЛАВА II
Вклад МВД России в разработку всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях

§ 2.1. Правовые и организационные основы разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях

Происходящая в последние десятилетия «цифровая революция» открывает колоссальные перспективы для развития государств, но также создает новые возможности для преступников и может способствовать повышению уровня и усложнению характера преступности. Кибератаки усиливаются в своих размерах, сложности и стоимости.

Поиск универсального решения противодействию глобальной преступности в сфере информационно-коммуникационных технологий в современных условиях возможен только путем переговоров в формате ООН. Именно поэтому Россия вместе с единомышленниками выступает за разработку универсальных норм, которые разделяли бы все заинтересованные стороны и которые закладывали бы основы эффективного и транспарентного международного сотрудничества по борьбе с этой угрозой с учетом интересов всех без исключения стран и основывались на принципах суверенного равенства сторон и невмешательства во внутренние дела государств.

В качестве первого шага по инициативе России в 2018 г. Генеральной Ассамблеей ООН была принята резолюция 73/187 «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Ее соавторами стали 36 государств, проголосовали за данную резолюцию 94 государства.

В 2019 г. в качестве логического продолжения своих подходов Россия совместно с единомышленниками выступила инициатором внесения в ходе 74-й сессии Генассамблеи ООН очередной резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Ее соавторами стали 47 государств, проголосовали за данную резолюцию 79 государств[1].

В соответствии с принятой 27 декабря 2019 г. резолюцией 74/247 Генассамблея ООН учредила Специальный межправительственный комитет экспертов открытого состава (далее – Спецкомитет) для разработки конвенции ООН о сотрудничестве в сфере противодействия использованию информационно-коммуникационных технологий в преступных целях[2]. Принятие этого документа подтверждает актуальность данной проблемы и при этом подчеркивает, что прогресс в этой области продвигается медленно.

27 июля 2021 г. Россия внесла в Спецкомитет российский проект первого в истории универсального договора о противо-

---

[1] Обращает на себя внимание значительное увеличение числа соавторов российских резолюций (с 36 в 2018 г. до 47 в 2019 г.) в отношении такой политизированной и неконсенсусной темы, что лишний раз подчеркивает возросший спрос мирового сообщества на разработку юридически обязательного универсального международно-правового договора в данной области. Но на прежнем уровне остается количество государств – противников идеи разработки такой конвенции (в 2018 г. – 59, в 2019 г. – 60). К ним, прежде всего, относятся все технологически развитые страны – США, ЕС и их союзники.

[2] Противодействие использованию информационно-коммуникационных технологий в преступных целях // The United Nations. URL: https://undocs.org/ru/A/C.3/74/L.11/Rev.1.

действии использованию информационно-коммуникационных технологий в преступных целях[1].

Таким образом, Российская Федерация, инициировавшая в 2019 г. создание профильного органа ООН для разработки всеобъемлющей международной конвенции, и собрала поддержку мирового сообщества, предложив проекты резолюций Генассамблеи ООН 74/247 и 75/282, регулирующие модальности Спецкомитета, первой субстантивно наполнила процесс разработки столь важного и необходимого международного договора, призванного поднять международное сотрудничество в этой сфере на качественно новый уровень. Работу над итоговым проектом конвенции планируется завершить в 2024 г. в ходе 78-й сессии Генассамблеи ООН[2].

Первая сессия Спецкомитета прошла в штаб-квартире ООН в Нью-Йорке с 28 февраля по 11 марта 2022 г. Разработана «Дорожная карта», определяющая порядок его работы.

§ 2.2. Предложения по доработке текста проекта всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях

В соответствии с Указом Президента Российской Федерации от 21 декабря 2016 г. № 699 «Об утверждении Положения

---

[1] О внесении в Спецкомитет ООН российского проекта универсальной международной конвенции по противодействию использованию ИКТ в преступных целях // МИД России. URL: https://archive.mid.ru/foreign_policy/news//-asset_publisher/cKNonkJE02Bw/content/id/4831832.

[2] Proposed roadmap and mode of work of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes // The United Nations Office on Drugs and Crime. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/V2201024.pdf.

о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации» (с изм. и доп., вступ. в силу с 01.01.2022) МВД России согласно своим полномочиям «…участвует в пределах своей компетенции в разработке и реализации основных направлений государственной политики Российской Федерации в области международной информационной безопасности»[1].

В этой связи представляется актуальным рассмотрение ведомственных предложений по проекту наиболее ожидаемого и востребованного универсального международного соглашения, регулирующего вопросы противодействия использованию информационно-коммуникационных технологий в преступных целях.

Согласно «Дорожной карте» по работе Спецкомитета на сессиях запланировано рассмотрение важных разделов будущей конвенции: преамбула, сфера охвата, цели, общие положения, вопросы криминализации; процессуальные меры и правоприменение; международное сотрудничество; положения о технической помощи; профилактические меры; механизмы реализации[2].

---

[1] Указ Президента Российской Федерации от 21 декабря 2016 г. № 699 «Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации» (с изм. и доп., вступ. в силу с 01.01.2022) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_209309/.

[2] Proposed roadmap and mode of work of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes // The United Nations Office on Drugs and Crime. URL: https://www.unodc.org/documents/Cybercrime/-AdHocCommittee/First_session/V2201024.pdf.

1. Преамбула

1.1. Представляется необходимым в первые позиции преамбулы добавить положение о необходимости строгого соблюдения принципа невмешательства во внутренние дела государства, суверенного равенства и территориальной целостности государств: *«…будучи убеждены в том, что информационное пространство должно строиться в строгом соответствии с основными принципами и нормами международного права, в том числе принципами уважения прав и свобод человека, невмешательства во внутренние дела государства, суверенного равенства и территориальной целостности».*

Присутствие данных принципов в преамбуле соглашения подчеркнет концептуальную черту данного договора – построение отношений в сфере противодействия использованию ИКТ в преступных целях на основе суверенного равенства и полного контроля любых правоотношений, подпадающих под государственную юрисдикцию. Данное положение подчеркивает принципиальную разницу со ст. 32 Будапештской конвенции Совета Европы 2001 г., допускающей трансграничный доступ государств к компьютерным данным иностранных государств в целях противодействия киберпреступности.

Актуализировать данный аспект особенно важно, поскольку на глобальном уровне до настоящего времени не разработано, не подписано и не ратифицировано ни одного международного договора, предметом которого являлись бы общие принципы построения системы МИБ. Вместе с тем информационное пространство как пятое общее пространство после наземного, морского, воздушного и космического требует координации, сотрудничества и особых регулирующих правовых мер на международном уровне[1]. Предлагаемые принципы актуальны в свете

[1] Волеводз А. Г. К вопросу о системе единого правового регулирования международной информационной безопасности и противодействия посягающим на нее преступлениям // XII Конвент РАМИ. URL: https://risa.ru/images/-12theses/0-1/8-vole-vodz.pdf.

правовых идей, изложенных в ст. 3 проекта конвенции «Защита суверенитета».

1.2. Представляется необходимым добавить в преамбулу позицию относительно признания разработанных региональных соглашений по рассматриваемой проблематике, которые, к сожалению, фрагментарны и носят разрозненный характер в части закрепляемых обязательств, подчеркнув необходимость разработки первого универсального соглашения в данной сфере.

К настоящему времени на региональном уровне приняты отдельные соглашения: Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий 2018 г., Конвенция Совета Европы о киберпреступности 2001 г., Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий 2010 г.

Результатом данной «регионализации» стала фрагментация позиций, препятствующая выработке общего понимания ключевых аспектов противодействия незаконным действиям в информационной сфере, а также уход некоторых разработанных инструментов в политическую плоскость.

В этой связи вполне приемлемо добавление в преамбулу следующего положения: «*…принимая к сведению с признательностью*[1] *многосторонние региональные документы по противодействию противоправным деяниям в информационной сфере, включая, в частности, Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий 2018 г., Конвенцию Совета Европы о киберпреступности 2001 г., Конвенцию Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий 2010 г., приветствуем принятие всеобъемлющего международного соглашения о противодействии использованию ин-*

[1] Или *«…признавая важность региональных документов о борьбе с киберпреступностью»*.

формационно-коммуникационных технологий в преступных целях, в полной мере учитывающего существующие международные документы и предпринимаемые на национальном, региональном и международном уровнях усилия по борьбе с использованием информационно-коммуникационных технологий в преступных целях».

Кроме того, обращение в преамбуле к нескольким региональным договорам в сфере противодействия информационным преступным проявлениям подчеркнет вклад отдельных региональных организаций в правовую регламентацию данной сферы кроме многочисленных упоминаний Совета Европы и Будапештской конвенции 2001 г.

Как отмечено в тезисах выступления главы российской делегации по п. 4 повестки дня первой субстантивной сессии Спецкомитета («Цели и охват конвенции») (Нью-Йорк, 2 марта 2022 г.), в рамках переговорного процесса ряд делегаций, ссылаясь на резолюцию Генассамблеи ООН 74/247, приводят в пример такой документ, как Конвенция Совета Европы по противодействию компьютерным преступлениям. Однако это «…далеко не единственный ныне существующий региональный документ. В соответствии с оперативным параграфом 2 резолюции 74/247 в своей работе Спецкомитет должен в полной мере учитывать существующие региональные инструменты».

Кроме того, во всех тематических резолюциях Генассамблеи ООН и в докладах ГПЭ отмечается большое значение международных и региональных норм о борьбе с преступлениями в сфере ИТ и проводимой работы по изучению путей укрепления существующих и разработки новых национальных, международно-правовых и других мер противодействия использованию ИТ в преступных целях[1].

---

[1] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2015 г. // Официальный сайт ООН. URL: https://undocs.org/ru/A/70/174 ; Резолюция Генеральной Ассамблеи ООН от 17 декабря 2017 г. A/RES/73/187 // Официальный сайт ООН. URL: https://undocs.org/ru/A/RES/73/187.

2. Общие положения

2.1. Положения по целям договора

В настоящее время на первом заседании Спецкомитета на обсуждения вынесены следующие цели конвенции:

– продвигать и укреплять меры по предотвращению и борьбе с использованием ИКТ в преступных целях / киберпреступности, защищая при этом пользователей ИКТ от таких преступлений;

– продвигать, облегчать и поддерживать международное сотрудничество в предотвращении и борьбе с использованием ИКТ в преступных целях / киберпреступности;

– предоставлять практические инструменты для расширения технической помощи между государствами-участниками и наращивания потенциала национальных органов по предотвращению и борьбе с использованием ИКТ в преступных целях / киберпреступности, а также усилить меры по содействию обмену информацией, опытом и передовой практикой[1].

Следует отметить, что в действующих региональных инструментах по преступности в сфере ИТ присутствуют более краткие и «сдержанные» конструкции, раскрывающие цели договоров *(прил. 1)*.

В Конвенции ООН по транснациональной организованной преступности 2000 г., на которую ссылаются в своих заявлениях делегаты Спецкомитета[2], цель соглашения представлена

[1] Proposals on objectives and scope of the Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes // The United Nations. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/V2201067.pdf.

[2] В заявлениях большинства делегатов государств-членов на первой сессии Спецкомитета, заявлениях межправительственных и неправительственных организаций подчеркнуто, что разрабатываемая конвенция должна в значительной мере опираться на Конвенцию ООН против транснациональной организованной преступности 2000 г. и Конвенцию ООН против коррупции 2003 г., а также на другие концепции, которые были согласованы консенсусом на конгрессах ООН по предупреждению преступности и уголовному правосудию и на других форумах ООН, в зависимости от обстоятельств.

в одно предложение: «…содействие сотрудничеству в деле более эффективного предупреждения транснациональной организованной преступности и борьбы с ней» (ст. 1).

Следует рассмотреть и цели Конвенции ООН против коррупции 2003 г., использование которой необходимо при разработке всеобъемлющей ИКТ-конвенции:

«a) содействие принятию и укрепление мер, направленных на более эффективное и действенное предупреждение коррупции и борьбу с ней;

b) поощрение, облегчение и поддержка международного сотрудничества и технической помощи в предупреждении коррупции и борьбе с ней, в том числе принятии мер по возвращению активов;

c) поощрение честности и неподкупности, ответственности, а также надлежащего управления публичными делами и публичным имуществом» (ст. 1).

Анализ положений наиболее значимых для проводимого исследования соглашений в части закрепленных целей позволяет выделить следующее:

– емкость «целевых» формулировок;

– акцент на двух важных направлениях противодействия: предупреждении и борьбе;

– неотъемлемый «целевой» элемент – международное сотрудничество.

С учетом специфики сферы информационно-коммуникационных технологий дополнительным элементом целей будущего договора должно выступать предоставление практических инструментов для расширения технической помощи между государствами-участниками и наращивания потенциала национальных органов по предотвращению и борьбе с использованием ИКТ в преступных целях, а также обмен информацией, опытом и передовой практикой. Эффективная техническая поддержка особенно важна для малых развивающихся государств,

поскольку способствует укреплению их внутренних возможностей в борьбе с транснациональной киберпреступностью.

В российском проекте конвенции рассматриваемые ключевые цели также нашли отражение и детализированы следующим образом: «…предупреждение, выявление, пресечение, расследование и преследование за совершаемые правонарушения и преступления в сфере ИКТ». Полагаем, что такая детализация позволит государствам сотрудничать в противодействии преступности в данной сфере на каждом этапе.

В одной из целей, отраженных в российском проекте, содержится следующее положение: «…преследование за их совершение как на внутригосударственном, так и на международном уровнях». Международный уровень юрисдикции в сфере противодействия преступности представлен работой международных органов юстиции, осуществляющих преследование и наказание за совершение международных преступлений. К таким органам юстиции относятся суды и трибуналы ad hoc, а также постоянно действующий Международный уголовный суд. К международным преступлениям относят акты геноцида, военные преступления, преступления против человечества и агрессию. Любая преступная деятельность в сфере ИКТ, насколько глобален ни был бы ущерб и насколько масштабно ни проходила бы связь между преступными элементами, является исключительно транснациональным преступлением, раскрытием и расследованием которого должны заниматься компетентные органы определенных государств в пределах своей юрисдикции и в рамках имеющихся механизмов международной помощи по уголовным делам.

В связи с этим, как представляется, цели проекта должны быть сохранены в полном объеме в части разработанной концепции, представленной в проекте, но при этом упрощены в части формулировок и правовых конструкций.

2.2. Положения по сфере применения договора

Как и всякий нормативный акт, международный договор имеет собственные сферы действия: пространственную, предметную, во времени и по кругу лиц. В международно-правовых актах нередко вместо термина «действие» используется термин «применение». Основные моменты, регламентирующие договорные вопросы между государствами, представлены в Венской конвенции о праве международных договоров 1969 г.

Если проанализировать сферы применения региональных договоров по информационным технологиям, то следует сделать выводы об отсутствии такой нормы в отдельных соглашениях (Будапештская конвенция 2001 г.), а также о различных подходах правового наполнения данного элемента договора (Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий 2010 г.) *(прил. 2).*

В соглашениях ООН против транснациональной организованной преступности (далее – ТОП) и борьбе с коррупцией закреплены идентичные статьи (ст. 3), регламентирующие сферы применения договоров. Содержание этих статей сводится к определению элементов борьбы с преступностью, которые должны быть реализованы для достижения целей договоров, общей характеристики составов противоправных деяний, входящих в предмет договоров, а также дополнительных условий, необходимых для реализации положений договоров.

В российском проекте будущей конвенции сфера применения сведена к базовым положениям, аналогичным тем, которые отражены в ст. 3 Конвенции ООН против коррупции 2003 г.

Вместе с тем с учетом развития переговоров в рамках Спецкомитета о составах преступлений, которые будут закреплены в разделе «Криминализация» будущего договора, сфера применения конвенции может быть расширена в отдельных вопросах международного сотрудничества, например, обмен элек-

тронными доказательствами по всем «традиционным» преступлениям.

Создание такого международно-правового механизма позволит осуществлять международное сотрудничество по широкому кругу преступлений, при совершении которых используются ИКТ.

В завершение рассмотрения вопроса о сфере применения следует отметить актуальность и обязательность закрепления правил по защите суверенитета государств – участников будущего соглашения.

Одна из ключевых проблем, не позволяющая ряду государств, включая Российскую Федерацию, присоединиться к Будапештской конвенции – содержание п. «b» ст. 32. В соответствии с этой частью документа участники получают трансграничный доступ к данным, которыми располагает другая сторона, без уведомления властей данного государства, располагающего соответствующей информацией:

«Статья 32. Трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным.

Сторона может без согласия другой Стороны:

«a) получать доступ к общедоступным (открытому источнику) компьютерным данным независимо от их географического местоположения;

b) получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему».

Фактически эта норма регламентирует не что иное, как обыск в компьютерных сетях (или в среде для хранения компь-

ютерных данных) за рубежом в целях обнаружения и изъятия искомой компьютерной информации.

Учитывая архитектуру глобальных компьютерных сетей, в любой стране мира можно найти провайдера, в распоряжении которого имеются законные технические механизмы доступа к компьютерным данным (как к сведениям о сообщениях, передаваемых по сетям электросвязи, так и к самим сообщениям), хранящимся за границей, или который сам (обладая физическими серверами) хранит компьютерные данные иностранного пользователя. При таких обстоятельствах получение доступа к компьютерной информации на территории иностранного государства будет осуществляться фактически бесконтрольно, с нарушением суверенных прав иностранного государства.

Кроме того, реализация данного предписания на практике потребует четкого уяснения и регламентации в национальном законодательстве понятия «лицо, на законном основании уполномоченное раскрыть компьютерные данные».

Следует отметить, что, несмотря на приведенные возражения, возможности операторов связи для доступа к находящихся за рубежом сведениям о сообщениях, передаваемых по сетям электросвязи, уже успешно используются на практике.

Обращает на себя внимание то, что предложенный Конвенцией порядок трансграничного доступа к информации оставляет открытыми некоторые вопросы:

– порядок обжалования решения о сборе компьютерных данных;

– уведомление заинтересованных граждан о проведенных в вышеназванном порядке процессуальных действиях;

– защита конфиденциальности информации, полученной таким способом;

– судебный и ведомственный контроль национальных судов и компетентных органов за законностью действий иностранных органов[1].

В этой связи и нашей делегацией, и делегациями ряда государств предлагается закрепление в будущей конвенции принципа «защиты суверенитета» при реализации отношений по договору. Такая норма содержится в двух ключевых договорах по борьбе с преступность – Конвенции ООН против ТОП 2000 г. и Конвенции ООН против коррупции 2003 г. Примечательно, что в обоих договорах статьи о защите суверенитета по своему содержанию идентичны друг другу:

«1. Государства-участники осуществляют свои обязательства согласно настоящей Конвенции в соответствии с принципами суверенного равенства и территориальной целостности государств и принципом невмешательства во внутренние дела других государств.

2. Ничто в настоящей Конвенции не наделяет государство-участника правом осуществлять на территории другого государства юрисдикцию и функции, которые входят исключительно в компетенцию органов этого другого государства в соответствии с его внутренним законодательством»[2].

Именно в такой формулировке и при сохранении такого принципа представляется необходимым вести переговорный процесс по всеобъемлющей конвенции.

В заключение отметим, что принцип защиты суверенитета закреплен также в ст. 4 Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий 2010 г.

---

[1] Волеводз А. Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. 2007. № 2. С. 17–25.

[2] Статья 4 Конвенции ООН против коррупции 2003 г., ст. 3 Конвенции ООН против ТОП 2000 г.

2.3. Терминология и определения

Анализ резолюций Генассамблеи ООН и докладов Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности позволяет сделать вывод о том, что в рамках исследуемой проблематики наиболее часто применяется терминологическая конструкция «использование информационно-коммуникационных технологий в преступных целях»[1].

В резолюциях, принимаемых Экономическим и Социальным Советом ООН по вопросам информационной безопасности, используется термин «киберпреступность»[2]. Следует отметить, что Управление ООН по наркотикам и преступности (далее – УНП ООН) уже долгие годы занимается всесторонним изучением проблем «киберпреступности»[3] в рамках специальной Группы экспертов[4].

В решениях Конгрессов ООН по предупреждению преступности и уголовному правосудию в свете анализа новых вызовов и угроз со стороны развивающейся и усложняющейся

---

[1] Резолюция Генеральной Ассамблеи ООН от 17 декабря 2018 г. «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Официальный сайт ООН. URL: https://undocs.org/ru/-A/RES/73/187 ; Доклад Генерального секретаря ООН «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Резолюция Генеральной Ассамблеи ООН A/74/130 от 30 июля 2019 г. // Официальный сайт ООН. URL: https://www.unodc.org/documents/Cybercrime/-SG_report/V1908184_R.pdf.

[2] Резолюция Экономического и Социального Совета от 23 июля 2019 г. E/RES/2019/19 «Содействие оказанию технической помощи и наращиванию потенциала для усиления национальных мер и укрепления международного сотрудничества в целях борьбы с киберпреступностью, включая обмен информацией» // Официальный сайт ООН. URL: https://undocs.org/ru/E/RES/2019/19.

[3] Всестороннее исследование проблемы киберпреступности // Официальный сайт УНП ООН. URL: https://www.unodc.org/documents/organizedcrime/-cybercrime/Cybercrime_Study_ Russian.pdf.

[4] Доклад Группы экспертов для проведения всестороннего исследования проблемы киберпреступности // Официальный сайт УНП ООН. URL: https://-undocs.org/pdf?symbol=ru/UNODC/CCPCJ/ EG.4/2019/L.1.

транснациональной организованной преступности используются такие формулировки, как «преступная деятельность, осуществляемая с помощью Интернета», «киберпреступность», «преступления, связанные с использованием компьютерной сети»[1].

В процессе разработки универсального договора в исследуемой области используются различные терминологические конструкции. Так, в 2017 г. Российская Федерация выступила в ООН с инициативным проектом конвенции о сотрудничестве в сфере противодействия информационной преступности. Проект на тот момент не нашел поддержки на площадке ООН, что побудило государства создать в 2019 г. межправительственный комитет экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Таким образом, на универсальном уровне для определения сферы сотрудничества государств по противодействию преступлениям в информационной области используются самые разные термины, что обусловливает разрозненность понятийного аппарата.

Терминология, используемая в региональных международных договорах, также позволяет судить о разнообразии подходов к ключевым дефинициям с учетом специфики отношений государств, приоритетов и характера угроз в информационном про-

---

[1] Проект Дохийской декларации о включении вопросов предупреждения преступности и уголовного правосудия в более широкую повестку дня ООН в целях решения социальных и экономических проблем и содействия обеспечению верховенства права на национальном и международном уровнях, а также участию общественности. Тринадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию // Официальный сайт ООН. URL: https://undocs.org/ru/A/CONF.222/L.6 ; Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушениями // Официальный сайт ООН. URL: https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-RU.pdf.

странстве, а также степени правовой интеграции государств различных регионов *(прил. 3)*.

В Конвенции СЕ о киберпреступности 2001 г. используется термин «киберпреступность». В Конвенции ЛАГ о борьбе с преступлениями в сфере ИТ 2010 г. и Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере ИТ 2018 г. на первый план выходит противодействие «преступлениям в сфере ИТ».

На национальном уровне правового регулирования присутствует полное расхождение в терминологии и подходах к противодействию преступлениям в сфере ИТ. Эта проблема была выявлена в Докладе Генерального секретаря ООН в соответствии с резолюцией 73/187 Генеральной Ассамблеи «Противодействие использованию информационно-коммуникационных технологий в преступных целях»[1]. По заявлениям государств, в их уголовно-правовой сфере регулирования используют следующие термины: «киберпреступность» (Австралия, Австрия, Япония, Малайзия); «неправомерное использование информационно-коммуникационных технологий» и «компьютерные преступления» (Боливия); «компьютерные преступления» (Иран, Перу, Шри-Ланка, Таиланд); «использование информационно-коммуникационных технологий в преступных целях» (Венесуэла, Аргентина).

[1] В данной резолюции Генеральная Ассамблея поручила 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 74-й сессии. Доклад содержит информацию о мнениях государств-членов, представленных во исполнение вышеупомянутой резолюции // Доклад Генерального секретаря ООН «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Резолюция Генеральной Ассамблеи ООН A/74/130 от 30 июля 2019 г. // Официальный сайт ООН. URL: https://www.unodc.org/documents/Cybercrime/SG_report/V1908184_R.pdf.

Возможно, подобные различия в терминологии, правовом значении и содержании преступлений в сфере ИТ обусловлены релевантностью их перевода с английского языка[1].

Что касается российского правового регулирования исследуемого вопроса, гл. 28 Уголовного кодекса Российской Федерации (УК РФ) обозначена как «Преступления в сфере компьютерной информации».

Несогласованность подходов к правовому регулированию вопросов противодействия преступлениям в сфере ИТ на национальном и региональном уровнях подчеркивает необходимость разработки всеобъемлющего универсального международного договора по противодействию преступлениям в сфере ИТ.

Анализ существующих легитимных дефиниций противоправных нарушений в сфере ИТ позволяет прийти к выводу о чрезмерно масштабированном подходе к терминологии в проекте всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Действующие региональные договоры сконцентрированы, главным образом, на определении ключевого термина, отраженного в названии (киберпреступность или информационные технологии), а также сопутствующих и раскрывающих его базовых понятиях (например, компьютерные данные, компьютерная система – Конвенция Совета Европы 2001 г.; информационная программа, информационная система, поставщик услуг, вредоносная программа – Конвенция ЛАГ о борьбе с преступлениями в сфере информационных технологий 2010 г., Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 г.).

---

[1] Касенова М. Б. Правовое регулирование трансграничного функционирования и использования Интернета : автореф. дис. ... д-ра юрид. наук : 12.00.03. М. : Российский государственный университет правосудия, 2016. С. 48–49.

Представляется, что вопрос о закрепляемой терминологии и определениях в проекте всеобъемлющей конвенции следует решать исходя из апробированной в региональных соглашениях концепции. На данный момент в российском проекте представлены 18 базовых дефиниций, что вызовет особое внимание у делегаций в рамках переговорного процесса, поскольку поставит перед ними сложную задачу по выработке универсальных позиций.

3. Положения о криминализации

Определение видов преступлений, связанных с использованием ИКТ в преступных целях, – вопрос, который вошел в повестку первого заседания Спецкомитета.

Данная позиция сложна в плане возможностей согласования предложений всех государств, которые различаются своими подходами с учетом угроз в ИКТ-сфере и уровнем технических возможностей по выявлению, пресечению и противодействию таким преступлениям.

Как справедливо отмечают представители делегации Российской Федерации в рамках переговорного процесса, Россия и целый ряд государств обращают внимание, что будущая конвенция посвящена не киберпреступности и сугубо компьютерным преступлениям, а использованию ИКТ в преступных целях. В соглашении должно быть отражено понимание того, что ИКТ выходит за рамки компьютеров и охватывает еще целый ряд технологий. Так называемый кибер не учитывает спутниковую, телефонную, радиосвязь.

Будущая конвенция должна носить всеобъемлющий характер в соответствии с резолюциями Генассамблеи ООН 74/247 и 75/282, т. е. она должна по возможности охватывать все составы преступных деяний, совершаемых с использованием ИКТ.

Указанную концепцию разделяют не все делегации. Так, некоторые участники переговорного процесса отмечают, что нормы конвенции должны покрывать только так называемую ки-

берпреступность, которая с подачи ряда стран ограничит охват конвенцией преступлений, совершаемых с использованием компьютеров, а также небольшого числа компьютерных преступлений, которые существуют благодаря появлению компьютеров. На английском языке это звучит как computer-dependent and computer-enabled crimes[1].

Такой подход не соответствует положениям резолюций Генассамблеи ООН 74/247 и 75/282.

Составы противоправных деяний, подлежащих криминализации в разрабатываемой конвенции, приведены в *прил. 4*. Их анализ позволяет сделать следующие выводы.

Во-первых, Конвенция СЕ 2001 г. является единственным договором, в котором составы преступлений распределены по тематическим группам. Такой подход облегчает оценку полноты закрепленных деяний и дает представление об объективности отнесения тех или преступлений к рассматриваемой ИТ-категории.

В российском проекте всеобъемлющей конвенции представлен самый обширный перечень составов, подпадающих под категорию «использование ИКТ в преступных целях». При этом составы размещены в простом перечислении, что усложняет их восприятие и дальнейшую экспертную оценку. *Предлагаем провести анализ всех представленных составов и сгруппировать их по подгруппам по аналогии с распределением статей в Будапештской конвенции 2001 г.*

Во-вторых, следует отметить, что в проекте всеобъемлющей конвенции нашли отражение практически все составы преступных деяний, признанных таковыми в региональных договорах по киберпреступности, за некоторым исключением. Так, в проекте

[1] Тезисы выступления главы российской делегации по п. 4 повестки дня первой субстантивной сессии Спецкомитета ООН по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях (Нью-Йорк, 2 марта 2022 г.) // UNODC. URL: https://www.unodc.org/unodc/ru/cybercrime/ad_hoc_committee/hom.

не закреплено мошенничество с использованием технологий (ст. 8 Конвенции СЕ 2001 г., ст. 11 Конвенции ЛАГ 2010 г.)[1]. В российском проекте учтены пожелания делегаций по апробации разработанных региональных правовых инструментов в борьбе с преступностью в сфере ИТ.

Кроме того, в российском проекте нашли закрепление следующие инновационные составы (в *прил. 4* данные составы выделены курсивом):

– неправомерное воздействие на критическую информационную инфраструктуру (ст. 11);

– несанкционированный доступ к персональным данным (ст. 12);

– склонение к самоубийству или доведение до его совершения (ст. 16);

– вовлечение несовершеннолетних в совершение противоправных действий, опасных для их жизни и здоровья (ст. 17);

– подстрекательство к подрывной или вооруженной деятельности (ст. 19);

– распространение наркотических средств и психотропных веществ (ст. 22);

– распространение фальсифицированных лекарственных средств и медицинских изделий (ст. 25);

– использование ИКТ для совершения деяний, признанных преступлениями в соответствии с международным правом (ст. 26);

– иные противоправные деяния (ст. 29).

Раздел «Криминализация деяний» российского проекта вызвал много дискуссий на площадке Спецкомитета. В частности, составы, отраженные в ст.ст. 22 и 25, имеют отношение к ситуациям использования ИКТ для совершения отдельных видов

[1] В проекте всеобъемлющей конвенции содержится ст. 18 «Создание и использование цифровой информации для введения пользователя в заблуждение». Однако ее содержание не в полной мере раскрывает мошеннические действия, закрепленные в региональных источниках.

ТОП. Вместе с тем достаточно проблематично определить наиболее сложные по уровню угроз и масштабности причиненных последствий виды транснациональной организованной преступности, требующие включения в состав будущего соглашения. Так, в ст. 16 Конвенции Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий 2010 г. к наказуемым деяниям, совершенным с использованием ИТ, относятся следующие виды ТОП:

– легализация преступных доходов;

– пропаганда употребления и незаконного оборота наркотических средств и психотропных веществ;

– торговля людьми, торговля человеческими органами;

– незаконный оборот оружия.

В этой связи на определенном этапе переговоров можно было бы рассмотреть возможность включения положения общего содержания, отражающего использование ИКТ для совершения транснациональных преступлений: «Использование информационно-коммуникационных технологий для совершения преступлений, связанных с транснациональной организованной преступностью». При этом под ТОП следует понимать те преступления, которые считаются таковыми в соответствии со ст. 3 Конвенции ООН против ТОП 2000 г.

Продолжая анализ проекта, отметим дискуссионность содержания ст. 26: «Использование ИКТ для совершения деяний, признанных преступлениями в соответствии с международным правом:

Каждое государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству использования ИКТ с целью совершения какого-либо деяния, представляющего собой преступление, охватываемого каким-либо международным договором из перечисленных в Приложении к настоящей Конвенции…».

Следует отметить, что представленные в Приложении к российскому проекту всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях международные договоры можно объединить в две группы:

1. Антинаркотические и антипсихотропные соглашения (Единая конвенция о наркотических средствах (Нью-Йорк, 30 марта 1961 г.), Конвенция о психотропных веществах (Вена, 21 февраля 1971 г.) и др.

2. Антитеррористические соглашения (Международная конвенция о борьбе с бомбовым терроризмом (Нью-Йорк, 15 декабря 1997 г.), Конвенция о борьбе с финансированием терроризма (Нью-Йорк, 9 декабря 1999 г.), Международная конвенция о борьбе с актами ядерного терроризма (Нью-Йорк, 13 апреля 2005 г.) и др.

Вместе с тем, в проекте, представленном нашей стороной, имеются самостоятельные статьи по наркотическим и психотропным веществам (ст. 22) и по террористической деятельности (ст. 20). Из всех 16 антитеррористических соглашений, принятых под эгидой ООН[1], в Приложении отражены только восемь.

В этой связи предлагаем расширить в Приложении к проекту перечень универсальных антитеррористических договоров с учетом отражения всех принятых к настоящему времени соглашений. В ином случае в проекте будет содержаться ограниченное количество проявлений террористических угроз, что приведет к формированию неполноценных основ международного сотрудничества в деле борьбы с терроризмом с использованием ИКТ.

Кроме того, предлагаем гармонизировать содержание ст.ст. 20 и 26 в части противодействия террористической деятельности. Так, например, в ст. 20 «Преступления, связанные с террористической деятельностью» отмечено: «…каждое госу-

[1] Терроризм. Конвенции и соглашения // Официальный сайт ООН. URL: https://www.un.org/ru/documents/decl_conv/conv_terrorism.shtml.

дарство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству совершенные с использованием ИКТ… сбор или предоставления средств для целей его финансирования». Вместе с тем в ст. 26 «Использование ИКТ для совершения деяний, признанных преступлениями в соответствии с международным правом» закреплено, что государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству использования ИКТ с целью совершения какого-либо деяния, представляющего собой преступление, охватываемое каким-либо международным договором из перечисленных в Приложении к настоящей Конвенции. Одним из таких преступлений является финансирование терроризма согласно Международной конвенции о борьбе с финансированием терроризма 1999 г. Указанные примеры наглядно отражают некоторую коллизию в правовой регламентации отдельных составов преступлений, связанных с незаконным использованием ИКТ в преступных целях.

Детализация вопроса по положениям о криминализации в рамках проекта конвенции была проведена на второй сессии Спецкомитета[1].

Спецкомитет рассматривал письменные представления государств-членов, изложенные в форме конкретных предложений по формулировкам или общих замечаний к положениям о криминализации с учетом глав, включенных в структуру конвенции, утвержденную на первой сессии[2].

---

[1] Она проходила с 30 мая по 10 июня 2022 г. в Вене.

[2] Подборка представленных государствами-членами предложений и материалов, касающихся положений о криминализации, общих положений и положений о процессуальных мерах и правоохранительной деятельности всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (A/AC.291/9) // Официальный сайт Генеральной Ассамблеи ООН. URL: https://documents-ddsny.un.org/doc/UNDOC/GEN/V22/023/25/PDF/V2202325.pdf?OpenElement.

Справедлива позиция делегации Австралии, отмечающей в рамках работы второй сессии Спецкомитета, что «…новая конвенция дает возможность улучшить международное сотрудничество в отношении киберпреступности и, вместе с тем, обеспечить согласованность с существующими международными конвенциями по борьбе с преступностью и другими соответствующими документами и избежать их ненужного дублирования… новая конвенция даст возможность повысить уровень глобальной согласованности подходов к преступлениям, совершаемым в киберпространстве. Это, в свою очередь, позволит уменьшить количество «убежищ» для киберпреступников и расширит возможности правоохранительных органов в борьбе с киберпреступной деятельностью в сети Интернет».

В ходе сессии Спецкомитета была выражена широкая поддержка включению в конвенцию положений, направленных на борьбу с киберпреступностью, в частности, киберзависимых преступлений и ограниченного круга преступлений с использованием кибертехнологий, причем возражений против включения этих положений выдвинуто не было.

Здесь следует отметить позицию делегации Анголы, подчеркивающую важность не только криминализации, но и типологизации (выделении групп, типов преступлений) преступлений в будущей конвенции.

Данный аспект особенно важен с учетом того, что в российском проекте всеобъемлющей конвенции представлен обширный перечень составов, подпадающих под категорию «использование ИКТ в преступных целях».

Все государства сошлись во мнении относительно следующих составов:

– незаконный доступ (Египет – неправомерный доступ и/или превышение права на доступ)[1];

[1] В скобках приведены формулировки делегаций отдельных государств относительно названий анализируемых статей.

– незаконный перехват информации (Бурунди – деяния, направленные против конфиденциальности компьютерных систем);

– незаконное воздействие на данные (Южная Африка, Россия, Беларусь, Бурунди, Китай, Никарагуа, Таджикистан: несанкционированное воздействие на цифровую информацию; Венесуэла: неправомерное манипулирование цифровой информацией посредством ее повреждения, удаления, изменения, блокирования или модификации; Танзания: незаконное уничтожение электронных данных и компьютерных систем);

– незаконное воздействие на компьютерные системы – (Ангола: компьютерный саботаж, Россия, а также от имени Беларуси, Бурунди, Китая, Никарагуа, Таджикистана: нарушение функционирования информационно-коммуникационных сетей; Южная Африка – воздействие на систему и нарушение функционирования информационно-коммуникационных сетей; Венесуэла – преднамеренные неправомерные деяния, преследующие цель нарушить функционирование информационно-коммуникационных сетей и влекущие или порождающие риск серьезных последствий; Новая Зеландия – воздействие на функционирование компьютера);

– неправомерное использование устройств (Россия – незаконный оборот устройств).

К сожалению, на этих составах консенсус государств завершается. Отметим, что данные составы нашли свое закрепление в Будапештской конвенции 2001 г. в подразд. 1 «Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем».

Кроме того, отметим, что ряд государств в своих предложениях уходят от терминологии «ИКТ», используя в качестве предмета посягательства «компьютер, компьютерные данные, компьютерную информацию». Такой подход не согласуется с положениями резолюций Генассамблеи ООН 74/247 и 75/282

относительно всеобъемлющего характера будущей конвенции, положения которой должны иметь юрисдикцию для более широкой сферы ИКТ.

В отношении группы «преступлений, совершаемых посредством кибертехнологий» позиции государств следующие: к таковым деяниям следует относить только те преступления, масштабы, скорость и последствия которых возросли в результате использования компьютерных систем. Такой подход выразили делегации Австралии, Ганы, Японии, Великобритании, стран Евросоюза.

Государства достигли относительного консенсуса в отношении следующих преступных деяний в данной категории[1]:

– мошенничество / с использованием компьютерных технологий (Ангола – мошенничество в сети Интернет; Австралия – мошенничество и кражи, совершаемые посредством кибертехнологий, включая вымогательство посредством вредоносных программ-вымогателей; Бурунди – под данный тип преступлений определен самостоятельный разд. 6, включающий в себя фишинг, кражу цифровых персональных данных, рассылку спама и др.; Россия – хищение с использованием ИКТ; Иордания – электронное мошенничество, мошенничество с IP-адресами);

– подлог с использованием кибертехнологий (Египет – фальсификация; Иордания – создание веб-сайта, похожего на реальный сайт, для введения в заблуждение или обмана пользователей);

– преступления, связанные с авторским правами и смежными правами (США поддержали включение данного состава).

Абсолютный консенсус в данной группе преступлений достигнут в отношении посягательств на детей, а именно криминализации преступлений, связанных с сексуальными посягательствами на детей в сети Интернет.

[1] Указанные составы нашли закрепление в Будапештской конвенции 2001 г.

В отдельных предложениях присутствуют краткие формулировки по криминализации составов: «детская порнография» (Бразилия, Бурунди, Танзания), «сексуальная эксплуатация детей» (Канада, Мексика, Новая Зеландия).

Предложения Российской Федерации изначально затрагивают преступления, связанные с изготовлением и оборотом материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием информационно-коммуникационных технологий, но могут быть рассмотрены и иные, более актуальные формулировки статей по данной проблематике.

В Будапештской конвенции составы преступлений против интересов детей сосредоточены в подразд. 3 «Правонарушения, связанные с содержанием данных», а именно в ст. 9 «Правонарушения, связанные с детской порнографией».

Оригинальны отдельные предложения по криминализации преступлений против интересов детей: «завлечение и соблазнение ребенка» (Канада), «киберпреследование ребенка» (Гана).

Представляет интерес позиция Египта, в предложениях которого в отношении несовершеннолетних предусмотрен только один состав – «вовлечение несовершеннолетних в совершение противоправных деяний», при этом порнография и другие преступления, связанные с порнографией, идут отдельными составами без привязки к возвратному статусу жертвы.

Вместе с тем отметим, что рассмотренные базовые составы киберзависимых преступлений; преступлений, совершаемых посредством кибертехнологий, а также посягающих на права детей, одобренные государствами для включения в будущую всеобъемлющую конвенцию, в той или иной формулировке закреплены в Будапештской конвенции 2001 г.

Однако разрабатываемая всеобъемлющая конвенция не должна сводиться к дублированию положений данного договора, хотя при ее разработке следует учитывать лучшие практики

и положительный опыт международно-правового регулирования противодействия киберпреступности на региональном уровне.

Как справедливо отметила делегация Японии в рамках второй сессии Спекомитета, «…важно сделать готовящуюся конвенцию применимой в долгосрочной перспективе», что определяет необходимость выработки более широкого подхода государств к наполнению составов в части криминализации положений.

Актуальной темой в свете задач, стоящих перед будущей всеобъемлющей конвенцией, явилась криминализация следующих прогрессивных и специальных составов, поддержанных лишь отдельными государствами:

– создание, использование и распространение вредоносных программ (Австралия, Россия, Иордания, Венесуэла, Вьетнам; Япония – с некоторой корректировкой формулировки: атаки с использованием вирусов-вымогателей);

– посягательства на объекты критической инфраструктуры: атаки на компьютерные системы критической инфраструктуры (Япония); незаконный доступ к критической инфраструктуре (Гана, Египет); неправомерный доступ к критической инфраструктуре (Иордания); неправомерное воздействие на критическую информационную структуру (Россия); умышленное преднамеренное создание, распространение и/или использование компьютерных программ или другой цифровой информации в целях незаконного манипулирования критической информационной структурой (Венесуэла);

– посягательства на персональные данные (Ангола, Бразилия, Колумбия, Россия, Танзания, Венесуэла, Вьетнам);

– склонение к самоубийству или доведение до его совершения (Ангола, Бразилия, Египет, Россия);

– распространение интимных изображений без согласия (Ангола, Канада, Гана, Новая Зеландия);

– вовлечение детей в совершение противоправных действий, опасных для жизни и здоровья (Венесуэла, Россия, Египет).

Российской Федерации необходимо уделить должное внимание лоббированию вопроса по криминализации данных положений в тексте будущей конвенции.

Вызывает достаточно много дискуссий и вопрос о том, какие из наиболее сложных транснациональных преступлений, совершаемых посредством ИКТ, должны быть криминализированы в будущей конвенции.

На рассмотрение вынесены следующие составы:

– осуществление террористической деятельности – Ангола, Бурунди, Египет, Иордания, Россия, Венесуэла, Вьетнам;

– незаконный оборот наркотических средств и психотропных веществ – Бурунди, Иордания, Россия, Южная Африка, Венесуэла;

– распространение материалов расистского или ксенофобского характера – Бурунди, Россия, Танзания;

– торговля людьми – Белоруссия, Бурунди;

– незаконный оборот оружия – Бурунди, Россия, Венесуэла;

– финансовые преступления – Ангола, Египет, Сальвадор, Иордания.

Ряд государств поддерживают криминализацию положения в части осуществления террористической деятельности посредством систем ИКТ. Данный состав нуждается в однозначной криминализации по нескольким причинам.

Во-первых, в настоящее время насчитывается 19 универсальных соглашений по борьбе с терроризмом и его различными проявлениями. Такие международные документы наряду с рядом важных резолюций Совета Безопасности ООН, относящихся к терроризму, например, 1267 (1999), 1373 (2001) и 1540 (2004), составляют так называемый универсальный правовой режим борьбы с терроризмом[1].

[1] Эти документы работают в тандеме с другими соответствующими правовыми обязательствами государств, в частности в области международного права в области прав человека.

С принятием резолюции Совета Безопасности 1373 (2001), призывающей государства присоединиться к этим документам, процент их ратификации заметно увеличился. На сегодняшний день нет ни одного государства – члена ООН, которое не подписало бы или не присоединилось по меньшей мере к одному универсальному документу антитеррористического направления.

Каждый из 19 универсальных правовых документов был разработан под эгидой ООН и ее специализированных учреждений, в частности ИКАО, ИМО, МАГАТЭ, и открыт для присоединения всех государств – членов ООН. Соглашения основаны на осуждении международного терроризма, который создает угрозу для международной безопасности и мира.

Современные тенденции использования сферы ИКТ международными террористическими организациями и лицами, причастными к террористической деятельности, также вызывают серьезную озабоченность государств и определяют настоятельную необходимость в выработке единых подходов к противодействию таким угрозам. Ввиду отсутствия в ближайшей перспективе правовых и договорных инициатив по разработке соглашения о борьбе с кибертерроризмом, включая затяжной характер переговорного процесса по принятию Всеобъемлющей конвенции по борьбе с терроризмом[1], государствам следует учесть предоставленную возможность по включению в разрабатываемый проект всеобъемлющей конвенции о противодействии использованию информационно-коммуникационных тех-

[1] Несмотря на достигнутый прогресс в переговорах и подготовке текста, по-прежнему сохраняется ряд серьезных препятствий, которые необходимо преодолеть, чтобы проект всеобъемлющей конвенции был принят в качестве текста договора. Одним из препятствий по-прежнему является определение терроризма и террористических преступлений, в частности в отношении самоопределения. Еще одним камнем преткновения стала попытка достичь договоренности относительно сферы применения конвенции в отношении действий вооруженных сил государства во время столкновений с негосударственными акторами, участвующими в вооруженной борьбе за самоопределение.

нологий в преступных целях положений по криминализации использования ИКТ для совершения преступлений, связанных с террористической деятельностью.

Во-вторых, рассматриваемые универсальные договоры по борьбе с терроризмом несут в себе всеобъемлющую цель по обеспечению сотрудников органов уголовного правосудия эффективными механизмами для предотвращения и наказания террористических актов.

В действующих международных антитеррористических актах, к сожалению, отсутствуют ссылки, установки на сферу ИКТ как нового пространства для осуществления террористической деятельности, что нивелирует правовые основания и межгосударственные возможности для раскрытия, расследования таких «киберпреступлений» и реализации института ответственности за их совершение.

Следует помнить усложняющиеся тенденции, в которых ИКТ могут использоваться для способствования совершению преступлений, связанных с терроризмом. Так, ИКТ могут использоваться для поощрения, поддержки террористических актов, содействия в их совершении и/или участия в них. В частности, Интернет может использоваться для таких целей террористической деятельности, как распространение пропаганды (включая вербовку, радикализацию и подстрекательство к терроризму); финансирование [терроризма]; подготовка [террористов]; планирование [террористических атак] (в том числе с использованием засекреченных каналов связи и информации

из открытых источников); исполнение [террористических актов]; и кибератаки[1].

Указанные тенденции, а также глобальные задачи по скорейшему урегулированию сотрудничества государств по противодействию использованию ИКТ в целях совершения террористических преступлений определяют необходимость обсуждения и консенсуального решения государств в отношении криминализации в проекте всеобъемлющей конвенции состава, связанного с террористической деятельностью.

В-третьих, необходимость активизации сотрудничества государств по криминализации преступлений, связанных с террористической деятельностью посредством ИКТ, обусловлена позицией Совета Безопасности ООН к данной угрозе, отражаемой в принимаемых резолюциях. Совет Безопасности ООН отмечает «…озабоченность по поводу того, что в глобализированном обществе террористы и их сторонники все шире

[1] Исламское государство регулярно использует социальные сети, особенно Twitter, для распространения своих сообщений. Данная организация использует зашифрованную службу обмена сообщениями Telegram для распространения изображений, видео и обновлений. В 2014 г. более 30 тыс. аккаунтов Twitter находились под контролем «Исламского государства». Группировка известна тем, что снимает видеоролики и фотографии, загружая подобные материалы в Интернет – казни заключенных методом обезглавливания, выстрелом в голову, помещением в клетку и т. п. Журналист Абдель Бари Атван описал медиаконтент ИГИЛ как часть «систематически применяемой политики». Что касается «Аль-Каиды» в Ираке, то следует заметить, что эта организация регулярно выпускает короткие видеоролики, прославляющие деятельность джихадистов-смертников. Данные видеоролики включают тренировочные клипы боевиков, кадры жертв, отзывы о террористах-смертниках.

Террористические группировки ведут информационно-пропагандистскую деятельность среди большого количества людей в таких социальных чатах, как Viber и WhatsApp, социальных сетях Facebook, Twitter, Instagram (запрещены в России: принадлежат корпорации Meta, которая признана в России экстремистской) и др. Важной целевой аудиторией террористических организаций в Интернете, помимо иностранных террористов-боевиков, являются жертвователи. См.: Абазов К. М. Проблема использования современных информационно-коммуникационных технологий международными террористическими организациями // Вопросы безопасности. 2018. № 3. С. 1–9.

используют новые информационно-коммуникационные технологии, в частности Интернет, для содействия террористическим актам, а также по поводу того, что такие технологии используются в целях подстрекательства, вербовки, финансирования или планирования террористических актов»[1]; подчеркивает необходимость проведения «…совместных действий государств-членов по предотвращению и пресечению использования ИКТ, включая Интернет, в террористических целях, таких как вербовка и подстрекательство к совершению террористических актов, а также финансирование, планирование и подготовка их деятельности»[2], «…чтобы государства-члены действовали в духе сотрудничества при принятии мер, призванных воспрепятствовать использованию террористами ИКТ, и продолжали добровольное сотрудничество с частным сектором и гражданским обществом в деле разработки и осуществления более эффективных мер по борьбе с использованием Интернета в террористических целях»[3].

Анализ ряда резолюций Совета Безопасности ООН позволяет прийти к выводу о важности многостороннего сотрудничества в борьбе с неправомерным использованием террористами ИКТ, в частности Интернета и новых цифровых технологий, в целях вербовки для совершения, подстрекательства к совершению, финансирования или планирования террористических актов[4].

---

[1] Резолюция Совета Безопасности ООН S/RES/2610(2021) от 17 декабря 2022 г. «Угрозы международному миру и безопасности, вызванные террористическими атаками» // Официальный сайт ООН. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/408/00/PDF/-N2140800.pdf?OpenElement.

[2] Резолюция Совета Безопасности ООН S/RES/2617(2021) от 30 декабря 2021 г. «Угрозы международному миру и безопасности, вызванные террористическими атаками» // Официальный сайт ООН. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/424/11/PDF/N2142411.pdf?OpenElement.

[3] Там же.

[4] Кибербезопасность // Официальный сайт Совета Безопасности ООН. URL: https://www.un.org/counterterrorism/ru/cybersecurity.

На данную проблему особое внимание обращается в обзорах Глобальной контртеррористической стратегии Организации Объединенных Наций: «…рекомендует государствам-членам изыскивать более эффективные пути сотрудничества в целях обмена информацией, оказания взаимной помощи и привлечения к ответственности лиц, использующих информационно-коммуникационные технологии для террористических целей, и принимать другие надлежащие совместные меры по устранению таких угроз»[1].

В этой связи предложения Российской Федерации в части включения в проект всеобъемлющей конвенции статьи «Преступления, связанные с террористической деятельностью» соответствуют объективным потребностям в совместных усилиях государств по борьбе с неправомерным использованием ИКТ. Разрабатываемый проект всеобъемлющей конвенции позволит государствам реализовать свои обязательства в данной сфере посредством закрепления уголовно-правовых норм в потенциальном универсальном договоре в данной сфере.

Данный аспект особенно важен с учетом следующих установок: террористические акты рассматриваются Советом Безопасности как угроза международному миру и безопасности, по большей части эти деяния не попадают в категорию «тяжких международных преступлений», таких как геноцид, военные преступления и преступления против человечества. При этом террористическая деятельность относится к категории деяний, являющихся предметом серьезной обеспокоенности международного сообщества. Это обусловлено, как правило, транснациональным характером терроризма, когда террористические акты и связанные с ними угрозы и последствия редко

[1] Доклад Генерального секретаря ООН «Деятельность системы Организации Объединенных Наций по осуществлению Глобальной контртеррористической стратегии Организации Объединенных Наций» от 12 апреля 2016 г. A/70/826 // Официальный сайт ООН. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/102/52/PDF/N1610252.pdf?OpenElement.

ограничиваются одной внутренней юрисдикцией и в целом носят трансграничный характер.

Немаловажным представляется достижение консенсуса по вопросу криминализации использования сферы ИКТ для совершения противоправных действий, связанных с экстремизмом. Весьма удивительно отсутствие поддержки данной инициативы Российской Федерации, представленной в проекте всеобъемлющей конвенции, со стороны европейских государств, учитывая принятый в 2003 г. Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем ETS № 189 (Страсбург, 28 января 2003 г.).

Вопросы, связанные с предупреждением и противодействием экстремизму, особенно в его насильственных формах, на протяжении длительного времени занимают особое место в международной повестке дня, особенно после террористических атак 11 сентября 2001 г., свидетельством чего является участие в решении этих задач многих учреждений ООН и других организаций.

Формирование международного подхода по противодействию экстремизму под эгидой ООН прошло несколько этапов. Первый этап (2001–2014) характеризуется поверхностным вниманием международного сообщества к проблематике экстремизма, которая в тот период рассматривалась преимущественно в контексте контртеррористической деятельности. Соответственно сформулированные принципы и определения в рамках развития контртеррористического подхода ООН по умолчанию распространялись на антиэкстремистскую деятельность. Однако развитие деструктивных международных процессов в первое десятилетие XXI в. потребовало пересмотра подходов международного сообщества к обеспечению международной безопасности, особенно в части противодействия новым угрозам.

В 2014 г. начался новый этап в развитии международного подхода противодействия экстремизму: в рамках контртеррористической деятельности ООН отдельное внимание получают вопросы противодействия распространению воинствующего экстремизма. В 2014–2016 гг. тема противодействия экстремистской деятельности включается в повестку заседаний Совета Безопасности ООН и Генеральной Ассамблеи ООН. В этот же период инициирован процесс разработки нормативно-правового обеспечения предупреждения экстремизма в рамках ООН. Однако необходимо отметить, что все принимаемые нормативные положения по борьбе с экстремизмом носят характер «мягкого права»[1]. Императивных норм по данной проблематике под эгидой ООН заключить пока не удалось, как, впрочем, и под эгидой региональных международных организаций[2] (пожалуй,

[1] Например, План действий по предупреждению воинствующего экстремизма. Резолюция Генеральной Ассамблеи ООН A/70/674 от 24 декабря 2015 г.

[2] В рамках межамериканского региона функционирует Организация американских государств (ОАГ), которая, несмотря на наличие угроз со стороны терроризма и экстремизма в регионе, принимает незначительные прямые меры по предупреждению и противодействию насильственному экстремизму на уровне периодических резолюций или инструментов, принятых Генеральной Ассамблеей ОАГ. Европейский регион и прилегающие к нему государства также столкнулись с последствиями, связанными с насильственной экстремистской деятельностью. В рамках деятельности ОБСЕ, куда входят страны, находящиеся за пределами Европейского региона, усилия основываются на подходе «Противодействие насильственному экстремизму и радикализации, ведущей к терроризму» (НЭРВТ) и связаны с Консолидированной концептуальной базой ОБСЕ для борьбы с терроризмом, принятой в декабре 2012 (Постоянный совет ОБСЕ, 2012). Аналогичным образом Европейский союз принимает активное участие в усилиях по вопросам, связанным с ПВЭ и НВЭ, в особенности после принятия Стратегии предупреждения радикализации и вербовки, впервые утвержденной в 2005 г. (Европейский союз, Европейский Совет, 2005) и периодически обновляемой. Концепция «предупреждения» составляет одно из четырех направлений, лежащих в основе Стратегии ЕС по борьбе с терроризмом (Европейский союз, Европейский Совет, 2005). В этой связи предотвращение форм радикализации является неотъемлемым элементом региональной контртеррористической деятельности ЕС, что также отражено в Повестке дня Европы в области безопасности 2015 г. (Европейский союз, Европейский Совет, 2015). См. : Борьба с терроризмом. Модуль 2. Условия, способствующие распространению терроризма. Нью-Йорк : УНП ООН, 2019. С. 28–29, 35.

кроме ШОС, в рамках которой была принята Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом от 14 июня 2001 г.).

В четвертом обзоре Контртеррористической стратегии ООН от 2014 г. подчеркнуто, что тенденцией последних лет становится радикализация настроений, обусловленная повышенной активностью экстремистских групп на многочисленных веб-сайтах и страницах социальных сетей. Распространение экстремистского контента через Интернет способствует: во-первых, прославлению терроризма и пропаганде его в качестве одной из тактик политической борьбы; во-вторых, созданию для террористов базы поддержки вне непосредственной зоны их операций[1].

В пятом обзоре от 2016 г. отмечено следующее: «Роль средств массовой информации и использование социальных сетей террористическими и насильственными экстремистскими группами обрели новое качество и, таким образом, представляют собой все более важный аспект, требующий принятия соответствующих мер. Даже сорванные заговоры привлекают внимание средств массовой информации, что служит цели исполнителей – посеять страх и вызвать соответствующую реакцию. Это свидетельствует о том, что средства массовой информации могут вселять в террористические группы еще большую уверенность и способствовать привлечению новых бойцов. Прогресс в развитии коммуникационных технологий, особенно Интернета, способствовал более широкому распространению идей и повлиял на системы вербовки»[2].

---

[1] Доклад Генерального секретаря ООН «Деятельность системы Организации Объединенных Наций по осуществлению Глобальной контртеррористической стратегии Организации Объединенных Наций» от 14 апреля 2014 г. (A/68/841) // Официальный сайт ООН. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/299/31/PDF/N1429931.pdf?OpenElement.

[2] Доклад Генерального секретаря ООН «Деятельность системы Организации Объединенных Наций по осуществлению Глобальной контртеррористической стратегии Организации Объединенных Наций» от 12 апреля 2016 г. A/70/826 // Официальный сайт ООН. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/102/52/PDF/N1610252.pdf?OpenElement.

Также необходимо отметить, что предупреждение и противодействие насильственному экстремизму являются первоочередной задачей в повестке дня другого главного органа ООН – Совета Безопасности в связи с угрозами, которые насильственный экстремизм и терроризм представляют международному миру и безопасности[1]. Кроме того, Совет Безопасности уделяет внимание укреплению международных усилий для устранения растущих масштабов нетерпимости, которая наряду с экстремизмом служит мотивом подстрекательства к террористическим актам.

Таким образом, позиция ООН по вопросу противодействия экстремизму и связанным с ним преступлениям направлена на формирование и расширение сотрудничества государств на международном, региональном, субрегиональном и двустороннем уровнях. Особую озабоченность вызывает стремительная динамика использования ИКТ для распространения материалов, содержащих призывы к совершению противоправных деяний по мотивам политической, идеологической, социальной, расовой, национальной или религиозной ненависти и вражды.

Вместе с тем, как было отмечено, международное взаимодействие в данной области, несмотря на значимость и масштабность угроз, выстраивается на основе норм soft law. В связи с этим ввиду отсутствия императивных универсальных норм и заключенных договоров по проблематике борьбы с экстремизмом предложения Российской Федерации по включению в проект всеобъемлющей конвенции положений, криминализирующих преступления, связанные с экстремистской деятельностью,

[1] Например, резолюции Совета Безопасности ООН S/RES/2617(2021) от 30 декабря 2021 г. «Угрозы международному миру и безопасности, вызванные террористическими атаками»; S/RES/2615(2021) от 22 декабря 2021 г. «Угрозы международному миру и безопасности, вызванные террористическими атаками»; S/RES/2501(2019) от 16 декабря 2019 г. «Угрозы международному миру и безопасности, вызванные террористическими атаками» и др. // Официальный сайт ООН. URL: https://www.un.org/securitycouncil/ru/content/resolutions\.

являются своевременными и как никогда актуальными, поскольку позволят обеспечить единый подход государств к реализации института уголовной ответственности за реализацию экстремизма в самой популярной для преступных сообществ сфере ИКТ.

Поддержка криминализации положений о преступлениях, связанных с незаконным оборотом оружия посредством ИКТ является значимым предложением со стороны Российской Федерации и ее партнеров. Независимо от того, используется ли огнестрельное оружие как орудие совершения насильственных преступлений, инструмент для демонстрации или удержания власти, предмет незаконной торговли или альтернативный способ платежа, наличие связи между огнестрельным оружием и преступностью не подлежит никакому сомнению. Огнестрельное оружие является частью организованной преступности и часто служит для нее основанием. При этом речь может идти о самых разных действиях – от мобилизации деятельности и пособничества организованной преступности до терроризма и повстанчества.

Международная нормативная база по огнестрельному оружию содержит различные источники и инструменты, включая как юридически обязательное «жесткое» право, так и «мягкое» право или инструменты, не имеющие обязательной силы. Два первых глобальных инструмента, принятых в этой области, – это юридически обязательная Конвенция Организации Объединенных Наций против транснациональной организованной преступности 2000 г. и дополнительный к ней Протокол против незаконного изготовления и оборота огнестрельного оружия, его составных частей и компонентов, а также боеприпасов к нему (Протокол по огнестрельному оружию) 2001 г.

Вскоре за ними последовали Программа действий Организации Объединенных Наций по предотвращению и искоренению незаконной торговли стрелковым оружием и легкими вооружениями и борьбе с ней 2001 г. и Международный документ, поз-

воляющий государствам, своевременно и надежно, выявлять и отслеживать незаконное стрелковое оружие и легкое вооружение 2005 г., имеющие рекомендательный характер.

И наконец, новейший юридически обязывающий Договор о торговле оружием 2013 г., дополняющий предыдущие глобальные инструменты, был принят с целью продолжения международных усилий в деле укрепления мира, безопасности и стабильности посредством предотвращения незаконного оборота и противодействия ему. Вместе эти глобальные инструменты представляют собой общую программу действий.

На региональном уровне они дополняются отдельными региональными инструментами и соглашениями, большинство из которых носят юридически обязательный характер[1], усиливающие действие глобальных инструментов, а также, в некотором роде, раскрывающие их смысл.

Помимо международных соглашений существуют иные механизмы и инструменты, например резолюции Совета Безопасности ООН, Генеральной Ассамблеи ООН или других межправительственных и руководящих органов (конференция сторон Конвенции против транснациональной организованной преступности и Протокола по огнестрельному оружию)[2].

Несмотря на то, что проблемы, связанные с преступностью и огнестрельным оружием, носят настолько сложный характер, что для их решения требуются целенаправленные меры, включающие соответствующие меры уголовного правосудия с точки зрения предотвращения, расследования и судебного преследо-

---

[1] Например, Межамериканская конвенция о борьбе с незаконным изготовлением и оборотом огнестрельного оружия, боеприпасов, взрывчатых веществ и других связанных с ними материалов 1997 г. ; Центральноафриканская конвенция о контроле над стрелковым оружием и легкими вооружениями, боеприпасами к ним, частями и компонентами, которые могут быть использованы для их изготовления, ремонта и сборки 2010 г., и др.

[2] Например, резолюции Совета Безопасности 2370 (2017) о предотвращении приобретения террористами оружия, 1373 (2001) об угрозах международному миру и безопасности, создаваемых террористическими актами, и др.

вания преступлений, к сожалению, ни в одном из рассмотренных международных соглашений нет привязки к ответственности за незаконный оборот оружия в сфере ИКТ. Вместе с тем эта сфера становится самой популярной площадкой для совершения данного вида преступлений.

Огнестрельное оружие рекламируется и продается в Клирнете (обычном Интернете) и в Даркнете. В Клирнете веб-сайты, чаты, дискуссионные форумы, платформы социальных сетей, онлайн-рынки и сайты классической рекламы используются для запроса, рекламы и продажи огнестрельного оружия. Огнестрельное оружие может рекламироваться и продаваться на сайтах Клирнета на законных основаниях или в нарушение существующих законов и условий обслуживания веб-сайтов.

Огнестрельное оружие рекламируется и продается и в Даркнете, преимущественно через крипторынки (сайты, похожие на сайты известных онлайн-торговых предприятий, где многие продавцы могут продавать свои товары и услуги) и сайты продавцов (где продавцы продают свои собственные товары или услуги). Техническая информация и другие данные, относящиеся к его разработке, сборке, приобретению и использованию огнестрельного оружия также сообщаются в Клирнете и Даркнете.

Нередко преступники наряду с продажей оружия оказывают комплекс криминальных услуг.

Учитывая позиции государств, высказанные в рамках второй сессии Спекомитета, что к «преступлениям, совершаемым посредством кибертехнологий» следует относить только те преступления, масштабы, скорость и последствия которых возросли в результате использования компьютерных систем, предложения Российской Федерации по криминализации преступлений, связанных с незаконным оборотом оружия в сфере ИКТ, следует принять как актуальные положения. В связи с массовым внедрением IT-технологий следует прогнозировать, что сетевой рынок

нелегального оружия будет расти, спрос будет огромным, при этом опасности для преступников сведены к минимуму.

Поэтому одной из наиболее важных задач является международное сотрудничество по противодействию незаконному обороту оружия, взрывчатых веществ и взрывных устройств в информационно-телекоммуникационной сети Интернет. Для этого следует формировать прочную договорную международную базу, основой которой могут стать положения всеобъемлющей конвенции.

Представляют повышенный интерес предложения Российской Федерации и государств-партнеров по криминализации незаконного распространения фальсифицированных лекарственных средств и медицинских изделий. Преступления, связанные с незаконным оборотом медицинской продукции, ставят под угрозу не только здоровье, но и жизни людей, в силу чего данный вид преступности характеризуется повышенной степенью общественной опасности. Появление сети Интернет обеспечило преступникам высокий уровень конфиденциальности, в связи с чем к началу XXI в. теневой фармацевтический рынок достиг глобальных масштабов и стал представлять угрозу для всего мирового сообщества.

Как отмечено на сайте Интерпола, «…растущий потребительский спрос, пандемия COVID-19 и широкое использование Интернета привели к тому, что реклама, продажа и поставка незаконных медицинских препаратов с несанкционированных и нерегулируемых веб-сайтов в последние годы стали растущей проблемой»[1].

[1] Pharmaceutical crime operations // INTERPOL. URL: https://www.interpol.int/Crimes/Illicit-goods/Pharmaceutical-crime-operations. В 2021 г. в результате операции «Пангея XIV» были изъяты незаконные медицинские изделия на общую сумму около 23 414 483 долл. США. Кроме того, были удалены 113 020 веб-сайтов, размещающих незаконную продукцию, что является самым высоким показателем с момента первой операции «Пангея» в 2008 г.

Торговля фальсифицированной медицинской продукцией осуществляется как офлайн, так и онлайн (через онлайн-торговые площадки, онлайн-аптеки, платформы электронной коммерции, социальные сети и другие платформы). Большинство интернет-аптек ведут бизнес незаконно и без соответствующих гарантий, в том числе не требуя действующего рецепта, работают без действующей лицензии (сертификата), не соблюдают национальные или международные правила в отношении аптек. Интернет-аптеки создают особые проблемы для следственных органов и органов судебного преследования, в том числе практические трудности при определении физического местонахождения.

В то же время необходимо отметить, что, несмотря на серьезность угрозы, на данном этапе в системе международного права по-прежнему отсутствует консолидированный универсальный международный договор в рассматриваемой области. Единственным международным соглашением в данной сфере является разработанный Советом Европы первый в истории международный договор, регулирующий совместную деятельность государств по борьбе с контрафактной медицинской продукцией и аналогичными преступлениями, представляющими угрозу общественному здоровью, – Конвенция Медикрим[1], в которой как преступления квалифицируются следующие деяния:

– производство поддельных медицинских изделий;

– поставка, предложение к поставке и оборот контрафактной медицинской продукции;

– подделка документов;

[1] Конвенция Совета Европы о борьбе с фальсификацией медицинской продукции и сходными преступлениями, угрожающими здоровью населения 2011 г. // Официальный сайт Совета Европы. URL: https://rm.coe.int/CoERM-Public-Common-Search-Services/Display-DCTMContent?documentId=0900001680-6a9503.

– несанкционированное производство или поставка лекарственных средств и реализация медицинских изделий, не соответствующих требованиям соответствия[1].

В отсутствие какой-либо правовой альтернативы Конвенция Медикрим является уникальным договором как с процессуально-правовой точки зрения (поскольку она закрепляет юридическое понятие фальсификации медицинских продуктов и сходных преступлений, которые раньше не являлись объектом международного уголовного права), так и с материально-правовой точки зрения (поскольку Конвенция Медикрим дает определение деяниям, причиняющим вред). Данный договор представляет собой существенный шаг на пути к установлению юрисдикции над преступными деяниями в сфере фармацевтики, квалифицируемыми в качестве уголовных в соответствии с нормами международного права, и привлечению преступников к уголовной ответственности.

Следует отметить, что согласно ст. 28 рассматриваемого соглашения: «Конвенция открыта для подписания государствами – членами Совета Европы, Европейским союзом и государствами, не являющимися членами Совета Европы, которые участвовали в разработке Конвенции или имеют статус наблюдателя при Совете Европы. Конвенция также открыта для подписания любым другим государством, не являющимся членом Совета Европы, по приглашению Комитета министров». На данный момент договор подписали 38 государств и ратифицировали 21 государство[2].

Вместе с тем даже открытый характер регионального международного соглашения Медикрим не позволит данному дого-

---

[1] Counterfeiting of medical products and similar crimes. MEDICRIME Convention // Council of Europe. URL: https://www.coe.int/en/web/medicrime/home.

[2] Council of Europe Convention on the counterfeiting of medical products and similar crimes involving threats to public health (CETS № 211). Status as of 16/07/2022 // Council of Europe. URL: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=211.

вору стать универсальным правовым регулятором в сфере сотрудничества государств по борьбе с фальсифицированной медицинской продукцией, а правовых аналогов под эгидой ООН в ближайшей перспективе разработано не будет.

Указанные обстоятельства актуализируют предложения Российской Федерации по включению в проект всеобъемлющей конвенции в качестве уголовно наказуемого деяния незаконное распространение фальсифицированных лекарственных средств и медицинских изделий посредством использования ИКТ. Благодаря включению данного положения в будущий универсальный договор государствам удастся закрепить на уровне ООН позиции по криминализации фармацевтической преступности в самой уязвимой сфере ИКТ, являющейся популярной для преступного мира, без необходимости разработки отдельного самостоятельного соглашения в данной области.

Рассматривая вопрос о том, какие наиболее важные виды транснациональной преступности подлежат криминализации во всеобъемлющей конвенции, следует отметить, что в отдельных предложениях государств присутствуют следующие варианты составов: экономические и финансовые преступления, совершаемые в сети Интернет (Ангола, Сальвадор); шантаж и публикация слухов, нанесение оскорбления с использованием компьютерной системы (Бурунди); завлечение и соблазнение ребенка (Канада); нарушение неприкосновенности частной жизни, подстрекательство к подрывной или вооруженной деятельности (Египет, Иордания); преступления, связанные с незаконным оборотом наркотиков, подстрекательство к подрывной или вооруженной деятельности и др. (Россия, Венесуэла); геноцид и преступления против человечности (Россия, Танзания); расширенный перечень преступных деяний (Вьетнам).

В отношении данного вопроса делегация Японии отмечает, что в новой конвенции следует предусмотреть основные и существенные положения, которые могли бы соблюдаться и при-

меняться как можно большим числом государств-членов. Поэтому необходимо избегать установления положений, ограничивающих число государств-членов, которые могут заключить новую конвенцию, ввиду различий в основных правовых концепциях, неизбежно существующих между государствами-членами[1]. Что касается преступлений, связанных с терроризмом; преступлений, связанных с огнестрельным оружием, и преступлений, связанных с наркотиками, то они могут представлять собой обычные преступления, даже если они совершены с использованием сети Интернет, и к ним также могут применяться существующие договоры, такие как Конвенция ООН против транснациональной организованной преступности.

Данная позиция, безусловно, дискуссионная, однако отдельные государства придерживаются аналогичной точки зрения (Норвегия, Европейский союз, Канада, США и др.).

Здесь важно помнить, что согласно резолюциям Генеральной Ассамблеи ООН 74/247 и 75/282 будущая конвенция должна носить всеобъемлющий характер, т. е. она должна по возможности охватывать все составы преступных деяний, совершаемых с использованием ИКТ.

Продолжая анализ положений о криминализации противоправных деяний в рамках всеобъемлющей Конвенции, отметим единый подход государств в отношении вопроса дополнительной ответственности за «покушение, пособничество и подстрекательство». Данное предложение было представлено от имени следующих делегаций: Бразилия, Сальвадор, Европейский союз

[1] Позиция Японии. Подборка представленных государствами-членами предложений и материалов, касающихся положений о криминализации, общих положений и положений о процессуальных мерах и правоохранительной деятельности всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (A/AC.291/9) // Официальный сайт Генеральной Ассамблеи ООН. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V22/023/25/PDF/V2202325.pdf?OpenElement.

и его государства-члены, Египет, Гана, Иордания, Новая Зеландия, Россия, Швейцария, Великобритания, Танзания, США.

Представляет интерес позиция Японии в отношении рассматриваемых составов: «…требование единого наказания за покушение на преступление или пособничество и подстрекательство к преступлению, или требование наказания на стадии подготовки или вступления в сговор, что недостаточно для признания состава покушения, было бы чрезмерным вмешательством во внутреннее уголовное законодательство отдельных государств». Криминализация этих правонарушений должна быть оставлена на усмотрение национального законодательства каждого государства-члена.

В заключение отметим абсолютное единство предложений государств в части криминализации ответственности юридических лиц в связи с преступлениями и иными противоправными деяниями, признанными в качестве таковых в соответствии с разрабатываемой конвенцией. Данное положение было апробировано ранее в рамках Будапештской конвенции 2001 г. (ст. 12 «Корпоративная ответственность»).

Вместе с тем вновь подчеркнем, что всеобъемлющая конвенция не должна сводиться к дублированию положений Будапештской конвенции 2001 г., поскольку Спецкомитет учрежден для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, в полной мере учитывая существующие международные документы и предпринимаемые на национальном, региональном и международном уровнях усилия по борьбе с использованием ИКТ в преступных целях.

Таким образом, государствам – участникам переговорного процесса по разработке всеобъемлющей конвенции необходимо избегать узкого подхода, блокирующего возможности разработки первого в истории универсального международного до-

говора по борьбе с киберпреступностью. Принятие такого договора крайне важно с учетом международно-правовой несогласованности современных подходов относительно регулирования сотрудничества государств в данной сфере под эгидой ООН, а также с учетом фрагментарности и разрозненности положений региональных источников.

4. Процессуальные меры и правоприменение

Положения о процессуальных мерах и правоприменении, содержащиеся в региональных соглашениях и российском проекте всеобъемлющей конвенции, приведены в *прил. 5* и *6*.

Следует отметить, что процессуальные действия, закрепленные в проекте конвенции (ст.ст. 31–38), полностью совпадают с апробированными механизмами, отраженными в Будапештской конвенции 2001 г. (ст.ст. 14–21). Большая часть этих мер также регламентирована нормами Конвенции Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий 2010 г.

Вместе с тем в проекте содержится одно положение, связанное со сбором информации, передаваемой с использованием ИКТ (ст. 33). Данная норма отсутствует в положениях Будапештской конвенции 2001 г., но содержится в тексте договора Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий 2010 г. (ст. 28).

Что касается правоприменения, то во всех указанных договорах и проекте конвенции содержится статья «Юрисдикция». Отметим, что ст. 39 проекта конвенции по своему содержанию близка к положениям ст. 15 Конвенции ООН против ТОП 2000 г. При этом в рассматриваемом проекте конвенции статья более актуализирована в части юрисдикции «в отношении преступлений, охватываемых настоящей Конвенцией, когда лицо, подозреваемое в совершении преступления, находится на его территории и оно не выдает такое лицо лишь на том основании, что оно является одним из его граждан». В проекте к данному по-

ложению добавлены также лица, которым государством предоставлен статус беженцев. И, пожалуй, самая важная новелла закреплена в ч. 4 ст. 39 проекта конвенции:

«4. Каждое государство-участник, на территории которого находится лицо, подозреваемое в совершении преступления и которое не выдает его, обязано, в случаях, предусмотренных в пунктах 1 и 2 настоящей статьи, без каких бы то ни было исключений и независимо от того, совершено ли оно на территории этого государства-участника, без излишних задержек передать дело своим компетентным органам для целей преследования путем проведения разбирательства в соответствии с законодательством этого государства».

Таким образом, необходимо отметить, что раздел международных договоров в сфере ИТ в части процессуальных вопросов и правоприменения является наиболее согласованным и проработанным.

5. Международное сотрудничество

Положения о международном сотрудничестве содержатся во всех рассматриваемых нами региональных договорах по киберпреступности. Эти документы, как правило, содержат общие широкие обязательства государств-членов и конкретные механизмы сотрудничества, в том числе традиционную выдачу, взаимную правовую помощь. Вместе с тем, следует отметить, что в анализируемых соглашениях по киберпреступности содержится ряд статей, закрепляющих инновационные формы сотрудничества государств, специфических для сферы ИТ и нетипичных для международного сотрудничества в борьбе с иными преступлениями. К данным формам, прежде всего, относятся: оперативное обеспечение сохранности и частичное раскрытие данных о потоках информации; сбор в режиме реального времени данных о потоках информации; взаимная правовая помощь в отношении информации, связанной с содержанием конкретных сообщений и др. *(прил. 7)*.

В реализации норм о международном сотрудничестве, закрепленных в анализируемых договорах по киберпреступности, имеются особенности. Несмотря на то, что эти соглашения могут обеспечить правовую основу для конкретных мероприятий по взаимодействию компетентных органов государств, следует помнить, что государства – участники данных соглашений также являются сторонами более широких многосторонних и двусторонних соглашений, касающихся сотрудничества по уголовным делам, в том числе таких соглашений, как Конвенция против ТОП 2000 г. В зависимости от характера расследуемого деяния потребности в сотрудничестве могут подпадать под действие ряда правовых механизмов. Так, например, Будапештская конвенция 2001 г. предусматривает, что стороны должны сотрудничать друг с другом не только «в соответствии с положениями настоящей главы», но и «путем применения соответствующих международных документов о международном сотрудничестве по уголовным делам, согласованных договоренностей, опирающихся на единообразное или основанное на взаимности законодательство, а также норм внутригосударственного права» (ст. 23). Аналогичная норма закреплена в ст. 46 «Общие принципы международного сотрудничества» российского проекта всеобъемлющей конвенции.

В рассматриваемых договорах вызывает вопросы положение, закрепляющее создание специализированных подразделений – контактных центров, работающих 24 часа в сутки 7 дней в проведении расследований, преследований или судебных разбирательств в связи с преступлениями, имеющими отношение к компьютерным системам и данным, или в сборе доказательств в электронно-цифровой форме в отношении преступлений. Такая помощь, как правило, может включать поддержку применения или, если это допускается внутренним правом или практикой, непосредственное применение следующих мер:

а) оказание технической консультативной помощи;

б) обеспечение сохранности данных в целях сбора доказательств и последующего предоставления информации в соответствии с его внутренним законодательством, а также действующими договорами о взаимной правовой помощи (ст. 66 российского проекта всеобъемлющей конвенции).

Данная норма содержится в Будапештской конвенции 2001 г. (ст. 35), Конвенции ЛАГ о борьбе с преступлениями в сфере информационных технологий 2010 г. (ст. 43).

К настоящему времени в рамках отдельных региональных механизмов уже создан и функционирует ряд сетей неформального сотрудничества в области киберпреступлений. Например, контактные центры 24/7 работают в рамках сотрудничества государств – участников Будапештской конвенции 2001 г. Несмотря на неоспоримые преимущества таких подразделений, многочисленное развитие таких сетей может поставить под угрозу идею «единого контактного центра» системы. Как отмечено во Всестороннем исследовании по киберпреступности ООН, из-за возможного наличия нескольких контактных центров в одном государстве другие страны могут не знать того, в какой центр в стране им необходимо обратиться. Это также может привести к задержке в предоставлении ответов на запросы, когда запрашиваемые страны должны проверить законность или личность координатора механизма, с которым они ранее не связывались[1].

Данный аспект необходимо учитывать при разработке технической и оперативной компоненты таких подразделений в государствах.

6. Техническая помощь и обмен опытом

Необходимо отметить, что нормы по оказанию технической помощи и обмена опытом особенно в интересах развивающихся

[1] Всестороннее исследование проблемы киберпреступности // УНП ООН. URL: https://www.unodc.org/documents/organised_crime/cybercrime/cybercrime_study_russian.pdf.

стран, в связи с их соответствующими планами и программами по борьбе с преступлениями в сфере ИКТ, включая подготовку кадров, а также оказание помощи и взаимный обмен соответствующим опытом и специальными знаниями нашли отражение только в проекте всеобъемлющей конвенции *(прил. 8)*. Раздел «Техническая помощь, обмен опытом» был определен как обязательный элемент структуры договора в рамках работы первой сессии Спецкомитета. В связи с этим следует подчеркнуть положительные тенденции по рассмотрению данного блока вопросов в проекте будущего универсального договора.

Так, важным направлением деятельности Интерпола по борьбе с преступлениями в сфере информационных технологий является обучение и подготовка профильных специализированных кадров. В 2019 г. Интерпол впервые за всю свою историю провел первый учебный курс полностью в режиме онлайн для полиции и судебных органов по тематике цифровых доказательств. В период пандемии в апреле 2020 г. была открыта Виртуальная академия с целями реализации возможности онлайн-обучения. Передовая платформа цифрового обучения предоставляет более 100 курсов для самостоятельного изучения, интерактивные модули и вебинары под руководством сертифицированных инструкторов для правоохранительных органов в 195 странах – членах Интерпола. Темы для изучения разнообразны и включают такие направления, как криптовалюты, дроны, цифровая криминалистика, киберпреступность, Даркнет, борьба с терроризмом, организованной преступностью в рамках Интерпола.

Интерпол оказывает содействие правоохранительным органам африканских государств и непосредственно Африполу в разработке и дальнейшей реализации инициативных стратегий, создает технические и оперативные условия для эффектив-

ного обмена информацией и повышения навыков по раскрытию и расследованию транснациональных преступлений[1].

Сотрудничество государств в рамках региональной полицейской организации Асеанапол по противодействию преступлениям в сфере информационных технологий также находится на стадии развития и осуществляется при поддержке Интерпола.

Таким образом, Интерпол в тесном сотрудничестве с экспертами и правоохранительными органами государств осуществляет координацию полицейского сотрудничества, поддерживает и развивает потенциал регионального сотрудничества в исследуемой области, а также содействует в подготовке полицейских кадров, специализирующихся на различных направлениях противодействия киберпреступлениями.

В российском проекте конвенции (глава V) предложен достаточно обширный комплекс мер по наращиванию потенциала и оказанию технической помощи государствам в этой области.

7. Профилактические меры

Одной из ключевых целей будущего всеобъемлющего договора является «предупреждение преступлений в сфере ИКТ». Для полноценного понимания способов и средств достижения данной цели в проект конвенции включен самостоятельный раздел «Меры по противодействию преступлениям и иным противоправным деяниям в информационном пространстве». Следует отметить, что нормы по предупреждению исследуемых преступлений нашли отражение только в проекте всеобъемлющей конвенции *(прил. 9)*. Раздел «Профилактические меры» был опреде-

[1] С 2017 г. реализуется проект «ENACT» – первый в своем роде проект, охватывающий весь Африканский континент. В Африке все чаще происходят инциденты с вредоносным программным обеспечением. Социальные сети используются для облегчения незаконного ввоза мигрантов, о чем свидетельствуют результаты международной операции «Саррауния». Установлено, что Африка также является растущим глобальным транзитным центром для оборота наркотиков и ряда других незаконных товаров, которые продаются и покупаются в интернет-пространстве.

лен как обязательный элемент структуры договора в рамках работы первой сессии Спецкомитета. В связи с этим следует подчеркнуть положительные тенденции по рассмотрению данного блока вопросов в проекте будущего универсального договора.

Необходимость развития государственно-частного партнерства по противодействию ИКТ-преступности обусловливается рядом причин, среди которых нехватка специализированных кадров в компетентных правоохранительных органах, владеющих необходимыми знаниями, умениями и навыками использования информационных технологий для эффективного осуществления профессиональной деятельности с учетом специфической среды совершения преступлений, а также недостаточная технологическая оснащенность сотрудников правоохранительных органов специальными средствами и программным обеспечением.

Изучение специфики деятельности частных партнеров позволило выявить перспективные направления развития государственно-частного взаимодействия в сфере информационных технологий: разработка программного обеспечения для выявления предупреждения и пресечения киберугроз; организация мероприятий по мониторингу информационных ресурсов; развитие аналитических технологий для обработки массивов информации; совершенствование правовых основ, регулирующих общественные отношения в сфере использования информационных технологий с привлечением частных партнеров.

Не менее актуальной тенденцией развития государственно-частного партнерства по противодействию преступлениям в сфере информационных технологий является привлечение частных партнеров к реализации задач правоохранительной деятельности: проведения компьютерных экспертиз, сбора цифровых доказательств, сотрудничества в области подготовки и переподготовки специализированных кадров по вопросам обеспечения информационной безопасности и противодействия преступлениям в сфере информационных технологий и др.

Ярким примером такого взаимодействия является многолетнее сотрудничество Интерпола с «Лабораторией Касперского», деятельность которой основана на глубоких экспертных знаниях и многолетнем опыте обеспечения информационной безопасности критической информационной инфраструктуры[1], государственных органов, бизнеса и рядовых пользователей.

30 сентября 2014 г. Интерпол подписал соглашение с «Лабораторией Касперского» о сотрудничестве в целях расширения масштабов взаимодействия специалистов информационной сферы и правоохранительных органов государств в их совместной борьбе с киберпреступностью. В рамках договора определено, что компания будет предоставлять аналитическую информацию о киберугрозах, а также оборудование и программное обеспечение для работы Центра киберкриминалистики Глобального комплекса инноваций в Сингапуре. Кроме того, «Лаборатория Касперского» взяла на себя обязательства по проведению серии тренингов для сотрудников Интерпола по анализу вредоносных программ, цифровой криминалистике и исследованию финансовых угроз[2].

В 2017 г. «Лаборатория Касперского» объявила о новом этапе сотрудничества с Интерполом, продлив и расширив соглашение о совместной работе. Цель этого сотрудничества – объединение усилий, знаний и экспертного опыта по противодействию преступлениям в сфере ИТ.

За длительный период сотрудничества «Лаборатория Касперского» и Интерпол реализовали ряд успешных совместных проектов. Компания принимает активное участие в организации

---

[1] Критическая инфраструктура – совокупность автоматизированных систем управления производственными и технологическими процессами критически важных объектов Российской Федерации и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, а также систем и сетей связи, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка.

[2] INTERPOL strengthens cooperation with Kaspersky Lab in global fight against cybercrime. 2014. News // Официальный сайт Интерпола. URL: https://-www.inter-pol.int/News-and-Events/-News/-2014/INTERPOL-strengthenscooperation-with-Kas-persky-Lab-in-global-fight-against-cybercrime.

международных операций, направленных на противодействие преступлениям в сфере ИТ. Так, в 2017 г. операция, проводимая под руководством Глобального комплекса инноваций Интерпола, направленная на борьбу с киберпреступностью в Азиатско-Тихоокеанском регионе, охватила следователей из Индонезии, Малайзии, Мьянмы, Филиппин, Сингапура, Таиланда, Вьетнама, а также экспертов «Лаборатории Касперского» и шести других компаний частного сектора. В ходе проведения операции было выявлено почти 9 тыс. серверов управления и контроля (C2) и сотни взломанных веб-сайтов, включая правительственные порталы, а также около 270 сайтов, зараженных вредоносным кодом, использующим уязвимости в приложении для разработки веб-сайтов. В ходе совместного расследования и совместной операции Интерпола и «Лаборатории Касперского» в феврале 2022 г. удалось предотвратить хищение средств из центрального банка одной из стран Латинской Америки[1].

Кроме того, благодаря экспертной поддержке «Лаборатории Касперского» Интерполу удалось обнаружить и вывести из строя ботнет Simda – сеть из более чем 770 тыс. зараженных компьютеров по всему миру[2]. Международная операция координирова-

---

[1] «Лаборатория Касперского» и Интерпол предотвратили киберограбление центрального банка в Латинской Америке // Официальный сайт «Лаборатории Касперского». URL: https://www.kaspersky.ru/about/press-releases/2022_-laboratoriya-kasperskogo-i-interpol-predotvratili-kiberograblenie-nacionalnogo-banka-v-latinskoj-amerike.

[2] Simda является зловредом, используемым для распространения незаконного программного обеспечения и различных видов вредоносных программ, включая те, что обладают возможностью похищать финансовые данные. Злоумышленники продают доступ к зараженным машинам другим киберпреступникам, которые затем устанавливают на них дополнительные программы. Simda распространяется через множество веб-сайтов, скомпрометированных злоумышленниками. Когда пользователь заходит на эти страницы, вредоносный код незаметно инициирует скачивание содержимого сайта и заражает компьютер. В общей сложности заражению подверглись 770 тыс. компьютеров в 190 странах мира, преимущественно в США, Великобритании, России, Канаде и Турции. См.: «Лаборатория Касперского» и Интерпол договорились о новом этапе совместной работы // Официальный сайт «Лаборатории Касперского». URL: https://www.kaspersky.ru/about/press-releases/2017_interpol-and-kaspersky-lab-strengthen-partnership.

лась Глобальным комплексом инноваций Интерпола[1] и имела масштабные результаты по удалению компьютерных киберугроз во многих государствах[2]. В данной операции эксперты «Лаборатории Касперского», откомандированные для работы в Интерпол, оказывали помощь в предоставлении технического анализа вредоносной программы Simda, сборе статистической информации с помощью Kaspersky Security Network и т. д.

Опыт взаимодействия Интерпола и «Лаборатории Касперского» подтверждает, что сотрудничество правоохранительных органов с частными компаниями стратегически важно, поскольку это помогает более успешно справляться с киберугрозами, масштаб и сложность которых растет с невероятной скоростью.

---

[1] INTERPOL coordinates global operation to take down Simda botnet // Официальный сайт Интерпола. URL: https://www.inter-pol.int/News-and-Events/-News/2015/INTERPOL-coordinates-global-operation-to-take-down-Simda-botnet.

[2] В рамках операции, координируемой Глобальным комплексом инноваций Интерпола в Сингапуре, группа ведущих IT-компаний, включая «Лабораторию Касперского», Microsoft и Trend Micro, в сотрудничестве с международными правоохранительными органами осуществили вывод из строя ботнета Simda – компьютерной сети, состоящей из сотен тысяч зараженных компьютеров по всему миру. В результате операции командные серверы, с помощью которых киберпреступники управляли зараженными машинами, были обезврежены. См.: «Лаборатория Касперского» объединяет усилия с Интерполом и коллегами по IT-безопасности для вывода из строя ботнета Simda // Официальный сайт «Лаборатории Касперского». URL: https://www.-kaspersky.ru/about/press-releases/2015_kaspersky-lab-with-interpol-botnet-simda.

ГЛАВА III
Направления развития и совершенствования сотрудничества по линии МВД России с партнерами Российской Федерации по вопросам противодействия угрозе использования информационно-коммуникационных технологий в преступных целях

§ 3.1. Правоохранительное сотрудничество в борьбе с преступлениями в сфере информационных технологий в рамках Содружества Независимых Государств

Свои национальные интересы, связанные с развитием международного сотрудничества по противодействию преступлениям в сфере ИКТ, Российская Федерация реализует на площадке ООН с учетом стратегических региональных приоритетов, определенных Концепцией внешней политики Российской Федерации[1]. В современных условиях развития мирового сообщества ключевым приоритетом России является развитие сотрудничества с государствами – участниками Содружества Независимых Государств и дальнейшее укрепление межгосударственного взаимодействия на пространстве СНГ.

Преступления, совершаемые с использованием информационных технологий, приобретают транснациональный характер и создают угрозу национальной безопасности государств –

[1] Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации 30 ноября 2016 г.) // Официальный сайт МИД России. URL: https://www.mid.ru/foreign_policy/official_documents//-asset_publisher/CptICkB6BZ29/ content/id/2542248.

участников СНГ. Кроме того, как отмечено в Концепции сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий 2013 г., происходит сращивание различных видов преступности, главным образом, за счет использования средств компьютерной техники и информационных сетей в качестве оперативных средств связи и телекоммуникаций, при этом субъекты, совершающие преступления с использованием информационных технологий, непрерывно совершенствуют средства и методы, применяемые в преступной деятельности[1].

В этой связи эффективная борьба с преступлениями, совершаемыми с использованием информационных технологий, может быть обеспечена на основе тесного взаимодействия правоохранительных органов государств – участников СНГ, а также с правоохранительными органами других государств.

Ключевым международным договором, определяющим правовые основы взаимодействия государств – участников СНГ в борьбе с преступностью в информационной сфере, является Соглашение о сотрудничестве в борьбе с преступлениями в сфере информационных технологий в рамках СНГ 2018 г. Его вступление в силу позволило создать современные правовые механизмы практического взаимодействия российских компетентных органов с коллегами из других стран СНГ для эффективного предупреждения, выявления, пресечения, расследования и раскрытия преступлений в сфере информационных технологий. Речь идет о возможном сотрудничестве в сфере обмена информацией о готовящихся или совершенных преступлениях и при-

[1] Концепция сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий. Одобрена Решением Совета глав государств Содружества Независимых Государств о Концепции сотрудничества государств – участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий от 25 октября 2013 г. // Антитеррористический центр государств – участников Содружества Независимых Государств. URL: https://www.cisatc.org/1289/135/152.

частных к ним лицах; исполнения запросов об оказании содействия в предоставлении сведений, которые могут помочь в расследовании, а также проведения скоординированных операций[1].

Российская Федерация ратифицировала данный договор в соответствии с Федеральным законом от 1 июля 2021 г. № 237-ФЗ «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий»[2], сделав определенные оговорки: «Российская Федерация оставляет за собой право признавать деяния, предусмотренные подпунктами «г»[3], «д»[4], «ж»[5] и «з»[6] п. 1 ст. 3 Соглашения, как в качестве уголовно наказуемых в соответствии с Уголовным кодексом Российской Федерации, так и в качестве администра-

---

[1] О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий 2018 г. // Официальный сайт Правительства Российской Федерации. URL: https://docs.cntd.ru/document/607124270.

[2] Федеральный закон от 1 июля 2021 г. № 237-ФЗ «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_388782/.

[3] Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации, либо сопряженное с несанкционированным доступом к охраняемой законом компьютерной информации.

[4] Распространение с использованием информационно-телекоммуникационной сети Интернет или иных каналов электрической связи порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего.

[5] Незаконное использование программ для компьютерных систем и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб.

[6] Распространение с использованием информационно-телекоммуникационной сети Интернет или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма.

тивно наказуемых в соответствии с Кодексом Российской Федерации об административных правонарушениях».

Сотрудничество государств – участников СНГ по противодействию преступлениям в исследуемой области реализуется, главным образом, в рамках деятельности Совета министров внутренних дел (далее – СМВД) и Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств – участников СНГ (далее – БКБОП).

25 октября 2013 г. решением Совета глав государств (далее – СГГ) утверждена Концепция сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием ИТ, в соответствии с которой СМВД совместно с БКБОП осуществляют работу по следующим основным направлениям:

– совершенствование правовых основ международного сотрудничества в области борьбы с преступлениями, совершаемыми с использованием ИТ;

– организация и проведение согласованных межведомственных профилактических, оперативно-разыскных мероприятий и специальных операций по противодействию преступлениям, совершаемым с использованием ИТ;

– создание совместных следственно-оперативных групп из представителей компетентных органов государств – участников СНГ в целях раскрытия преступлений транснационального характера, совершаемых с использованием ИТ;

– поддержание и развитие взаимодействия с международными организациями и центрами, занимающимися противодействием преступлениям, совершаемым с использованием ИТ;

– развитие сотрудничества в области разработки, производства, поставки и оказания помощи государств – участников СНГ по внедрению специальных программно-технических средств, необходимых для обнаружения, фиксации, изъятия

и исследования следов преступлений, совершаемых с использованием ИТ;

– обмен опытом и передовыми технологиями, разработка методических пособий и проведение научных исследований по вопросам борьбы с преступлениями в сфере ИТ;

– развитие и использование Объединенного банка данных органов безопасности и специальных служб государств – участников СНГ по борьбе с организованной преступностью и др.

Анализ задач, решаемых СМВД совместно с БКБОП по противодействию преступлениям в сфере информационных технологий, позволил сделать вывод о том, что они носят преимущественно технический, информационный и нормативный характер. Вместе с тем, в настоящее время с учетом роста угроз со стороны киберпреступности возникла необходимость перехода от координации и связанного с ней информационного обеспечения компетентных органов государств – участников СНГ к согласованному правоохранительному взаимодействию указанных государств.

В этой связи в качестве предложения видится возможным учредить узкопрофильную структуру по проблематике борьбы с преступлениями в сфере ИТ, которая позволит координировать совместное правоохранительное взаимодействие государств – участников СНГ в лице их компетентных органов – Центра по противодействию преступлениям в сфере информационных технологий СНГ.

Предложения по созданию такого подразделения уже обсуждались на площадке СНГ. Так, в одном из аналитических обзоров о состоянии преступности в сфере ИТ на пространствах СНГ, подготовленном Научно-консультативным советом при СМВД и БКБОП, была обозначена перспективная задача по созданию на межгосударственном уровне Центра ситуационного предупреждения киберпреступлений[1], в компетенцию которого

[1] Подразделение (рабочая группа), действующее на постоянной основе, возможно, в составе БКБОП.

предлагалось включить: моделирование ситуаций, угрожающих интересам обеспечения безопасности государств; выработку мер предупреждения преступлений в сфере ИТ, а также методов их выявления и пресечения; организацию комплексных совместных и (или) межведомственных профилактических, оперативно-разыскных мероприятий и специальных операций[1].

Из указанного обзора следует, что работа Центра будет сосредоточена на аналитической и превентивной работе: межгосударственном исследовании факторов, состояния, динамики и тенденций развития киберпреступности на территориях государств – участников СНГ, что позволит своевременно определять новые криминальные угрозы и вызовы, вырабатывать соответствующие меры противодействия.

В одном из заявлений заместителя министра внутренних дел Узбекистана Н. Тураходжаева было отмечено следующее: «Предлагаем среди правоохранительных структур стран – участников СНГ рассмотреть возможность создания базового научно-исследовательского подразделения, осуществляющего свою деятельность на постоянной основе, в функции которого будет входить проведение анализа совершаемых преступлений с использованием информационных технологий»[2].

Вместе с тем объективные реалии происходящих событий в информационном пространстве определяют необходимость создания постоянно действующего специализированного отрас-

---

[1] Новые способы совершения преступлений в сфере ИТ на территории государств – участников СНГ : аналитический обзор / [И. Б. Колчевский и др.]. М. : ВНИИ МВД России, 2018. С. 68–69.

[2] Из выступления Н. Тураходжаева на Международном экспертном форуме СНГ по вопросам обеспечения информационной безопасности, организованном Институтом стратегических и межрегиональных исследований при Президенте Республики Узбекистан совместно с Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан и Исполнительным комитетом СНГ, 29 июня 2021 г. // Кибербезопасность – проблема общая. О Международном экспертном форуме СНГ // Интернет-портал СНГ. URL: https://ecis.info/news/566/95743/.

левого органа СНГ по вопросам противодействия преступлениям в сфере ИТ. Подобный опыт активно практикуется в других областях. Так, в рамках противодействия международному терроризму и иным проявлениям экстремизма функционирует Антитеррористический центр СНГ (АТЦ)[1]. Его деятельность направлена на координацию взаимодействия компетентных органов в области борьбы с международным терроризмом и иными проявлениями экстремизма. К числу ключевых функций АТЦ относятся:

– выработка предложений СГГ и другим органам СНГ о направлениях развития сотрудничества в борьбе с международным терроризмом и иными проявлениями экстремизма;

– анализ информации о состоянии, динамике и тенденциях распространения международного терроризма и иных проявлений экстремизма;

– проведение аналитических исследований по актуальным вопросам международной антитеррористической деятельности;

– формирование и развитие Специализированного банка данных;

– участие в подготовке и проведении антитеррористических командно-штабных и оперативно-тактических учений;

– содействие государствам в подготовке и проведении оперативно-разыскных мероприятий и комплексных операций по борьбе с международным терроризмом и иными проявлениями экстремизма, в осуществлении межгосударственного розыска лиц, совершивших преступления террористического характера и скрывающихся от уголовного преследования или исполнения судебного приговора, и др.

Особенностью подобного формата сотрудничества государств – участников СНГ является возможность компетентного

[1] Положение об Антитеррористическом центре государств – участников Содружества Независимых Государств // Официальный сайт АТЦ СНГ. URL: https://www.cisatc.org/132/166/189.

согласованного комплексного решения проблем, связанных со специализированной сферой преступной деятельности. В этом состоит эффективность и значимость работы АТЦ.

По аналогии с обозначенным органом на сегодняшний день представляется востребованным учреждение Центра по противодействию преступлениям в сфере ИТ. Указанная структура позволит укрепить межгосударственное взаимодействие в борьбе с противоправными деяниями, совершаемыми в сфере ИТ, и повысить результаты предупреждения, раскрытия и расследования преступлений в исследуемой области.

В случае принятия положительного решения относительно учреждения Центра по противодействию преступлениям в сфере ИТ в качестве постоянно действующего специализированного отраслевого органа СНГ к числу его основных функций представляется возможным отнести следующие:

1. Развитие межгосударственного взаимодействия в борьбе с преступлениями в сфере ИТ:

– подготовка предложений СГГ и другим структурам СНГ относительно направлений развития межгосударственного взаимодействия в борьбе с преступлениями в сфере ИТ;

– участие в разработке модельных законодательных актов, нормативных правовых документов и международных договоров, регулирующих вопросы противодействия преступлениям в сфере ИТ;

– участие в подготовке межгосударственных программ по борьбе с преступлениями в сфере ИТ;

– установление рабочих контактов с международными организациями, занимающимися проблемами противодействия преступлениям в сфере ИТ, и специализированными подразделениями других государств;

– проведение аналитических исследований в области актуальных вопросов международного сотрудничества по противодействию преступлениям в сфере ИТ;

– разработка моделей согласованных операций по противодействию преступлениям в сфере ИТ, а также оказание поддержки в их проведении.

2. Координация взаимодействия правоохранительных органов по противодействию преступлениям в сфере ИТ:

– участие в проведении командно-штабных и оперативно-тактических учений по противодействию преступлениям в сфере ИТ;

– содействие государствам – участникам СНГ в проведении оперативно-разыскных мероприятий, комплексных операций по противодействию преступлениям в сфере ИТ, в осуществлении межгосударственного розыска лиц, совершивших противоправные деяния в сфере ИТ и скрывающихся от уголовного преследования или исполнения судебного приговора;

– содействие в подготовке кадров, специализирующихся в области противодействия преступлениям в сфере ИТ.

3. Стратегическая оценка современных вызовов и угроз, а также опыта сотрудничества государств – участников СНГ в сфере ИТ:

– анализ информации по состоянию, динамике и тенденциям развития преступлений в сфере ИТ;

– организация научно-практических конференций и семинаров, обмен опытом в области противодействия преступлениям в сфере ИТ.

4. Создание и развитие Специализированного банка данных по противодействию преступлениям в сфере ИТ с использованием возможностей Объединенных банков данных других органов СНГ, предоставление на регулярной основе информации по запросам компетентных органов:

– о международных преступных организациях, совершающих противоправные деяния в сфере ИТ;

– состоянии и тенденциях развития преступлений в сфере ИТ;

– неправительственных организациях и лицах, содействующих криминальным структурам в совершении преступлений в сфере ИТ[1].

Реформы в данном секторе сотрудничества государств – участников СНГ будут соответствовать тенденциями, заложенным в Концепции дальнейшего развития Содружества Независимых Государств 2020 г.[2] Как определено в Концепции, в перспективе сотрудничество в сфере безопасности, борьбы с преступностью, поддержания и укрепления международной безопасности и стабильности, противодействия новым вызовам и угрозам остается одной из наиболее востребованных областей взаимодействия. Для ее реализации будет требоваться дальнейшая активизация государств – участников СНГ и соответствующих органов отраслевого сотрудничества СНГ в области борьбы с терроризмом, экстремизмом, трансграничной преступностью, а также в области обеспечения международной информационной безопасности и противодействия преступлениям в сфере информационно-коммуникационных технологий.

В завершение параграфа отметим, что идея создания специализированных структур информационного направления касается не только противодействия преступности в сфере ИТ, но и обеспечения информационной безопасности. Так, в ходе саммита в Минске в ноябре 2014 г. государства – участники СНГ выразили готовность поддержать инициативу по созданию еди-

---

[1] Мысина А. И. Международно-правовое регулирование сотрудничества государств по противодействию преступлениям в сфере информационных технологий : дис. ... канд. юрид. наук : 12.00.10. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.

[2] Концепция дальнейшего развития Содружества Независимых Государств. Приложение к Решению Совета глав государств Содружества Независимых Государств о Концепции дальнейшего развития Содружества Независимых Государств и Плане основных мероприятий по ее реализации от 18 декабря 2020 г. // Единый реестр правовых актов и других документов Содружества Независимых Государств. URL: http://cis.minsk.by/reestr/ru/index.-html#reestr/view/text?doc=6363.

ного Центра обеспечения безопасности киберпространства СНГ[1].

Таким образом, инициативы СНГ выполняют важные функции выстраивания правового пространства в сфере ИКТ, а также обеспечивают решение технических аспектов в сфере общей кибербезопасности.

§ 3.2. Направления взаимодействия в сфере информационной безопасности и борьбе с преступностью в рамках Шанхайской организации сотрудничества

Не менее активно Российская Федерация осуществляет взаимодействие с зарубежными партнерами по формированию правовых и институциональных основ сотрудничества в сфере информационной безопасности и противодействия преступности в данной области на евразийском пространстве по линии Шанхайской организации сотрудничества (далее – ШОС)[2].

Сотрудничество государств в области обеспечения международной информационной безопасности на уровне ШОС инициировано в результате блокирования работы ГПЭ ООН, дея-

---

[1] Международная информационная безопасность / [А. В. Бирюков и др.]. С. 312.

[2] Россия считает важным дальнейшее укрепление позиций ШОС в региональных и глобальных делах и расширение ее состава, выступает за наращивание политического и экономического потенциала ШОС, осуществление в ее рамках практических мер, способствующих укреплению взаимного доверия и партнерства в Центральной Азии, а также за развитие взаимодействия с государствами – членами ШОС, наблюдателями при ШОС и партнерами по диалогу ШОС // Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации 30 ноября 2016 г.) // Официальный сайт МИД России. URL: https://www.mid.ru/foreign_policy/-official_documents//asset_publisher/CptICkB6BZ29/content/id/254-2248.

тельность которой была «заморожена» до 2009 г.[1] Начиная с 2006 г. государства – члены ШОС предприняли ряд важных шагов по формированию основ региональной системы международной информационной безопасности.

Сходство позиций государств по основным проблемам в области международной информационной безопасности и намерение объединить усилия по противодействию информационным угрозам с учетом соблюдения принципов и норм международного права[2] побудили глав государств – членов ШОС учредить Группу экспертов по международной информационной безопасности (далее – Группа ШОС по МИБ)[3].

Логическим завершением работы Группы ШОС по МИБ стала разработка Соглашения между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности, подписанного 16 июня 2009 г. в Екатеринбурге (Россия)[4]. Рассматриваемое соглашение стало первым международным договором, направленным на комплексное противодействие угрозам международной информационной безопасности, связанным с использованием ИТ в противоправных целях.

В Соглашении были определены основные направления сотрудничества, среди которых комплекс мер в области обеспечения международной информационной безопасности, а также не-

---

[1] Проблематика международной информационной безопасности на площадках ШОС и БРИКС // Официальный сайт ШОС. URL: http://www.infoshos.ru/ru/?idn=20567.

[2] Заявление глав государств – членов Шанхайской организации сотрудничества по международной информационной безопасности от 15 июня 2006 г. // Официальный сайт ШОС. URL: http://infoshos.ru/ru/?id=94.

[3] Группа экспертов государств – членов ШОС по МИБ является постоянно действующим органом ШОС и осуществляет работу по координации профильных министерств и ведомств с 2006 г.

[4] Соглашение между правительствами государств – членов ШОС о сотрудничестве в области обеспечения информационной безопасности 2009 г. // Официальный сайт ШОС. URL: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.

сколько уголовно-правовых направлений: противодействие угрозам использования ИКТ в террористических целях и информационной преступности. Заключение данного соглашения активизировало деятельность мирового сообщества по формированию глобальной системы в рассматриваемой области, в частности в рамках ООН. Договоренности государств – членов ШОС вывели на новый уровень дискуссию по проблематике международной информационной безопасности, проводимую в ходе работы новой ГПЭ ООН[1]. Кроме того, в 2011 г. Секретариат ШОС подписал меморандум о взаимопонимании с УНП ООН[2].

Результаты деятельности Группы ШОС по МИБ наглядно показали эффективность работы относительно новой региональной международной организации, в рамках которой удалось разработать и такой значимый документ, как Правила поведения в области обеспечения международной информационной безопасности, в котором раскрывается официальная согласованная позиция Российской Федерации и ее партнеров по ШОС, основанная на идее необходимости регулирования поведения государств в информационном пространстве[3].

Обновленная редакция обозначенного документа была распространена 9 января 2015 г. на 69-й сессии Генассамблеи ООН. В 2018 г. государства – члены ООН одобрили большинством голосов резолюцию «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», в которую по инициативе Российской Федерации вошел свод разработанных государствами – членами ШОС 13 правил, норм

---

[1] Сотрудничество в области безопасности в рамках ШОС (справочный материал) // Официальный сайт МИД России. URL: http://www.infoshos.ru/-ru/?idn=20567.

[2] Сотрудничество с ООН // Официальный сайт ШОС. URL: http://rus.-sectsco.org/ cooperation/20151208/16875.html.

[3] Правила поведения в области обеспечения международной информационной безопасности // Официальный сайт ООН. URL: https://www.un.org/-ga/search/view_ doc.asp?

и принципов ответственного поведения государств в информационном пространстве[1].

После разработки региональной концепции международной информационной безопасности и ее апробации на универсальной площадке ООН в декларативных документах ШОС на первый план стали выходить вопросы сотрудничества государств по противодействию преступлениям в сфере ИТ. Вместе с тем формировать самостоятельную Группу экспертов или иной специализированный орган для разработки нормативного акта по борьбе с информационным проявлением преступности государства – члены ШОС не намерены. В данном направлении они привержены идее разработки всеобъемлющей конвенции под эгидой ООН[2].

Однако анализ декларативных документов ШОС подтверждает готовность государств – членов ШОС укреплять сотрудничество в области борьбы с преступлениями в информационной сфере посредством организации мониторинга потенциальных угроз в информационном пространстве и повышения эффективности противодействия подобным угрозам[3].

С учетом специфики первоначальных задач, стоящих перед ШОС, пресечение актов терроризма, сепаратизма и экстремизма в Средней Азии, проводится масштабная работа по борьбе с такими проявлениями в киберпространстве.

---

[1] Резолюция Генеральной Ассамблеи ООН A/RES/73/27 от 11 декабря 2018 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // Официальный сайт ООН. URL: https://-undocs.org/pdf?

[2] О заявлении Совета глав государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности // Официальный сайт МИД России. URL: https://www.mid.ru/foreign_policy/-news//asset_publisher/cKNonk-JE02Bw/content/id/4420179.

[3] Астанинская декларация глав государств – членов ШОС 2017 г. // Официальный сайт Президента Российской Федерации. URL: http://www.kremlin.-ru/supplement/5206 ; Циндаоская декларация Совета глав государств – членов ШОС 2018 г. // Официальный сайт Президента Российской Федерации. URL: http://www.kremlin.ru/supplement/5315.

Практическая деятельность по обнаружению и противодействию террористической активности в информационном пространстве, пресечению распространения террористической идеологии и пропаганды в сети Интернет осуществляется на базе Региональной антитеррористической структуры ШОС (далее – РАТС). В целях организации международного розыска лиц, причастных к террористической, экстремистской и сепаратистской деятельности, на пространствах ШОС ведется формирование Единого разыскного реестра органов безопасности и специальных служб государств – членов ШОС[1].

Государства – члены ШОС подчеркивают значимость выработки передовых практик противодействия распространению незаконного контента в сети Интернет, а также международных стандартов с учетом признания за государствами ведущей роли в противодействии распространению экстремистского, сепаратистского и террористического контента в Интернете и использованию ИКТ в террористических целях[2].

Отмечая важность осуществляемого по линии РАТС обмена информацией о выявленных в сети Интернет материалах, пропагандирующих террористическую, сепаратистскую и экстремистскую деятельность, государства – члены ШОС выступают за углубление сотрудничества между компетентными органами в рамках РАТС в данной сфере[3].

Осознавая общественную опасность обозначенных тенденций, ШОС определяет своим приоритетом реализацию Про-

---

[1] Противодействие терроризму в рамках ШОС (справка) // Официальный сайт МИД России. URL: https://www.mid.ru/san-hajskaa-organizacia-sotrudnicestva-sos-/-/asset_ publisher/0vP3h-QoCPRg5/content/id/187762.

[2] Московская декларация Совета глав государств – членов ШОС от 10 ноября 2020 г. // Официальный сайт ШОС. URL: http://rus.sectsco.org/news/-20201110/689169.html.

[3] Заявление Совета глав государств – членов ШОС о противодействии распространению террористической, сепаратистской и экстремистской идеологии, в том числе в сети Интернет. 10 ноября 2020 г. // Официальный сайт ШОС. URL: http://rus.sectsco.org/documents/20201110/690013.html.

граммы сотрудничества по противодействию данным рискам[1], а также вопросы развития и расширения институциональной системы ШОС на базе РАТС. Так, на саммите ШОС в ноябре 2020 г. президент Казахстана Касым-Жомарт Токаев выступил за оперативное создание Центра информационной безопасности на базе РАТС[2]. Представляется, что реализации обозначенной инициативы станет логическим продолжением развития тенденции создания специализированных структур в исследуемой области, а также значительно повысит эффективность деятельности ШОС по противодействию угрозам информационной безопасности и преступлениям в сфере ИТ.

Перспективными направлениями развития ШОС в исследуемой сфере являются не только правовые концепции, например связанные с разработкой конвенции безопасного функционирования и развития сети Интернет, нацеленные на противодействие киберпреступности и предупреждение угроз информационной безопасности[3], но и проекты по совершенствованию институциональных механизмов взаимодействия по борьбе с преступностью, в том числе в сфере информационных технологий.

В соответствии с принятой в 2021 г. Душанбинской декларацией двадцатилетия ШОС в целях совершенствования механизмов противодействия вызовам и угрозам безопасности государствами – членами ШОС рассматриваются следующие инициативы: о создании Антинаркотического центра ШОС в г. Душанбе в качестве отдельного постоянно действующего органа (Республика Таджикистан), об учреждении на базе Региональной антитеррористической структуры (РАТС) ШОС

[1] Официальный сайт ШОС. URL: http://www.infoshos.ru/.

[2] Следует отметить, что впервые с этой идеей К.-Ж. Токаев выступил в июне 2019 г. на саммите ШОС в Бишкеке // Казахстан выступил за скорейшее создание Центра информационной безопасности ШОС // Официальный сайт ШОС. URL: http://www.infoshos.ru/ru/?idn=25857.

[3] В Москве прошло заседание группы экспертов государств – членов ШОС по международной информационной безопасности // Официальный сайт ШОС. URL: http://rus.sectsco.org/news/20191112/599223.html.

в г. Ташкенте Универсального центра по противодействию вызовам и угрозам безопасности государств – членов ШОС (Российская Федерация), о создании Центра информационной безопасности ШОС (Республика Казахстан), об учреждении Центра по противодействию международной организованной преступности в г. Бишкеке (Кыргызская Республика)[1].

Эти же решения нашли закрепление в Самаркандской декларации Совета глав государств – членов ШОС, принятой по итогам заседания Совета глав государств – членов ШОС в г. Самарканде 16 сентября 2022 г.[2]

Кроме того, в числе важнейших инициатив, озвученных в рамках саммита ШОС, – предложение организовать в рамках группы экспертов организации специализированную дискуссию по вопросам применимости международного права в сфере использования ИКТ и выработки терминологии в сфере информационной безопасности. Важным шагом могло бы стать и создание реестра командных пунктов в рамках ШОС по обмену сведениями о компьютерных инцидентах с целью обнаружения, предотвращения и ликвидации последствий кибератак. Не менее важно формирование списка подразделений и контактных лиц, ответственных за взаимодействие в правоохранительной сфере по пресечению, выявлению и расследованию преступлений, связанных с использованием ИКТ. Серьезной проблемой остается и нехватка квалифицированных специалистов в области международной информационной безопасности. В их подготовке заинтересованы все страны – члены ШОС[3].

---

[1] Душанбинская декларация двадцатилетия ШОС от 17 сентября 2021 г. // Официальный сайт ШОС. URL: http://rus.sectsco.org/news/20210917/7791-42.html.

[2] Самаркандская декларация Совета глав государств – членов ШОС от 16 сентября 2022 г. // Официальный сайт ШОС. URL: file:///D:/Downloads/-Самаркандская_декларация.pdf.

[3] Торин А. Информационная безопасность стран – участниц ОДКБ: актуальные проблемы и пути их решения // Международная жизнь. URL: https://-interaffairs.ru/news/show/37487.

В перспективе актуальным направлением представляется реализация Плана взаимодействия государств – членов ШОС по вопросам обеспечения международной информационной безопасности на 2022–2023 гг. В частности, в документе представлен ряд правоохранительных сфер сотрудничества и определены механизмы по их реализации, способствующие противодействию преступлениям в сфере ИТ в рамках ШОС.

Так, согласно п. 7 Плана «Взаимодействие в правоохранительной сфере по расследованию преступлений, связанных с использованием ИКТ, в том числе в террористических целях», на постоянной основе запланированы:

– обмен опытом между государствами – членами ШОС в области борьбы с информационной преступностью и информационным терроризмом, в том числе путем налаживания двустороннего и многостороннего сотрудничества;

– расширение рабочих контактов между компетентными органами государств – членов ШОС, занимающихся вопросами борьбы с информационной преступностью и информационным терроризмом;

– подготовка и направление запросов в отношении лиц, причастных к совершению преступлений в сфере ИКТ;

– проведение мероприятий по обсуждению инициатив государств – членов ШОС, направленных на противодействие использованию ИКТ в террористических и иных преступных целях, а также согласованию позиций по их продвижению на международных площадках.

Заслуживает отдельного внимания проработка вопроса по реализации возможностей использования электронной подписи и защиты информации при трансграничном информационном обмене (п. 11 Плана). В целях реализации данного направления в течение 2022 г. были проведены консультации в рамках Группы экспертов ШОС по международной информационной безопасности по вопросу организации и порядку об-

мена информацией в интересах формирования согласованной политики по использованию электронной подписи и защите информации при международном информационном обмене, включая выработку организационно-технических процедур[1].

Данное направление особенно актуально с точки зрения правоохранительного аспекта по противодействию угрозе использования информационно-коммуникационных технологий в преступных целях, поскольку в настоящее время на повестке дня стоит проблема информационного обмена между МВД России и правоохранительными органами иностранных государств, в том числе в аспекте допустимости электронных доказательств, полученных по электронным каналам связи.

§ 3.3. Сотрудничество по борьбе с информационными угрозами в рамках БРИКС

Создание БРИКС[2], инициированное в 2006 г. Российской Федерацией, явилось одним из наиболее значимых геополитических событий начала нового столетия. Данное объединение смогло за короткое время стать весомым актором мировой политики. Становление БРИКС отражает объективную тенденцию мирового развития к формированию полицентричной системы международных отношений и усилению экономической взаимозависимости государств. В такой системе все более широкое применение находят неинституциональные структуры глобального управления и сетевая дипломатия.

---

[1] Сообщение для СМИ об итогах заседания Группы экспертов ШОС по международной информационной безопасности (Ташкент, 13 июля 2022 г.) // Официальный сайт ШОС. URL: http://rus.sectsco.org/news/20220719/8551-25.html.

[2] Изначально объединение включало Бразилию, Россию, Индию и Китай (БРИК). В феврале 2011 г. к БРИК присоединилась Южно-Африканская Республика, после чего объединение получило название БРИКС. В ноябре 2022 г. заявку на вступление в БРИКС подал Алжир.

Основу влиятельности БРИКС на международной арене составляют растущая экономическая мощь государств-участников, значимость их деятельности как одной из главных движущих сил развития глобальной экономики, значительная численность населения, наличие богатых природных ресурсов. Политическая влиятельность БРИКС определяется тем, что входящие в объединение государства являются авторитетными участниками ведущих международных организаций и структур, а также региональных объединений[1].

Российская Федерация строит отношения с партнерами по БРИКС на основе Устава ООН, общепризнанных принципов и норм международного права, а также принципов, согласованных между участниками объединения, таких как открытость, прагматизм, солидарность, неблоковый характер и ненаправленность против третьих сторон[2].

Сотрудничество со странами БРИКС является стратегическим направлением внешней политики Российской Федерации, что подчеркивается в Концепции внешней политики утвержденной, Президентом Российской Федерации[3].

Практическое взаимодействие в рамках БРИКС охватывает торгово-экономическую, научно-техническую, сельскохозяй-

---

[1] Российская Федерация – Содружества Независимых Государств, Организации Договора о коллективной безопасности, Евразийского экономического сообщества, Таможенного союза; Российская Федерация и КНР – Шанхайской организации сотрудничества, Азиатско-тихоокеанского экономического сотрудничества; Бразилия – Союза южноамериканских государств, Южноамериканского общего рынка, Сообщества латиноамериканских и карибских государств; Южно-Африканская Республика – Африканского союза, Сообщества развития Юга Африки; Индия – Ассоциации регионального развития стран Южной Азии.

[2] Концепция участия Российской Федерации в объединении БРИКС от 15 апреля 2013 г. // НПП «Гарант-сервис». URL: https://www.garant.ru/products/ipo/prime/doc/70257510/.

[3] Указ Президента Российской Федерации от 30 ноября 2016 г. № 640 «Об утверждении Концепции внешней политики Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_207990/.

ственную, гуманитарную, природоохранную и другие сферы. По итогам председательства России в БРИКС в 2015–2016 гг. началась работа по новым направлениям: энергоэффективность, промышленность, миграция, телекоммуникации, экология, содействие международному развитию. На современном этапе одним из важнейших и перспективных направлений становятся информационно-коммуникационные технологии, в более широком плане – «цифровая экономика»[1].

Взаимодействие в рамках БРИКС будет содействовать реализации национальных интересов в информационной сфере, определенных в Доктрине информационной безопасности Российской Федерации 2016 г.[2]

Значимость сотрудничества в данной сфере подчеркнута в Концепции участия Российской Федерации в объединении БРИКС, прямо устанавливающей, что одной из основных наших целей является поэтапное создание общего информационного пространства государств – участников БРИКС[3]. Так, согласно Концепции основными целями Российской Федерации в области сотрудничества с государствами – участниками БРИКС по вопросам международной безопасности среди прочего являются «сотрудничество в интересах обеспечения международной информационной безопасности, использование возможностей БРИКС для продвижения инициатив в этом направлении в рамках различных международных форумов

---

[1] Киберпространство БРИКС: правовое измерение : монография / [И. И. Шувалов и др.] ; под ред. Д. Руйпин, Т. Я. Хабриева. М. : Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2017. С. 3–4.

[2] Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_208191/.

[3] Концепция участия Российской Федерации в объединении БРИКС от 15 апреля 2013 г. // НПП «Гарант-сервис». URL: https://www.garant.ru/products/ipo/prime/doc/70257510/.

и организаций, прежде всего ООН; укрепление в формате БРИКС сотрудничества в области противодействия использованию информационно-коммуникационных технологий в военно-политических, террористических и криминальных целях, а также в целях, противоречащих обеспечению международного мира, стабильности и безопасности».

С целями выработки практических предложений, касающихся основных областей сотрудничества, а также координации позиций государств объединения на различных площадках была сформирована Рабочая группа экспертов по вопросам безопасности в сфере использования ИКТ как специализированный орган по проблематике ИКТ, аналогичный ранее созданным Группам в некоторых международных организациях.

В соответствии с Уфимской декларацией, принятой на VII саммите БРИКС 9 июля 2015 г., сотрудничество государств-участников в сфере ИКТ развивается в следующих областях:

– обмен информацией и передовой практикой;

– эффективная координация мер по противодействию киберпреступности;

– взаимодействие по вопросам реагирования на компьютерные инциденты в области компьютерной безопасности;

– совместные проекты в области НИОКР; разработка международных норм, принципов и стандартов[1].

Кроме того, в Уфимской декларации была признана необходимость разработки под эгидой ООН универсального договора по борьбе с использованием ИКТ в преступных целях. Такой подход находил отражение во всех последующих декларациях, принятых по итогам саммитов БРИКС (Уфимская – 2015 г., Декларации Гоа – 2016 г., Сямэнская – 2017 г., Йоханнесбургская декларация – 2018 г., Декларация Бразилиа – 2019 г., Москов-

[1] VII саммит БРИКС – Уфимская декларация (г. Уфа, Российская Федерация, 9 июля 2015 г.) // НПП «Гарант-сервис». URL: https://base.garant.ru/71480256/.

ская декларация – 2020 г., Делийская декларация – 2021 г., Пекинская декларация – 2022 г.)[1].

Таким образом, начиная с 2014 г. главы государств в ежегодных документах по итогам саммитов подтверждают «приверженность выработке универсального и имеющего обязательную юридическую силу международно-правового документа в данной области», фиксируют желание «изучать возможности для сотрудничества в области борьбы с киберпреступлениями» и обязуются «сотрудничать в выявлении возможностей для осуществления совместных действий по решению общих проблем безопасности в сфере использования ИКТ».

Консолидированная позиция экспертов государств – участников БРИКС позволяет объединять усилия для отстаивания собственных подходов в рамках деятельности экспертных групп на площадке ООН по вопросам международной информационной безопасности и противодействия преступности в сфере ИКТ. Однако необходимо отметить, что к настоящему времени два государства – участника БРИКС являются участниками Будапештской конвенции 2001 г. – Южно-Африканская Республика и присоединившаяся к договору в феврале 2022 г. Бразилия[2]. Как отмечают специалисты, реализация Будапештской конвенции будет требовать от этих государств усилий по гармонизации своего законодательства «с европейскими стан-

---

[1] VII саммит БРИКС – Уфимская декларация (г. Уфа, Россия, 9 июля 2015 г.) ; VIII саммит БРИКС – Декларация Гоа (Гоа, Индия, 16 октября 2016 г.) ; IX саммит БРИКС – Сямэньская декларация (г. Сямэнь, Китай, 4 сентября 2017 г.) ; X саммит БРИКС – Йоханнесбургская декларация (г. Йоханнесбург, ЮАР, 26 июля 2018 г.) ; XI саммит БРИКС – Декларация Бразилиа (г. Бразилиа, Бразилия, 14 ноября 2019 г.) ; XII саммит БРИКС – Московская декларация (г. Москва, Россия, 17 ноября 2020 г.) ; XIII саммит БРИКС – Делийская декларация (г. Нью-Дели, Индия, 9 сентября 2021 г.) ; XIV саммит БРИКС – Пекинская декларация (г. Пекин, КНР, 23-24 июня 2022 г.) // Национальный комитет по исследованию. БРИКС. URL: https://nkibrics.ru/-pages/summit-docs.

[2] Brazil joins the convention on cybercrime: how will it impact other brics countries? // BRICS information portal. URL: https://infobrics.org/post/35219/.

дартами», проведения последовательной политики в рамках своих обязательств по БРИКС в части разработки международного обязательного договора по противодействию незаконному использованию сферы ИКТ, а также одновременного выполнения соглашений внутри БРИКС по кибербезопасности[1].

Активная позиция Российской Федерации по сотрудничеству в сфере ИКТ в рамках БРИКС привела к расширению направлений взаимодействия, реализация которых может оказывать содействие в превенции преступности в сфере ИКТ: национальные системы цифровой идентификации, большие данные для государственной политики, национальные системы управления данными и «умные» города[2].

В перспективной повестке объединения – развитие практического сотрудничества между странами БРИКС в области МИБ, в том числе посредством реализации принятой в 2017 г. «Дорожной карты» практического сотрудничества стран БРИКС в обеспечении безопасности в сфере использования ИКТ и в рамках деятельности Рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ[3].

Кроме того, перспективным направлением является формирование нормативно-правовых рамок для сотрудничества стран БРИКС по вопросам МИБ, а также рассмотрение и подготовка соответствующих предложений, в том числе о разработке межправительственного соглашения БРИКС о сотрудничестве в об-

---

[1] Brazil joins the convention on cybercrime: how will it impact other brics countries? // BRICS information portal. URL: https://infobrics.org/post/35219/.

[2] Сотрудничество стран БРИКС в сфере ИКТ по предложению России расширено четырьмя новыми направлениями // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://digital.gov.ru/ru/events/39262/.

[3] Пекинская декларация (г. Пекин, Китай, 23–24 июня 2022 г.) // Национальный комитет по исследованию. БРИКС. URL: https://nkibrics.ru/pages/-summit-docs.

ласти обеспечения безопасности в сфере использования ИКТ и двусторонних соглашений между государствами объединения[1].

Данный проект на протяжении многих лет инициирует Российская Федерация, последовательно пытаясь добиться подписания пятистороннего соглашения в сфере информационной безопасности под эгидой БРИКС. В Форталезской декларации, принятой по итогам VI саммита БРИКС 15 июня 2014 г., впервые закреплено российское предложение о разработке пятистороннего межправительственного соглашения о сотрудничестве в области обеспечения безопасности в сфере использования ИКТ. Рабочий проект данного документа был официально распространен российской стороной в апреле 2015 г. и представлен в ходе заседания Рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ (далее – РГ БРИКС; г. Москва, 16–18 июня 2015 г.). Делегации заслушали подробную презентацию проекта соглашения, высказали свои комментарии и взяли документ на проработку в столицах.

Необходимость создания правовых рамок для сотрудничества государств – участников БРИКС в сфере обеспечения МИБ путем разработки упомянутого соглашения последовательно закреплялась в итоговых декларациях саммитов объединения вплоть до 2018 г. (включительно). При этом к предметному рассмотрению и согласованию распространенного Россией проекта страны не приступили. В 2019 г. в Декларации Бразилиа XI саммита БРИКС вышеуказанная «формула» была дополнена бразильским предложением о разработке двусторонних соглашений по МИБ между странами объединения.

В рамках российского председательства в БРИКС в 2020 г. продолжили выводить партнеров на разработку проекта пятистороннего межправительственного соглашения в соответствии

[1] Делийская декларация (г. Нью-Дели, Индия, 9 сентября 2021 г.) // Национальный комитет по исследованию. БРИКС. URL: https://nkibrics.ru/pages/-summit-docs.

с ранее достигнутыми договоренностями лидеров. Вновь обсудили данный вопрос в ходе 6-го заседания профильной РГ БРИКС (26–27 августа 2020 г.) и 7-го заседания РГ БРИКС (12 августа 2021 г.).

Несмотря на активную проработку данного вопроса, результатов эти инициативы не имеют до сих пор. Как отмечают эксперты, полную и открытую поддержку Российской Федерации выразила лишь ЮАР[1].

Другие участники БРИКС воздерживаются от динамичного переговорного процесса по данной проблематике, поскольку имеют свои оценки ситуации в информационной сфере и сфере информационной безопасности. Так, по мнению партнеров из КНР, страны БРИКС уже достигли взаимопонимания в вопросах обеспечения информационной безопасности; механизмы противодействия трансграничной сетевой преступности, обмена данными и технического взаимодействия между ними уже существуют. Наращивать взаимодействие в вопросах информационной безопасности представители КНР предлагают лишь «между различными исследовательскими центрами стран БРИКС»[2]. Представители Бразилии отмечают, что БРИКС необходимы лишь «стандарты безопасности, которые позволят странам без опасений обмениваться информацией». Иными словами, открыто обозначили свою неготовность на данном этапе подключаться к каким-либо принципиально новым пятисторонним договоренностям – юридическим или политическим – в сфере МИБ. Их позицию поддержали индийские партнеры.

---

[1] Муратшина К. Г. К вопросу о сотрудничестве в области информационной безопасности в рамках БРИКС // Гуманитарное знание и искусственный интеллект: стратегии и инновации : материалы международной конференции. Екатеринбург : Издательство Уральского университета, 2020. С. 614–620.

[2] Информационный бюллетень о деятельности стран БРИКС в области научно-технического и инновационного сотрудничества во второй половине 2020 г. Секретариат Совета НТИ БРИКС, 2020.

Российская Федерация продолжает работу над проектом соглашения по кибербезопасности в БРИКС, надеясь найти компромисс и консенсус с партнерами[1].

Однако стоит отметить, что в Пекинской декларации 2022 г. вопрос о заключении пятистороннего договора по вопросам МИБ не нашел своего закреплении по аналогии с решениями, принятыми на предыдущих саммитах.

Несмотря на замедленную динамику в вопросе пятистороннего межправительственного соглашения о сотрудничестве в области обеспечения безопасности в сфере использования ИКТ, между Российской Федерацией и государствами – участниками БРИКС успешно заключены двусторонние соглашения по данной тематике. Состояние действия международных договоров и их характер приведены в *прил. 10*.

Российской Федерации предстоит дальнейшая проработка взаимодействия с Бразилией и ЮАР по соглашениям в области обеспечения МИБ, поскольку заключенные с данными государствами договоры до сих пор не вступили в силу. Как представится, на данном направлении могут возникнуть сложности ввиду присоединения ЮАР и Бразилии (февраль 2022 г.) к Будапештской конвенции 2001 г.

Важным шагом в развитии сотрудничества между участниками БРИКС в вопросах обеспечения использования сферы ИКТ явилось проведение в августе 2021 г. 1-го семинара по цифровой криминалистике для стран БРИКС в рамках председательства Индии[2]. Мероприятие позволило объединить широкое экспертное сообщество из стран БРИКС, представителей правительств, экспертов правоохранительных органов, специалистов информационной безопасности в рамках обсуждения широкого круга вопросов, связанных с обработкой цифровых

---

[1] Шестая буква БРИКС: международная безопасность и интересы России / [ред. В. А. Орлов, С. Д. Семенов]. М. : ПИР-Пресс, 2021.

[2] 1st Workshop on Digital Forensics for BRICS Countries // BRICS information portal. URL: https://infobrics.org/post/33914.

доказательств, защиты данных и конфиденциальности, криминалистическим анализом новых технологий, а также обсуждением будущих проблем цифровой криминалистики и разработками по их преодолению.

В качестве предложения представляется возможным инициировать от имени Российской Федерации позицию по ежегодному проведению таких научно-экспертных мероприятий на территории председательствующего государства с целями обмена передовым опытом эффективного использования цифровой криминалистики в гражданских/уголовных или административных расследованиях.

Завершая рассмотрение вопроса о сотрудничестве по борьбе с информационными противоправными угрозами в рамках БРИКС, следует отметить общность подходов государств в формате ШОС и БРИКС к формированию системы международной информационной безопасности.

Принятые в 2019 г. 73-й сессией Генеральной Ассамблеи ООН российские проекты резолюций «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» и «Противодействие использованию информационно-коммуникационных технологий в преступных целях» аккумулировали идеи, ранее отраженные в итоговых документах саммитов упомянутых объединений, и открыли качественно новый этап дискуссии на главной международной площадке – Организации Объединенных Наций[1].

Государства ШОС и БРИКС, разделив с Россией соавторство резолюций Генассамблеи ООН, по праву стали лидерами мирового сообщества на пути построения глобальной системы международной информационной безопасности.

---

[1] Бойко С. Проблематика международной информационной безопасности на площадках ШОС и БРИКС // Международная жизнь. URL: https://inter-affairs.ru/news/show/21480.

§ 3.4. Сотрудничество государств – членов Организации Договора коллективной безопасности в сфере информационной безопасности и противодействия использованию информационно-коммуникационных технологий в террористических и других преступных целях

Активное сотрудничество в исследуемой области на постсоветском пространстве осуществляется также в рамках Организации Договора коллективной безопасности (далее – ОДКБ). В частности, в Стратегии коллективной безопасности ОДКБ на период до 2025 г. отмечается, что одним из ключевых факторов, отнесенных к современным вызовам и угрозам среди прочих является использование информационных и коммуникационных технологий в преступных целях[1]. В этой связи формирование безопасного информационного пространства государств – членов ОДКБ представляет собой одну из основных стратегических задач в сфере обеспечения коллективной безопасности (п. 5.3 Стратегии ОДКБ до 2025 г.).

В комплекс взаимосвязанных мер развития коллективной информационной системы безопасности входят следующие направления:

– формирование системы информационной безопасности государств – членов ОДКБ;

– развитие межгосударственного сотрудничества и укрепление межведомственной координации в сфере обеспечения информационной безопасности;

---

[1] Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 г. Утверждена Решением Совета коллективной безопасности Организации Договора о коллективной безопасности от 14 октября 2016 г. // Официальный сайт ОДКБ. URL: https://odkbcsto.org/documents/statements/strategiya_kollektivnoy_bezopasnosti_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_na_period_do_/#loaded.

– совершенствование механизмов по противодействию угрозам в информационной сфере;

– проведение совместных мероприятий по противодействию и нейтрализации противоправной деятельности в информационно-телекоммуникационном пространстве государств – членов ОДКБ;

– взаимодействие в вопросах обеспечения международной информационной безопасности;

– выработка согласованных правил взаимодействия в информационной сфере, продвижение их на международный уровень;

– создание условий и реализация совместных практических мероприятий, направленных на формирование основ скоординированной информационной политики в интересах государств – членов ОДКБ (п. 6 Стратегии ОДКБ до 2025 г.).

Из представленного перечня следует, что государства – члены ОДКБ проводят последовательную комплексную политику одновременного развития правовых и организационных основ укрепления МИБ и противодействия преступной деятельности в информационной сфере как одной из угроз, подрывающих информационную безопасность.

В 2017 г. было подписано Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности. В ст. 3 в качестве основных угроз информационной безопасности выступают: «использование информационно-коммуникационных технологий террористическими и экстремистскими организациями, организованными преступными группами (сообществами)»; «осуществление противоправной деятельности с использованием ИКТ».

Обеспечение информационной безопасности государств – членов ОДКБ реализуется посредством комплекса мероприятий:

– по формированию правовых основ сотрудничества и совершенствованию международной правовой базы в сфере обеспечения информационной безопасности (ст. 5);

– по выработке практических механизмов совместного реагирования на угрозы информационной безопасности (ст. 6);

– в рамках развития мер укрепления доверия в области обеспечения информационной безопасности (ст. 7);

– в рамках совершенствования технологической основы обеспечения информационной безопасности (ст. 8);

– посредством создания условий для взаимодействия компетентных органов Сторон в целях реализации настоящего Соглашения (ст. 9).

Важным вкладом в коллективные усилия государств – членов ОДКБ по борьбе с вызовами их коллективной безопасности в условиях роста информационных угроз является План мероприятий по развитию скоординированной информационной политики в интересах государств – членов Организации Договора о коллективной безопасности от 2018 г.[1] Среди прочего указанный документ предусматривает противодействие угрозам использования информационных и коммуникационных технологий для осуществления противоправных действий в отношении государств – членов ОДКБ, а также проведение мероприятий, направленных на формирование общественного сознания с це-

[1] Решение Совета коллективной безопасности Организации Договора о коллективной безопасности «О Плане мероприятий по развитию скоординированной информационной политики в интересах государств – членов Организации Договора о коллективной безопасности» // Документы, принятые по итогам сессии Совета коллективной безопасности Организации Договора о коллективной безопасности 8 ноября 2018 г. // Официальный сайт Президента Российской Федерации. URL: http://www.kremlin.ru/supplement/5357.

лью неприятия идеологии международных террористических и религиозно-экстремистских проявлений[1].

Как показывает опыт деятельности спецслужб государств – членов ОДКБ, из всех коммуникационных технологий именно компьютерные являются основным средством создания и поддержания деятельности террористических и религиозно-экстремистских организаций. По данным «Лаборатории Касперского», в 2019 г. четыре из шести государств – членов ОДКБ (Белоруссия, Армения, Киргизия и Казахстан) вошли в состав двадцатки стран с наибольшим числом пользователей, подвергшимся атакам через Интернет[2]. Связанные с этим вызовы поставили перед государственными структурами и спецорганами государств – членов ОДКБ серьезную задачу по организации противодействия терроризму и экстремизму в Интернете.

В общем спектре вызовов и угроз безопасности государств – членов ОДКБ одно из центральных мест занимает угроза их информационному суверенитету. В последние годы на национальном уровне в государствах – членах ОДКБ происходит понимание масштабов этой угрозы и необходимости выработки

[1] Последний аспект чрезвычайно важен для государств – членов ОДКБ, особенно тех, что расположены в Центральноазиатском регионе. Они испытывают на себе мощное воздействие международных террористических организаций, занимающихся через СМИ и Интернет вербовкой своих сторонников с прицелом на их последующее использование для дестабилизации внутриполитической ситуации в указанных государствах. Учитывая высокий уровень интернет-проникновения в государствах – членах ОДКБ, которое растет с каждым годом, социальные сети в настоящее время служат той средой, в которой разворачивается серьезная борьба за умы, в первую очередь, молодых людей.

[2] Киселев А. О современных подходах к развитию системы информационной безопасности в формате ОДКБ // Союзники. ОДКБ. URL: https://odkb-info.org/about_odkb/ekspertnoemnenie/?ELEMENT_ID=81.

комплексных мер противодействия ей[1]. Эта задача нашла отражение в утвержденной Президентом Российской Федерации 5 декабря 2016 г. Доктрине информационной безопасности Российской Федерации, где защита суверенитета России в информационном пространстве посредством осуществления самостоятельной и независимой политики отнесена к числу основных направлений обеспечения национальной безопасности.

В принятой Постановлением Совета Безопасности Республики Беларусь 18 марта 2019 г. Концепции информационной безопасности Республики Беларусь отмечается, что «…глобальное возрастание роли информации в системе общественных отношений, открытость информационного пространства и повышение уровня информатизации населения обусловливают новые меры безопасности информационной сферы с точки зрения обеспечения государством полноценной реализации своих суверенных прав и интересов социально-экономического развития».

В утвержденной 3 мая 2019 г. постановлением Правительства Киргизской Республики Концепции информационной безопасности Киргизской Республики на 2019–2023 гг. «распространение в сети Интернет противоправного контента, материалов деструктивного характера, а также иной идеологии, нарушающей нравственные устои общества» отнесено к числу главных внешних угроз для информационной сферы государства.

Аналогичные по смыслу нормы и принципы закреплены в национальном законодательстве и других государств – членов ОДКБ. С учетом этого весьма своевременной представляется задача гармонизации национального законодательства госу-

[1] Семериков В. А. Выступление Исполняющего обязанности Генерального секретаря ОДКБ В. Семерикова на «круглом столе» в Государственной Думе Российской Федерации на тему: «Развитие информационно-коммуникационного сотрудничества на пространстве ОДКБ» // Официальный сайт ОДКБ. URL: https://odkb-csto.org/secretary_general/appearance/vystuplenie-ispolnyayushchego-obyazannosti-generalnogo-sekretarya-odkb-valeriya-semeriko-va-na-kruglo/.

дарств-членов в части, касающейся противодействия угрозам их суверенитету в информационной сфере, а также разработка правовых актов на эту тему в формате Организации. Оптимальной площадкой для решения этой задачи, на наш взгляд, могла бы стать Парламентская Ассамблея ОДКБ, обладающая необходимым опытом и соответствующим экспертным потенциалом.

Вопросы защиты информационного (в некоторых источниках – цифрового) суверенитета[1] особенно актуальны в повестке ОДКБ в настоящее время. Как справедливо отметил заместитель Генерального секретаря ОДКБ В. А. Семериков, выступая на форуме информационной безопасности «ИНФОФОРУМ–2022», Организация видит необходимость в принятии мер по защите цифрового суверенитета в целях предотвращения преступлений и терактов с использованием информационных технологий[2]. Именно поэтому важно на уровне межгосударственного взаимодействия в рамках ОДКБ поступательно, по нарастающей выстраивать защиту от существующих и потенциальных угроз.

---

[1] Цифровой суверенитет – это способность государства проводить (формировать и реализовывать) самостоятельный политический курс в цифровой сфере (отстаивать интересы, обеспечивать безопасность и т. д.) внутри страны и международных отношениях. одним из главных условий, необходимых для формирования и поддержания национального цифрового суверенитета, должна быть способность государства проводить независимую внешнюю и внутреннюю политику в цифровом пространстве. Даже в условиях наличия необходимых составляющих (независимая цифровая инфраструктура, суверенная нормативная правовая база, профессиональные компетенции в цифровой сфере) процессы цифровизации внутри государства могут преследовать цели и интересы внешних акторов. См.: Цифровой суверенитет современного государства: содержание и структурные компоненты (по материалам экспертного исследования) / [В. А. Никонов и др.] // Вестник Томского государственного университета. Философия. Социология. Политология. 2021. № 60. С. 206–216.

[2] Заместитель Генерального секретаря ОДКБ Валерий Семериков выступил на форуме информационной безопасности «ИНФОФОРУМ–2022» // Официальный сайт ОДКБ. URL: https://odkb-csto.org/news/news_odkb/zamestitel-generalnogo-sek-retarya-odkb-valeriy-semerikov-vystupil-na-forume-informatsionnoy-bezo-pasn/#loaded.

Несмотря на активное развитие правовых, организационных, технических, оперативных и иных мер и механизмов по поддержанию коллективной МИБ, ОДКБ выступает за продвижение универсальной системы ответственного поведения государств под эгидой ООН в новом, активно формирующемся информационном пространстве. В Заявлении министров иностранных дел государств – членов ОДКБ о координации совместных усилий в сфере информационной безопасности, включая противодействие использованию информационно-коммуникационных технологий в террористических и других преступных целях, от 15 сентября 2021 г. отмечено: «Государства – члены ОДКБ вновь подчеркивают ключевую роль ООН в противодействии угрозам в сфере использования ИКТ и придают особое значение осуществляемой в рамках ООН деятельности по выработке правил, норм и принципов ответственного поведения государств в информационном пространстве. Государства-члены убеждены в необходимости продолжить совместную работу и координацию усилий ОДКБ в рамках единого переговорного механизма под эгидой ООН – Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий. Государства – члены ОДКБ в рамках международного сотрудничества выражают готовность к распространению своего передового опыта в этой сфере»[1].

В данном контексте следует отметить активную позицию ОДКБ по разработке правовых инициатив в сфере МИБ для

[1] Заявление министров иностранных дел государств – членов ОДКБ о координации совместных усилий в сфере информационной безопасности, включая противодействие использованию информационно-коммуникационных технологий в террористических и других преступных целях, от 15 сентября 2021 г. // Официальный сайт ОДКБ. URL: https://odkb-csto.org/documents/statements/zayavlenie-ministrov-inostrannykh-del-gosudarstv-chle-nov-odkb-o-koordinatsii-sovmestnykh-usiliy-v-sf/?#loaded.

представления и обсуждения на площадке ООН. Так, 17 декабря 2018 г. Генеральная Ассамблея ООН большинством голосов приняла российскую резолюцию «Противодействие использованию информационно-коммуникационных технологий в преступных целях», соавторами которой выступили партнеры России по ОДКБ. Резолюция была поддержана большинством голосов[1].

Развивая коллективную региональную стратегию МИБ, государства – члены ОДКБ уделяют должное внимание противодействию преступлениям в сфере ИКТ.

В настоящее время в формате ОДКБ активно действуют механизмы практического взаимодействия в указанной области, среди которых следует отметить:

– Протокол о взаимодействии государств – членов ОДКБ по противодействию преступной деятельности в информационной сфере, который содействует сотрудничеству специальных подразделений органов безопасности и внутренних дел в ходе расследования соответствующих преступлений[2], вступивший в силу и подписанный в 2014 г.;

– операция постоянного действия «ПРОКСИ» (от полного названия «противодействие криминалу в сфере информации») в формате ОДКБ, проводимая с 2009 г. В ее рамках реализуются скоординированные мероприятия по противодействию преступности в сфере информационных технологий. В пределах своей компетенции в ней участвуют специальные подразделения органов национальной безопасности, внутренних дел (по-

[1] В ходе голосования США и страны ЕС наглядно продемонстрировали, что не намерены выносить тему МИБ на площадку ООН. Их стратегическая задача по-прежнему состоит в поддержании выгодного для них статус-кво в международном информационном пространстве, нацеленного на сохранение цифрового неравенства между различными членами мирового сообщества.

[2] Протокол о взаимодействии государств – членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере от 23 декабря 2014 г. // Официальный сайт ОДКБ. URL: https://odkb-csto.org/documents/documents/pravovaya_baza_odkb/#-loaded.

лиции), подразделения по борьбе с незаконным оборотом наркотиков, с незаконной миграцией, структуры органов финансовой мониторинга (разведки) государств – членов ОДКБ;

– Консультационный координационный центр по реагированию на компьютерные инциденты (ККЦ ОДКБ) в формате Организации по решению глав государств – членов ОДКБ, созданный в 2014 г. Осуществляется деятельность по отражению масштабных компьютерных атак, пресечению распространения вредоносного программного обеспечения и противодействию другим типам противоправной активности в информационном пространстве государств – членов ОДКБ.

Как отметил в своем выступлении заместитель Генерального секретаря ОДКБ В. А. Семериков на неформальной межсессионной встрече Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования ИКТ (РГОС), опыт ОДКБ в части работы Консультационного координационного центра по реагированию на компьютерные инциденты может стать эффективным региональным вкладом в деятельность РГОС[1].

Одной из основных задач Центра является организация взаимодействия уполномоченных органов, в том числе сбора и обмена информацией, при реагировании на компьютерные инциденты в информационных пространствах государств – членов ОДКБ.

В этих целях разработан регламент информационного взаимодействия контактных пунктов ККЦ ОДКБ, который предназначен для формализации процессов сбора и обмена информа-

[1] Выступление заместителя Генерального секретаря ОДКБ В. Семерикова на неформальной межсессионной встрече Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования информационно-коммуникационных технологий от 7 декабря 2022 г. // Официальный сайт ОДКБ. URL: https://odkb-csto.org/news/news_odkb/vystuplenie-zamestite-lya-generalnogo-sekretarya-odkb-valeriya-semerikova-na-neformal-noy-mezhsessionn-/#loaded.

цией по компьютерным инцидентам между уполномоченными органами в рамках информационно-технического взаимодействия контактных пунктов ККЦ ОДКБ. Указанный документ определяет основные направления и формы сотрудничества государств, в том числе при оказании взаимной помощи, а также порядок действий контактных пунктов в случае возникновения компьютерных инцидентов.

По мнению В. А. Семерикова, принятый на международном уровне аналогичный инструмент позволит унифицировать взаимодействие государств – членов ООН в области безопасности при использовании ИКТ и самих ИКТ, а также избегать политизации технических по своему происхождению вопросов реагирования на компьютерные инциденты. Согласованный порядок будет способствовать налаживанию диалога между техническими специалистами, что в конечном счете приведет к снижению напряженности и недоверия в глобальном информационном пространстве.

За последние годы результаты профильной операции под эгидой ОДКБ в сфере МИБ и противодействия использованию ИКТ в преступных целях «ПРОКСИ» свидетельствуют, что информационная среда остается уязвимой для террористического, экстремистского воздействия и иных неправомерных целей, включая распространение информации для подрыва конституционного строя, разжигания межнациональной и религиозной розни и активно используется в указанных целях на фоне значимых политических событий[1].

[1] Заявление министров иностранных дел государств – членов ОДКБ о координации совместных усилий в сфере информационной безопасности, включая противодействие использованию информационно-коммуникационных технологий в террористических и других преступных целях, от 15 сентября 2021 г. // Официальный сайт ОДКБ. URL: https://odkb-csto.org/documents/-statements/-zayavlenie-ministrov-inostrannykh-del-gosudarstv-chle-nov-odkb-o-koordinatsii-sovmestnykh-usiliy-v-sf/?#loaded.

К приоритетным направлениям сотрудничества государств – членов ОДКБ при проведении операции «ПРОКСИ» относятся:

– противодействие деятельности, посягающей на основы конституционного строя и безопасности государства;

– обмен информацией и проведение совместных мероприятий по противодействию противоправной деятельности международных хакерских групп, причастных к разработке программного обеспечения, предназначенного для неправомерного доступа к компьютерной информации, а также привлечению к ответственности администраторов криминальных сетевых ресурсов;

– противодействие противоправной деятельности по незаконному обороту наркотиков и использованию сети Интернет для наркоторговли и наркотрафика;

– противодействие террористической и экстремистской деятельности, осуществляемой с использованием ИКТ[1].

Таким образом, операция «ПРОКСИ» является действенным инструментом коллективного сотрудничества государств – членов ОДКБ, поскольку совместные действия в рамках данной операции по противодействию использования сферы информационных технологий в преступных целях способствуют укреплению коллективной безопасности государств – членов ОДКБ.

Развивая свои коллективные правовые основы, государства – члены ОДКБ заявляют о приверженности разработке под эгидой ООН конвенции по противодействию использованию ИКТ в преступных целях в соответствии с профильной резолюцией Генассамблеи ООН[2].

---

[1] Руководители национальных штабов государств – членов ОДКБ по проведению операции «ПРОКСИ» обсудили обеспечение информационной безопасности // Официальный сайт ОДКБ. URL: https://odkb-csto.org/news/-news_odkb/rukovoditeli-natsionalnykh-shtabov-gosudarstv-chlenov-odkb-po-provede-niyu-operatsii-proksi-obsudili/#loaded.

[2] Заявление министров иностранных дел государств – членов ОДКБ о координации совместных усилий в сфере информационной безопасности.

Выражая обеспокоенность в связи с использованием ИКТ в целях, подрывающих усилия по поддержанию международного и регионального мира, безопасности и стабильности, государства – члены ОДКБ сформировали следующие перспективы координации совместных усилий в сфере информационной безопасности, включая противодействие использованию ИКТ в террористических и других преступных целях:

– совершенствование механизмов и мер по предотвращению конфликтов, которые могут возникнуть в том числе как следствие противоправного использования ИКТ, а также преодолению дефицита доверия между сторонами конфликтов;

– усиление координации дальнейших совместных мер в борьбе с использованием ИКТ в террористических и других преступных целях, тесное взаимодействие, в том числе обмен положительным опытом и практиками противодействия угрозам международного терроризма в сфере использования ИКТ в террористических и других преступных целях, как на региональном, так и на международном уровне;

– укрепление сотрудничества в области обеспечения МИБ с акцентом на практической составляющей взаимодействия – проведение совместных операций постоянного действия ОДКБ по противодействию преступлениям в сфере ИТ «ПРОКСИ», а также мероприятий по реагированию на компьютерные инциденты;

– разработка правовых и технических основ по защите цифрового суверенитета государств – членов ОДКБ от существующих и потенциальных угроз, принятие необходимых мер по предотвращению применения ИКТ для вмешательства во внутренние дела суверенных государств, любых посягательств на территориальную целостность, государственный суверенитет и независимость государств – членов Организации, а также в иных деструктивных целях;

– поддержка усилий ООН в противодействии угрозам в сфере использования ИКТ и приверженность формированию

под эгидой ООН правил, норм и принципов ответственного поведения государств в информационном пространстве, а также правовых основ по противодействию использованию ИКТ в преступных целях;

– активизация совместной работы по совершенствованию механизма взаимодействия в обеспечении информационной безопасности на основе Соглашения о сотрудничестве государств – членов ОДКБ в области обеспечения информационной безопасности;

– дальнейшее развитие отношений со стратегическим партнерами, в первую очередь с государствами, входящими в ШОС, СНГ и БРИКС, для повышения эффективной деятельности международных и региональных организаций в сфере борьбы с использованием ИКТ в террористических и других преступных целях.

Последний аспект в развитии перспектив сотрудничества государств – членов ОДКБ в сфере информационной безопасности, включая противодействие использованию ИКТ в террористических и других преступных целях, в настоящее время чрезмерно актуален. Безусловно, важным ресурсом укрепления сотрудничества ОДКБ в сфере информационной безопасности является привлечение к совместной работе государств – наблюдателей и партнеров по диалогу, углубление контактов с заинтересованными странами и международными организациями, в первую очередь с государствами, входящими в ШОС, СНГ и БРИКС.

Как справедливо отмечено в Заявлении министров иностранных дел государств – членов Организации Договора о коллективной безопасности по случаю 30-летия Содружества Независимых Государств и 20-летия Шанхайской организации сотрудничества от 15 сентября 2021 г., чрезвычайно важно «…дальнейшее продолжение налаженной за годы нашего взаимодействия практики поддержки инициатив друг друга в рам-

ках международных структур …и координировать действия ОДКБ, СНГ и ШОС в русле подлинного и эффективного партнерства в продвижении взаимовыгодных интересов государств-участников на международных площадках»[1].

Практическим примером такого трехстороннего взаимодействия является проведенная в Секретариате ОДКБ в феврале 2022 г. трехсторонняя встреча, посвященная укреплению взаимодействия и обмену опытом борьбы с международным терроризмом и экстремизмом, в которой приняли участие Генеральный секретарь ОДКБ, директор Исполнительного комитета Региональной антитеррористической структуры ШОС и руководитель АТЦ СНГ[2].

Важность взаимодействия по информационной безопасности в СНГ, ШОС и ОДКБ была обозначена в Совместном заявлении Президента Российской Федерации В. В. Путина и Президента Киргизской Республики С. Н. Жапарова о сотрудничестве в области обеспечения международной информационной безопасности, принятого 9 декабря 2022 г. по итогам проведенного заседания Высшего Евразийского экономического совета в г. Бишкеке (Киргизская Республика). В частности, в заявлении отмечено: «Главы государств приветствуют прогресс, достигнутый государствами – участниками Содружества Независимых Государств, государствами – членами Организации Договора о коллективной безопасности и Шанхайской организации со-

[1] Заявление министров иностранных дел государств – членов Организации Договора о коллективной безопасности по случаю 30-летия Содружества Независимых Государств и 20-летия Шанхайской организации сотрудничества // Официальный сайт ОДКБ. URL: https://odkb-csto.org/documents/statements/-sovmestnoe-zayavlenie-gosudarstv-chlenov-organizatsii-dogovora-o-kollektivnoy-bezopasnosti-k-30-leti/#loaded.

[2] Выступление Генерального секретаря ОДКБ С. В. Зася на заседании Совета Безопасности ООН 16 февраля 2022 г. // Официальный сайт ОДКБ. URL: https://odkb-csto.org/news/speech/vystup-lenie-generalnogo-sekretarya-odkb-s-v-zasya-na-zasedanii-so-veta-bezopasnosti-oon-16-fevralya-2/?sphrase_id=74393#loaded.

трудничества в углублении сотрудничества в области международной информационной безопасности, и признают необходимость наращивания практического взаимодействия в этих региональных форматах на основе имеющихся договоренностей»[1].

В свете проведенного анализа в качестве перспективы представляется необходимым инициировать участие, в первую очередь, государств – участников СНГ, не входящих в ОДКБ, в реализации операций «ПРОКСИ». ОДКБ не только располагает наработанными практиками взаимодействия государств – членов Организации по противодействию преступной деятельности в информационной сфере, но и готова делиться опытом проведения таких специальных оперативно-профилактических операций. Данный подход определяет позицию ОДКБ в привлечении международных и региональных организаций, отдельных государств не только к наблюдению за ходом проводимых учений и операций, но и к участию в них. Механизмы взаимодействия и партнерства, наработанные в ОДКБ, позволяют это сделать.

Кроме того, перспектива видится в дальнейшем укреплении сотрудничества с государствами – членами ШОС, БРИКС, СНГ, не входящими в ОДКБ, в целях продвижения инициатив и концепций Российской Федерации на универсальном уровне под эгидой ООН.

[1] Совместное заявление Президента Российской Федерации В. В. Путина и Президента Киргизской Республики С. Н. Жапарова о сотрудничестве в области обеспечения международной информационной безопасности от 9 декабря 2022 г. // Официальный сайт Президента Российской Федерации. URL: http://www.kremlin.ru/supplement/5878.

§ 3.5. Двусторонние форматы взаимодействия Российской Федерации со стратегическими партнерами по вопросам противодействия угрозе использования информационно-коммуникационных технологий в преступных целях

Помимо межгосударственного сотрудничества в рамках различных международных организаций предусмотрен формат двустороннего взаимодействия государств по различным аспектам информационной безопасности. В рамках проведенного исследования был изучен официальный сайт МИД России на предмет выявления двусторонних договоров Российской Федерации с другими государствами по вопросам противодействие преступлениям в сфере ИКТ. Анализ позволил установить наличие двусторонних межправительственных соглашений о сотрудничестве в области обеспечения МИБ, частью которых являются положения о противодействии использования ИКТ в преступных целях. В частности, такие договоры подписаны от имени Правительства Российской Федерации с правительствами следующих государств: Бразилии, Белоруссии, Кубы, Китая,

Индии, ЮАР, Вьетнама, Ирана, Киргизии, Никарагуа, Узбекистана, Азербайджана, Армении[1].

Двусторонние международные межправительственные соглашения Российской Федерации в исследуемой области имеют сходное содержание. Среди общих принципиальных и практически значимых моментов рассматриваемых двусторонних

[1] Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности 2015 г. ; Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилия о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности 2010 г. ; Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности 2013 г. ; Соглашение между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности от 2014 г. ; Соглашение между Правительством Российской Федерации и Правительством Республики Индия о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий 2016 г. ; Соглашение между Правительством Российской Федерации и Правительством Южно-Африканской Республики о сотрудничестве в области обеспечения международной информационной безопасности 2017 г. ; Соглашение между Правительством Российской Федерации и Правительством Социалистической Республики Вьетнам о сотрудничестве в области обеспечения международной информационной безопасности 2018 г. ; Соглашение между Правительством Российской Федерации и Правительством Исламской Республики Иран о сотрудничестве в области обеспечения информационной безопасности 2021 г. ; Соглашение между Правительством Российской Федерации и Правительством Киргизской Республики о сотрудничестве в области обеспечения международной информационной безопасности 2021 г. ; Соглашение между Правительством Российской Федерации и Правительством Республики Никарагуа о сотрудничестве в области обеспечении международной информационной безопасности 2021 г. ; Соглашение между Правительством Российской Федерации и Правительством Республики Узбекистан о сотрудничестве в области обеспечения международной информационной безопасности 2021 г. ; Соглашение между Правительством Российской Федерации и Правительством Республики Армения о сотрудничестве в области обеспечения информационной безопасности 2022 г. ; Соглашение между Правительством Российской Федерации и Правительством Азербайджанской Республики о сотрудничестве в области обеспечения международной информационной безопасности 2022 г.

международно-правовых актов представляется целесообразным выделить следующее:

– основаны на общепризнанных принципах и нормах международного права;

– закрепляют ключевые аспекты внешнеполитической позиции России по информационной безопасности и противодействию преступлениям в сфере информационных технологий;

– предусматривают обязательство воздержаться от кибератак в двусторонних отношениях;

– фиксируют право на защиту информационных ресурсов государства от неправомерного использования и несанкционированного воздействия, в том числе от компьютерных атак на них;

– позволяют обеспечить формирование взаимного доверия.

Таким образом, двусторонние международные договоры Российской Федерации по вопросам обеспечения информационной безопасности и противодействия преступлениям в сфере информационных технологий не закрепляют инновационных подходов к международно-правовому регулированию рассматриваемой сферы, однако имеют особое значение для развития партнерских отношений между Россией и зарубежными государствами.

В контексте развития международного сотрудничества в борьбе с преступлениями в сфере ИТ отдельного внимания заслуживает налаживание двустороннего транснационального взаимодействия в отдельных областях правоохранительной деятельности. Так, 12 октября 2017 г. подписано Соглашение о сотрудничестве между Министерством внутренних дел Российской Федерации и Государственным комитетом судебных

экспертиз Республики Беларусь в сфере судебно-экспертной деятельности[1].

Указанный международный договор разработан МВД России во взаимодействии с Государственным комитетом судебных экспертиз Республики Беларусь в целях формирования двусторонней международно-правовой основы сотрудничества в сфере судебно-экспертной деятельности. Соглашение направлено на развитие межведомственного сотрудничества в области проведения научных исследований в сфере судебно-экспертной деятельности, научно-методического обеспечения производства судебных экспертиз и экспертных исследований, оказания практической и методической помощи, в том числе обмена опытом с учетом экспертной практики. Международное сотрудничество на основании рассматриваемого международного договора предусматривает осуществление сторонами непосредственно, а также через Федеральное государственное казенное учреждение «Экспертно-криминалистический центр Министерства внутренних дел Российской Федерации» и Государственное учреждение «Научно-практический центр Государственного комитета судебных экспертиз Республики Беларусь».

[1] В Минске подписано Соглашение о сотрудничестве между Министерством внутренних дел Российской Федерации и Государственным комитетом судебных экспертиз Республики Беларусь в сфере судебно-экспертной деятельности // Официальный сайт МВД России. URL: https://xn--b1aew.xn--p1ai/mvd/-struc-ture1/Centri/JEkspertno_krimina-listicheskij_centr/Publikacii_-i_vis-tup-lenija/item/11329811/.

ГЛАВА IV
Исследование проблем информационного обмена между МВД России и правоохранительными органами иностранных государств, а также механизмов обмена информацией в рамках расследования преступлений в сфере компьютерной информации между государствами

§ 4.1. Актуальные теоретико-правовые вопросы расследования преступлений в сфере информационно-коммуникационных технологий и использования информационно-коммуникационных технологий в процессе доказывания

В Российской Федерации, как и во многих государствах, уголовное и уголовно-процессуальное законодательство ориентировано на реализацию расследования преступлений, совершаемых в сфере информационных технологий, использования информационных технологий в процессе доказывания преступлений, а также решения процедурных вопросов в суде.

Следует отметить, что законодательством Российской Федерации термины «цифровое доказательство» и «электронное доказательство» не предусмотрены. Такое же положение присутствует во многих уголовных и уголовно-процессуальных нормативных актах различных государствах: Китая, Швейцарии, Франции, Великобритании, Австралии. Однако это не препятствует в получении значимой для расследования информации с использованием информационных технологий, поскольку допустимость доказательств, полученных с использованием

информационных технологий, регулируется общими положениями в отношении традиционных доказательств.

Положения УПК РФ допускают сбор и использование в доказывании сведений, содержащихся на электронных носителях, которые могут признаваться электронными (цифровыми) доказательствами.

В соответствии с ч. 1 ст. 74 УПК РФ доказательством по уголовному делу являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель в порядке, определенном УПК РФ, устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела.

Согласно ч. 2 ст. 74 УПК РФ в качестве доказательств допускаются вещественные доказательства (п. 4), протоколы следственных и судебных действий (п. 5), иные документы (п. 6).

Иные документы могут содержать сведения, зафиксированные как в письменном, так и в ином виде (ч. 2 ст. 84 УПК РФ). Указанной нормой не ограничивается вид носителя информации, на котором может содержаться иной документ.

В соответствии с ч. 4 ст. 84 УПК РФ документы, обладающие признаками, указанными в ч. 1 ст. 81 УПК РФ, признаются вещественными доказательствами. Следовательно, УПК РФ не исключает использование в доказывании информации, содержащейся на электронных носителях.

Частью 8 ст. 166 УПК РФ к протоколу следственного действия допускается приложение электронных носителей[1] ин-

[1] Электронный носитель – материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники (п. 3.1.9 ГОСТ 22.051–2013 «ЕСКД. Электронные документы. Общие положения», введенного приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2013 г. № 1628-ст).

формации, полученной или скопированной с других носителей информации в ходе производства следственного действия.

Таким образом, порядок сбора и использования следователем (дознавателем) в доказывании сведений, содержащихся на электронных носителях информации (электронных (цифровых) доказательств), в достаточной степени определен действующим уголовно-процессуальным законодательством Российской Федерации.

Изложенное позволяет констатировать общность подходов многих государств в части внедрения новых технологий в сферу уголовного судопроизводства, использования данных технологий в процессе доказывания обстоятельств совершения преступления при отсутствии на законодательном уровне понятия «электронное доказательство» и фактического употребления данного термина применительно к способу получения электронной информации. При этом допустимость доказательств, полученных с использованием информационных технологий, регулируется общими положениями, касающимися традиционных доказательств. Конкретные национальные правила, связанные с допустимостью доказательств, полученных таким способом, отсутствуют.

Вместе с тем в последнее время эксперты и специалисты все чаще высказывают позицию о целесообразности закрепления в УПК РФ понятий «электронное доказательство»[1], «электронный документ»[2].

---

[1] Информационно-аналитические материалы по вопросам целесообразности совершенствования законодательства, затрагивающего вопрос противодействия преступлениям в сфере ИКТ, в том числе на основе положительного международного опыта (в частности, закрепления понятия «электронное доказательство», способов их получения и использования в процессуальной и оперативно-разыскной деятельности).

[2] Информационно-справочные материалы по исполнению подпункта 1.2 постановления Координационного совещания руководителей правоохранительных органов Российской Федерации от 17 июля 2020 г. № 1.

Такая позиция подкрепляется практическими проблемами раскрытия преступлений в сфере ИКТ, в частности с использованием криптовалют. Отмечается, что доказательственной базой по результатам мониторинга транзакций с криптовалютой, анализа и выявления признаков, указывающих на преступную составляющую сделки, являются исключительно электронные доказательства, использование которых пока еще недостаточно регламентировано. Данная ситуация требует правового разрешения посредством внесения изменений в ст. 74 УПК РФ в части закрепления понятия «электронное доказательство»[1] и возможной разработки криминалистической методики сбора электронных доказательств.

Кроме того, изменения, связанные с процессом цифровизации, диктуют необходимость соответствующей разработки уголовно-процессуальных норм, регламентирующих копирование, изъятие, сохранение, обработку, передачу, а также представление в суд цифровой информации, имеющей доказательственное значение. Также необходимо учитывать, что электронные доказательства легко подвергаются изменениям и уничтожению, поэтому на законодательном уровне необходимо предусмотреть надежные гарантии подлинности электронно-цифровых документов, которыми могут быть, в частности: запрет на изменение электронной информации, используемой в доказывании по уголовному делу; доступность электронных цифровых документов для последующего изучения и использования в процессе доказывания; обеспечение хранения в неизменном виде.

---

[1] Ряд специалистов предлагают следующую формулировку понятия «электронные доказательства» – это электронный носитель информации, содержащий сведения об обстоятельствах, подлежащих доказыванию по конкретному уголовному делу и обладающий значительным объемом памяти, простотой передачи и копирования сведений с одного носителя на другой, возможностью удаленного доступа к содержанию электронного носителя и телекоммуникационным системам, полученный в порядке, установленном уголовно-процессуальным кодексом Российской Федерации.

Проблематика «электронного документа», безусловно, в самое ближайшее время станет также актуальной ввиду тенденций развития института правовой помощи по уголовным делам и совершенствования организации взаимодействия с компетентными органами иностранных государств в данной сфере посредством электронных каналов связи.

Следует отметить, что уголовно-процессуальное законодательство Российской Федерации не содержит дефиницию «электронного документа», раскрывая в ст. 474.1 сферу применения в отношении формы подачи процессуальных документов, рассмотрения дела с использованием документов в электронном виде, изготовления и направления судебных актов, т. е. характеризуя действия, совершаемые в пределах национальной системы электронного взаимодействия. В то же время в соответствии с п. 1 постановления Пленума Верховного Суда Российской Федерации от 26 декабря 2017 г. № 57 под электронным документом понимается документ, созданный без предварительного документирования на бумажном носителе и подписанный электронной подписью. Отметим, что Верховный Суд Российской Федерации объединяет понятия «электронный документ» и «электронный образ документа» (т. е. электронная копия бумажного документа, заверенная электронной подписью) в понятие «документ в электронном виде», что представляется обоснованным[1].

Направление запросов о правовой помощи по уголовным делам в электронном виде не противоречит, например, Конвенции о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам от 22 января 1993 г., Европейской конвенции о взаимной правовой помощи по уголовным

[1] Справка по вопросу о сокращении сроков рассмотрения запросов о правовой помощи, в том числе путем организации взаимодействия с компетентными органами государств – участников СНГ (по пересылке запросов и исполнениях материалов запросов) в электронном виде.

делам от 20 апреля 1959 г. с учетом Второго дополнительного протокола от 8 ноября 2001 г.

Двусторонние договоры Российской Федерации о взаимной правовой помощи по уголовным делам, например Договор между Российской Федерацией и Объединенными Арабскими Эмиратами о взаимной правовой помощи по уголовным делам от 25 ноября 2014 г., Конвенция между Российской Федерацией и Алжирской Народной Демократической Республикой о взаимной правовой помощи по уголовным делам от 10 октября 2017 г., прямо предусматривают в случаях, не терпящих отлагательства, возможность направления копии запроса любым способом связи, позволяющим обеспечить письменную передачу информации в целях его исполнения. Однако в силу положений рассматриваемых международных договоров в последующем необходимо направление запросов адресатам на бумажном носителе.

Таким образом, организация направления запросов о правовой помощи и материалов исполненных запросов в электронном виде с учетом определенных организационно-правовых и технических особенностей реализации данного процесса представляется возможной и перспективной. При этом основными задачами при создании соответствующего электронного канала связи являются:

– обеспечение конфиденциальности передаваемой информации и защиты персональных данных всех субъектов, чьи данные направляются;

– верификация и аутентификация передающей стороны и передаваемых документов;

– предотвращение неправомерного доступа к информации;

– возможность использования электронной подписи, порядок ее признания на территории иностранного государства;

– функциональная совместимость браузеров при создании электронной платформы для направления запросов о правовой

помощи и материалов исполненных запросов, а также обмена иной информацией.

Как отмечают эксперты, разрешать вопросы организации обмена электронными документами при оказании правовой помощи допустимо следующими путями:

– заключение международных договоров или внесение изменений в действующие двусторонние и многосторонние договоры Российской Федерации;

– принятие модельных законов, которые содержат положения рекомендательного характера, адресованные государствам – участникам международной организации, направленные на гармонизацию национального законодательства.

В рамках взаимодействия государств – участников СНГ начата работа по созданию единой платформы для обмена правовой информацией в сфере осуществления уголовного судопроизводства. На данный момент уже действует постановление от 25 ноября 2016 г. № 45-13 Межпарламентской ассамблеи государств – участников СНГ «О модельном законе “О трансграничном информационном обмене электронными документами”»[1], которым принят одноименный модельный закон. Закон раскрывает термины «электронный документ», «интеграционная платформа», «электронный вид информации», «юридическая сила электронного документа» и ряд других. Кроме того, модельным законом регламентирован механизм фактической реализации трансграничного электронного документооборота за счет создания государствами – участниками СНГ специального Межгосударственного координирующего органа для формирования и обеспечения функционирования трансграничного

[1] Постановление Межпарламентской ассамблеи государств – участников Содружества Независимых Государств от 25 ноября 2016 г. № 45-13 «О модельном законе “О трансграничном информационном обмене электронными документами”» // Информационная система «Континент». URL: http://continent-online.com/-Document/?doc_id=37590479.

пространства доверия; обеспечение трансграничного электронного документооборота за счет создания межгосударственной информационной системы государств – участников СНГ на основе применения службы доверенной третьей стороны, организуемой на уровне каждого государства, а также в Межгосударственном координирующем органе а также определены требования, предъявляемые к электронному документу, и предусмотрены вопросы защиты информации.

Не менее актуальным вопросом является возможность использования информационных технологий в ходе досудебного и судебного производства по уголовным делам. Как справедливо отмечают эксперты, такая возможность создает дополнительные предпосылки для процессуальной экономии, снижения рисков фальсификаций доказательств, облегчения процедуры направления участникам уголовного процесса документов, ознакомления их с материалами уголовного дела, что, безусловно, способствует соблюдению принципа разумного срока уголовного судопроизводства и обеспечению защиты прав, свобод и интересов участников процесса.

В настоящее время с учетом зарубежного опыта уголовного судопроизводства в электронном формате проработка указанного вопроса постоянно осуществляется в Российской Федерации на межведомственном уровне. МВД России поддержаны идеи совершенствования судебного производства и высказаны предложения о проработке в рамках дорожной карты вопроса цифровизации судебного и досудебного производства по уголовным делам.

Анализ предложений профильных ведомств по внесению изменений в действующее законодательство Российской Федерации позволяет выделить следующие ключевые направления:

1. Закрепление в ст. 5 УПК РФ среди базовых понятий таких дефиниций, как «электронное информирование», «видеоконференц-связь», «электронный документ»[1].

2. Разработка порядка проведения допроса, очной ставки и опознания путем использования систем видеоконференц-связи[2].

3. Установление возможности уведомления участников уголовного судопроизводства о принятых процессуальных решениях и вызова для производства процессуальных действий с использованием дистанционных технологий, а также ознакомления их с копиями материалов уголовного дела, содержащимися на электронных носителях, вручения копии обвинительного заключения, обвинительного акта или обвинительного постановления в электронном виде[3].

4. Проработка возможности унификации правил дистанционного получения информации о начавшемся судебном процессе (судебные извещения), дистанционного доступа к материалам электронных дел, включая получение судебных актов или их копий в электронном виде, дистанционного участия в судебных заседаниях[4].

---

[1] Информационно-справочные материалы по исполнению подпункта 1.2 постановления Координационного совещания…

[2] Федеральный закон от 30 декабря 2021 г. № 501-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&rnd=lJ6u8w&base=LAW&n=405493#P08EU3TERZdngLGW1.

[3] Решение коллегии Министерства внутренних дел Российской Федерации от 28 мая 2021 г. № 2 км «О состоянии и мерах по повышению эффективности и качества предварительного следствия в органах внутренних дел», объявленное приказом МВД России от 15 июня 2021 г. № 447 // СПС «КонсультантПлюс». URL: http://www.consultant.ru.

[4] Дорожная карта реализации целевой модели суперсервиса «Правосудие онлайн» федерального проекта «Цифровое государственное управление» национальной программы «Цифровая экономика Российской Федерации», утвержденной протоколом Президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 21 сентября 2020 г. № 20.

Как уже отмечалось, применение ИКТ при совершении преступлений осложняет их выявление, пресечение, расследование и раскрытие, что обусловливает необходимость внедрения новых правовых, криминалистических и организационных механизмов и средств. Развитие понятия «электронное доказательство», совершенствование законодательства, регулирующего получение, хранение и представление в суде этих доказательств, будет способствовать развитию новой уголовно-процессуальной информационной технологии, отвечающей современным реалиям и требованиям противодействия преступлениям в сфере ИКТ.

Перспективным направлением совершенствования правоохранительного сотрудничества исполнительных и судебных органов власти Российской Федерации с компетентных органами зарубежных государств выступает организация электронного документооборота в области уголовного судопроизводства, которая повлечет за собой трансформацию национального законодательства государств, заинтересованных в создании подобного международного пространства взаимодействия.

Кроме того, в настоящее время действующее уголовно-процессуальное законодательство Российской Федерации нуждается в совершенствовании в части вопроса «цифровизации» судебного и досудебного производства по уголовным делам. Указанные обстоятельства актуализируют дальнейшую комплексную работу сформированных межведомственных рабочих групп по подготовке проекта федерального закона о внесении изменений в Уголовно-процессуальный кодекс Российской Федерации в части регулирования вопросов дистанционного участия в уголовном процессе.

§ 4.2. Международно-правовые основы сотрудничества государств – участников Содружества Независимых Государств в сфере информационного взаимодействия и обмена информацией в электронном виде

Одной из наиболее значимых перспектив совершенствования работы правоохранительных органов по противодействию преступлениям в сфере информационно-коммуникационных технологий выступает внедрение технических и оперативных инноваций в практическую деятельность сотрудников различных подразделений. В частности, большое значение для МВД России имеет развитие возможностей обмена данными в электронном виде с правоохранительными органами зарубежных государств, в первую очередь по линии СНГ.

Основным механизмом сотрудничества государств – участников СНГ в сфере информационного взаимодействия является Межгосударственный информационный банк (далее – Банк), функционирующий в соответствии с Соглашением о взаимоотношениях министерств внутренних дел в сфере обмена информацией от 3 августа 1992 г. (далее – Соглашение 1992 г.) и Соглашением об обмене информацией в сфере борьбы с преступностью от 22 мая 2009 г. (далее – Соглашение 2009 г.).

Статьей 5 Соглашения 1992 г. и ст. 8 Соглашения 2009 г. предусмотрено, что держателем Банка является МВД России. Компетентным подразделением по данному вопросу выступает ФКУ «ГИАЦ МВД России», который обеспечивает обработку, хранение и выдачу по запросам органов внутренних дел государств – участников СНГ имеющейся в Банке информации, а также статистических сведений о состоянии преступности и результатах расследований преступлений; осуществляет с помощью разыскных учетов информационное обеспечение деятельности по розыску лиц, объявленных компетентными

органами государств – участников СНГ в межгосударственный розыск; сотрудничает с компетентными органами государств – участников СНГ по вопросам компьютеризации, совершенствования программного и информационного обеспечения, создания единой автоматизированной системы передачи данных.

С учетом роста современных угроз со стороны транснациональной преступности в информационно-коммуникационной сфере совершенствование порядка обмена информацией между государствами – участниками СНГ имеет большое значение для повышения эффективности международного сотрудничества по вопросам, относящимся к компетенции органов внутренних дел. В настоящее время между государствами – участниками СНГ проводится работа по заключению двусторонних международных договоров, регламентирующих вопросы сотрудничества между органами внутренних дел по вопросам информационного взаимодействия и обмена информацией в электронном виде. В частности, следует отметить Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел, от 13 декабря 2018 г. (Далее – Соглашение с Беларусью 2018 г.), а также аналогичные межправительственные договоры, подписанные Российской Федерацией с Республикой Узбекистан (15 декабря 2020 г.)[1] и Республикой Армения (13 мая 2021 г.)[2]. Отметим не менее

[1] Соглашение между Правительством Российской Федерации и Правительством Республики Узбекистан об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел, от 15 декабря 2020 г. не вступило в силу. Далее – Соглашение с Узбекистаном 2020 г.

[2] Соглашение между Правительством Российской Федерации и Правительством Республики Армения об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел Российской Федерации и Полиции Республики Армения, от 13 мая 2021 г. не вступило в силу. Далее – Соглашение с Арменией 2021 г.

важное для Российской Федерации Соглашение между Правительством Российской Федерации и Правительством Республики Южная Осетия об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел (10 ноября 2019 г.).

Данные соглашения допустимо назвать типовыми договорами об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел. Вместе с тем, несмотря на их внешнюю схожесть в содержательном аспекте, по тексту имеются некоторые разночтения и правовые нюансы.

Анализ соглашений с Беларусью 2018 г., Узбекистаном 2020 г., Арменией 2021 г. позволяет прийти к следующим выводам.

Преамбулы во всех обозначенных договорах идентичны и содержат следующее положение: «Правительство Российской Федерации и Правительство… (соответствующего государства), руководствуясь общепризнанными принципами и нормами международного права, желая развивать сотрудничество между компетентными органами государств Сторон по вопросам информационного взаимодействия и обмена информацией в электронном виде, согласились о нижеследующем…».

Содержание норм относительно предмета договора несколько отличается. Так, ст. 1 Соглашения с Узбекистаном 2020 г. и ст. 1 Соглашения с Арменией 2021 г. содержат полностью идентичные нормы, позволяющие отметить следующее:

– предметом соглашений выступает информационное взаимодействие в электронном виде в рамках действующих в отношениях между Российской Федерацией и Республикой Узбекистан / Армения международных договоров, компетентными органами по выполнению которых определены Министерство внутренних дел Российской Федерации и Министерство внут-

ренних дел Республики Узбекистан / Полиция Республики Армения;

– в рамках соглашений не осуществляется обмен информацией, составляющей государственную тайну государств-Сторон;

– взаимный обмен информацией в электронном виде осуществляется с использованием информационных систем, программно-технических средств и (или) за счет доступа компетентного органа государства – другой Стороны к ресурсам информационных систем, находящихся в ведении компетентных органов государств-Сторон (далее – информационные системы);

– компетентные органы государств-Сторон обязуются содействовать обеспечению безопасности, полноты и достоверности информации, находящейся в информационных системах;

– правовой основой информационного взаимодействия между компетентными органами государств-Сторон выступают настоящие Соглашения, технические протоколы, национальное законодательство государств-Сторон и международные договоры, участниками которых являются их государства.

Представляет интерес содержание ст. 1 Соглашения с Республикой Беларусь 2018 г., согласно которой предметом договора выступает не только информационное взаимодействие, но и правовое регулирование при обмене информацией в электронном виде, включая персональные данные. Остальные положения данной статьи идентичны аналогичным ст. 1 Соглашения с Узбекистаном 2020 г. и Соглашения с Арменией 2021 г.

Положения о компетентных органах государств по реализации анализируемых соглашений содержатся в ст. 2 и носят идентичный характер. Так, компетентным органом от Российской Федерации выступает Министерство внутренних дел Российской Федерации, от компетентных органов Сторон – национальные компетентные органы государств-участников в сфере

внутренних дел. Следует отметить некоторое уточнение из ст. 2 Соглашения с Арменией 2021 г., согласно которому «об изменениях своих компетентных органов каждая из Сторон в течение месяца в письменной форме уведомляет другую Сторону по дипломатическим каналам».

Идентичными по содержанию представляются положения ст. 3 анализируемых соглашений, касающихся технических протоколов с некоторой разницей: в Соглашении с Узбекистаном 2020 г. и Соглашении с Арменией 2021 г. речь идет о двух типах технических протоколов: протоколы информационного взаимодействия и протоколы технологического взаимодействия. В то время как в Соглашении с Беларусью 2018 г. предусмотрено также заключение протокола о защите информации. Вместе с тем, исходя из анализа вопросов, отражаемых в технических протоколах, предусмотренных Соглашением с Узбекистаном 2020 г. и Соглашением с Арменией 2021 г., следует отметить, что по своему содержанию они регламентируют в том числе вопросы защиты информации.

В ст. 4 рассматриваемых соглашений содержатся положения о компетенции (юрисдикции, полномочиях) компетентных органов государств в рамках информационного взаимодействия и обмена информацией в электронном виде. Как представляется, допустимо констатировать, что общее содержание статей идентично за исключением отдельных позиций, приведенных в *прил. 11*. Особенности есть и в Соглашении с Беларусью 2018 г., поскольку, во-первых, предмет договора расширен за счет персональных данных, во-вторых, в самостоятельный технический протокол вынесена проблематика по защите информации. Данные особенности нашли отражение в отдельных формулировках ст. 4 рассматриваемого соглашения.

Положения о хранении и уничтожении информации закреплены в ст. 5 всех трех соглашений и представляются полностью идентичными по своему содержанию: «Хранение и уничтожение

информации осуществляются в соответствии с техническими протоколами, национальным законодательством государств-Сторон и их международными обязательствами, в том числе после прекращения действия настоящего Соглашения. Уничтожение информации из информационных систем осуществляется компетентными органами государств-Сторон, в ведении которых находятся информационные системы».

Ограничения в предоставлении доступа к информации (ст. 6 соглашений) также идентичны: «Компетентный орган государства-Стороны, предоставляющий информацию, имеет право приостанавливать доступ компетентного органа государства-Стороны, получающего информацию, к информационным системам в случаях выявления нарушения требований информационной безопасности и правил работы в информационных системах.

В срок, не превышающий трех рабочих дней со дня выявления причин, препятствующих осуществлению информационного взаимодействия, компетентный орган государства-Стороны, приостановивший доступ, направляет компетентному органу государства – другой Стороны уведомление в письменной форме с указанием причин, даты начала и срока приостановления доступа.

Предоставление информации возобновляется после устранения причин, препятствующих осуществлению информационного взаимодействия».

Вопрос о расходах Сторон при реализации соглашений в целом изложен единообразно в ст. 7 анализируемых соглашений: «Стороны самостоятельно несут расходы по реализации настоящего Соглашения». Вместе с тем допустимы иные формы распределения финансового бремени, «если в каждом конкретном случаен не будет согласован иной порядок» (ст. 7 Соглашения с Арменией 2021 г.).

Правила об изменениях договоров регламентированы идентичными положениями ст. 8: «По согласию Сторон в настоящее Соглашение могут быть внесены изменения, которые оформляются отдельным протоколом, вступающим в силу в порядке, предусмотренном ст. 12 настоящего Соглашения».

При реализации положений анализируемых соглашений рабочим языком является русский язык (ст. 9).

В качестве способов урегулирования споров, возникших между Сторонами в связи с толкованием или применением положений Соглашений, закреплены переговоры и консультации между компетентными органами государств Сторон (ст. 10).

Положения всех трех соглашений не затрагивают прав и обязательств, вытекающих из других международных договоров, участниками которых являются государства-Стороны (ст. 11).

Правила вступления и прекращения соглашений идентичны: «вступают в силу со дня получения по дипломатическим каналам последнего письменного уведомления о выполнении Сторонами внутригосударственных процедур, необходимых для его вступления в силу.

Настоящее Соглашение прекращает свое действие по истечении 6 месяцев с даты получения одной из Сторон письменного уведомления другой Стороны о намерении прекратить действие настоящего Соглашения» (ст. 12).

Анализ заключенных Правительством Российской Федерации двусторонних соглашений об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел, с отдельными государствами – участниками СНГ позволил не только изучить структуру и особенности типовых договоров в данной сфере, но и прийти к выводу, что такие договоры необходимы для эффективной реализации Соглашения о сотрудничестве в борьбе с преступлениями в сфере информационных технологий в рамках СНГ 2018 г.

Кроме того, полагаем, что для полноценной проработки вопросов защиты информации при информационном взаимодействии и обмене информацией в электронном виде МВД России необходимо прорабатывать возможность заключения с государствами – участниками СНГ всех трех видов технических протоколов, включая протокол защиты информации[1]. Основные содержательные характеристики указанных протоколов и их особенности приведены в *прил. 12*.

Значение технического протокола защиты информации как самостоятельного документа, содержащего конкретные требования в части безопасности передачи информации ограниченного доступа при информационном взаимодействии и обмене информацией в электронном виде между Сторонами, достаточно велико.

Данный протокол регламентирует строгий механизм передачи информации по защищенным каналам связи с использованием абонентских пунктов в рамках Мультисервисной сети обмена криминалистической информацией между правоохранительными органами (полициями) государств – участников СНГ. В рамках абонентского пункта при помощи программного комплекса ViPNet Client создаются клиентские автоматизированные рабочие места, которые служат для предоставления информации из информационных ресурсов и передачи данных между участниками электронного обмена.

Программный комплекс российского производства ViPNet Client предназначен для защиты рабочих мест корпоративных пользователей, надежно защищает от внешних и внутренних сетевых атак за счет фильтрации трафика. Кроме того, он обеспечивает защищенную работу с корпоративными данными че-

[1] В настоящее время такие протоколы разработаны в соответствии с Соглашением с Беларусью 2018 г. и Соглашением между Правительством Российской Федерации и Правительством Республики Южная Осетия об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел 2019 г.

рез зашифрованный канал, в том числе для удаленных пользователей. Сценарии использования:

1. Работа в корпоративной сети, защищенной от внутреннего нарушителя. Соединение с ресурсами, сервисами, а также другими пользователями осуществляется через каналы, функционирующие по принципу «точка–точка». Это позволяет надежно защитить информацию от других пользователей, в том числе внутри корпоративной сети.

2. Безопасная работа удаленного пользователя с корпоративными ресурсами и сервисами через защищенные каналы. Шифрование трафика защитит работу с внутренними ресурсами и сервисами при передаче данных через Интернет.

3. Защищенное общение пользователей. Обеспечить защиту корпоративных пользователей также позволит совместное использование ПК ViPNet Client с приложениями ViPNet Connect и ViPNet Деловая почта. Кроме того, ViPNet Client поддерживает защищенные каналы для корпоративных коммуникаций на основе сторонних решений, в том числе IP-телефонии, видеоконференц-связи и т. д.

4. Защита виртуальной машины. ViPNet Client поддерживает работу на виртуальных машинах и позволяет использовать средства защиты ViPNet в VDI-средах.

Правовые основы такого взаимодействия закреплены в Регламенте подключения абонентских пунктов к Мультисервисной сети обмена криминалистической информацией между МВД (Полициями) государств – участников СНГ от 2021 г.

Регламент разработан в соответствии с Положением о единой сети автоматизированных банков данных дактилоскопических следотек, пулегильзотек и телекоммуникационных систем связи министерств внутренних дел государств – участников СНГ и Инструкцией об организации обмена информацией между автоматизированными банками данных дактилоскопических следотек, пулегильзотек и телекоммуникационных систем связи

министерств внутренних дел государств – участников СНГ, утвержденными решением Совета Министров внутренних дел государств – участников СНГ от 17 сентября 2010 г.

Регламент содержит порядок подключения абонентских пунктов, размещенных на территориях государств-участников СНГ (иностранных государств)[1], к Мультисервисной сети обмена криминалистической информацией между МВД (Полициями) государств – участников СНГ, а также состав оборудования абонентского пункта Мультисервисной сети.

Мультисервисная сеть представляет собой защищенную сеть передачи информации, которая использует в качестве транспортной сети сеть связи общего пользования и/или информационно-телекоммуникационную сеть международного информационного обмена информацией (Интернет), с целью повышения оперативности обмена информацией между подразделениями МВД (Полициями) государств – участников СНГ.

Система обеспечения информационной безопасности Мультисервисной сети разработана в соответствии с Моделью угроз и нарушителя «Мультисервисной сети обмена криминалистической информацией между МВД (Полициями) государств – участников СНГ», утвержденной заместителем Министра внутренних дел Российской Федерации 29 июня 2012 г.

Управление осуществляется из Центра управления безопасности, размещенного в МВД России, и строится на базе средств защиты информации, в том числе средств криптографической защиты информации, сертифицированных в соответствии с законодательством Российской Федерации по требованиям ФСБ России и ФСТЭК России.

Информационный обмен между абонентами осуществляется в порядке «запрос – ответ». Информация, предназначенная для передачи абоненту, переносится на абонентский пункт по-

[1] Под данным термином понимается государство, не входящее в состав СНГ.

средством использования учетных съемных машинных носителей информации.

Порядок подключения абонентских пунктов к системе включает следующие стадии:

– заявительная;
– стадия рассмотрения заявки;
– закупка оборудования;
– формирование и передача ключевой информации и учетных записей абоненту;
– тестовый обмен информацией;
– ввод в эксплуатацию.

Общее управление системой обеспечения информационной безопасности Мультисервисной сети осуществляется уполномоченными подразделениями МВД России в части управления защищенной ViPNet-сетью при помощи программного комплекса VipNet Administrator.

В завершение рассмотрения вопроса о важности заключения технических протоколов защиты в рамках информационного взаимодействия и обмена информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел, отметим аспект использования электронной подписи.

При реализации Соглашения с Беларусью 2018 г. и Соглашения с Южной Осетией 2019 г. использование электронной подписи в качестве обязательного элемента не указано. В соответствии с п. 9 Технического протокола защиты информации с Беларусью и п. 8 Технического протокола с Южной Осетией 2019 г. передача файлов между компетентными органами, а также подписание передаваемых файлов электронной подписью (при взаимном решении сторон о необходимости ее использования) осуществляется с использованием компонента «Деловая почта» программного комплекса ViPNet Client, который мы рассматривали ранее.

Вместе с тем, регулирование вопроса использования электронной цифровой подписи (далее – ЭЦП) как инструмента аутентификации отправителя и подтверждения подлинности содержания запроса не является для государств – участников СНГ абсолютно новым направлением взаимодействия, поскольку еще в 2000 г. были приняты Модельный закон СНГ «Об электронной цифровой подписи»[1] и Модельный закон СНГ «Об электронном документе»[2], согласно которому электронная подпись является обязательным реквизитом электронного документа, используемым для идентификации отправителя электронного документа другими субъектами электронного документооборота; национальным законодательством или договором могут быть установлены требования по использованию конкретных видов электронных подписей в электронном документе (ст. 6).

Как отмечают специалисты, основными факторами, затрудняющими трансграничное использование ЭЦП для целей придания электронному документу юридической силы документа, подписанного собственноручно, являются юридическая и техническая несовместимость[3]. Техническая несовместимость препятствует взаимодействию систем удостоверения подлинности. Юридическая несовместимость может иметь место в случаях, когда нормативная правовая база государств, между которыми должен осуществляться обмен документами, подписанными ЭЦП, предусматривает различные требования

---

[1] Модельный закон «Об электронной цифровой подписи» (принят на 16-м пленарном заседании Межпарламентской ассамблеи государств – участников СНГ 9 декабря 2000 г.) // Информационная система «Континент». URL: http://-continent-online.com/Document/?doc_id=1022916&#pos=0;0.

[2] Модельный закон «Об электронном документе» (Приложение к постановлению Межпарламентской ассамблеи государств – участников СНГ от 29 ноября 2013 г. № 39-18) // Информационная система «Континент». URL: http://continent-online.com/Document/?doc_id=31527037&#pos=3;55.

[3] Справка по вопросу о сокращении сроков рассмотрения запросов о правовой помощи, в том числе путем организации взаимодействия с компетентными органами государств – участников СНГ (по пересылке запросов и исполнениях материалов запросов) в электронном виде.

в отношении удостоверения подлинности документов и признания их действительности, содержит терминологические различия основных понятий, различия в требованиях к квалифицированной электронной подписи.

Как представляется, данная проблема успешна решена в нормативном и техническом плане в пределах информационного пространства государств – участников Евразийского экономического союза (далее – ЕАЭС), являющихся одновременно государствами – участниками СНГ. В частности, в рамках ЕАЭС была создана Интегрированная информационная система, предназначенная для обеспечения межгосударственного обмена данными и электронными документами в рамках Союза, создания общих для государств-участников информационных ресурсов, реализации общих процессов, а также обеспечения деятельности ЕАЭС.

Так, в решении Совета Евразийской экономической комиссии от 18 сентября 2014 г. № 73 «О Концепции использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов» отмечается, что в государствах – участниках ЕАЭС в соответствии с их законодательством обеспечение юридической силы электронных документов и организация защищенного документооборота построены на гарантиях их подлинности и целостности посредством применения национальных криптографических методов и средств[1].

Однако с учетом того, что отдельные применяемые органами государственной власти государств – участников ЕАЭС способы реализации криптографических алгоритмов между собой несовместимы, поскольку в соответствии с нормативной право-

[1] Решение Совета Евразийской экономической комиссии от 18 сентября 2014 г. № 73 «О Концепции использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_169491/.

вой базой государств-участников к использованию на их территориях допускаются только сертифицированные по национальным стандартам криптографические средства, то, как следствие, применение единых криптографических средств ЭЦП при трансграничном электронном обмене данными в настоящее время невозможно. Выходом из ситуации явилось предложение по внедрению службы доверенной третьей стороны – организации, наделенной в соответствии с законодательством государств-участников правом осуществлять деятельность по проверке ЭЦП в электронных документах в фиксированный момент времени в отношении лица, подписавшего электронный документ, основными задачами которой являются:

– осуществление легализации (подтверждение подлинности) электронных документов и ЭЦП субъектов информационного взаимодействия в фиксированный момент времени;

– обеспечение проверки ЭЦП отправителя, созданной в соответствии с законодательством государства-участника, в юрисдикции которого находится этот отправитель;

– обеспечение гарантий доверия в международном (трансграничном) обмене электронными документами;

– обеспечение правомерности применения ЭЦП в исходящих и (или) входящих электронных документах в соответствии с законодательством государств – участников электронного взаимодействия.

Доверенные третьи стороны организуются на уровне каждого договаривающегося государства. С технической точки зрения взаимосвязанная структура доверенных третьих сторон (программно-аппаратные комплексы) должна быть размещена во всех национальных сегментах и интеграционном сегменте интегрированной системы.

Доверенные третьи стороны оказывают участникам межгосударственного информационного обмена услуги по проверке ЭЦП отправителя в криптографическом стандарте юрисдикции

отправителя с подписанием квитанции как результата такой проверки. Электронный документ с результатом положительной проверки доверенной третьей стороной признается в юрисдикции получателя равнозначным электронному документу, подписанному собственной ЭЦП отправителя на основе нормы о признании ЭЦП, выданной в соответствии с законодательством другого государства[1].

Удостоверенный в установленном порядке электронный документ признается в юрисдикции уполномоченной доверенной третьей стороны получателя равнозначным электронному документу, подписанному собственной ЭЦП отправителя.

Уполномоченные доверенные третьи стороны должны признавать юридическую силу электронных документов, исходящих от отправителей, находящихся в юрисдикции государства другой уполномоченной доверенной третьей стороны, если электронные документы подписаны (заверены) ЭЦП другой доверенной третьей стороной, находящейся в юрисдикции государства отправителя.

Таким образом, институт доверенной третьей стороны является ключевым в процессе обеспечения трансграничного информационного взаимодействия. Основная цель удостоверяющего центра службы доверенной третьей стороны – обеспечение сертификата ключей проверки электронной цифровой подписи уполномоченных доверенных третьих сторон государств – участников информационного взаимодействия.

Развитием идей и механизмов, заложенных в данной концепции, стало принятие Стратегии развития трансграничного пространства доверия, утвержденной решением Коллегии Евразийской экономической комиссии от 27 сентября 2016 г.,

[1] Решение Совета Евразийской экономической комиссии от 18 сентября 2014 г. № 73 «О Концепции использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW.

в которой обеспечение возможности для всех органов государственной власти государств-участников использовать преимущественно электронные документы, подписанные электронными цифровыми подписями (электронными подписями), является одним из наиболее приоритетных направлений[1].

Как представляется, порядок признания юридической силы электронных документов, подписанных электронной подписью иностранных государств, прописанный в Концепции ЕАЭС, может послужить основой для соответствующих положений в соглашении об информационном взаимодействии в рамках СНГ и иных интеграционных образованиях с участием Российской Федерации, а также в рамках установления двустороннего трансграничного информационного взаимодействия с заинтересованными государствами, чьи технические и организационно-правовые ресурсы позволяют наладить электронный документооборот.

§ 4.3. Зарубежный опыт информационного обмена между правоохранительными органами государств в рамках расследования преступлений в сфере информационно-коммуникационных технологий

Европейский союз является интеграционной организацией с многопрофильными направлениями сотрудничества государств-членов. Одна из актуальных сфер взаимодействия – противодействие транснациональной преступности. Безусловной тенденцией последних лет является беспрецедентный рост противоправных угроз в сфере информационных технологий и свя-

[1] Решение Коллегии Евразийской экономической комиссии от 27 сентября 2016 г. № 105 «О Стратегии развития трансграничного пространства доверия» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_205236/?

занных с ними предикатных преступлений. В частности, в последних докладах Агентства Европейского союза по сотрудничеству правоохранительных органов (далее – Европол) «Оценка угроз организованной преступности в сети Интернет»[1] («IOCTA–2020»[2], «IOCTA–2021»[3]), подготовленных Европейским центром по борьбе с киберпреступностью, отмечается рост кибератак против информационных систем (прежде всего тех, которые осуществляются на основе криминальной бизнес-модели «киберпреступление как услуга»), сексуальное насилие и сексуальная эксплуатация несовершеннолетних, включая производство и распространение материалов о жестоком обращении с детьми, а также мошенничество с безналичными платежами (с акцентом на случаи крупномасштабного мошенничества, особенно на основе криминальных CNP-операций[4]).

---

[1] Каждый год публикуется базовый годовой стратегический отчет о состоянии информационной безопасности и актуальных угрозах со стороны киберпреступности в ЕС «Оценка угроз организованной преступности в Интернете» (Internet Organised Crime Threat Assessment – IOCTA). В документе помимо аналитических обзоров содержатся ключевые рекомендации правоохранительным и иным органам Союза, позволяющие эффективно и согласованно реагировать на вызовы и угрозы организованной преступности в Интернете, а также формировать стратегию, политику и тактику борьбы с киберпреступностью. Кроме того, IOCTA содержит краткий обзор географических угроз киберпреступности на пяти континентах.

[2] Internet Organised Crime Threat Assessment (IOCTA) 2020 // Europol. URL: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

[3] Internet Organised Crime Threat Assessment (IOCTA) 2021 // Europol. URL: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021.

[4] Card Not Presented – категория мошеннических действий с банковскими картами, при операции с которыми продавец не может проверить, есть ли у покупателя карта, и вынужден полагаться на предоставленную последним информацию. Для валидации платежа в этом случае используют номер карты, срок ее действия, имя и фамилию владельца, а также CVC-код. Для мошеннических CNP-операций злоумышленники используют похищенные данные действительных банковских карт.

В этой связи все чаще складывается ситуация, при которой жертва, преступник и ИКТ-инфраструктура, используемая для совершения преступных деяний и хранящая электронные доказательства или в которой функционирует поставщик онлайн-услуг (далее – ПОУ), находятся в разных юрисдикциях. Поэтому для государств – членов ЕС, как и для многих других государств на первый план выходят вопросы развития и внедрения практики обмена электронными доказательствами по уголовным делам между компетентными органами государств.

Здесь следует отметить, что в ЕС функционирует общее пространство свободы, безопасности и правосудия, определяющее единство нормативного регулирования правоохранительного взаимодействия компетентных органов государств-членов, реализуемое в рамках коммунитарной политики посредством специально созданных европейских органов и агентств[1]. Необходимо учитывать и участие ЕС в Будапештской конвенции 2001 г.[2], определяющей в ст. 32 вопросы трансграничного доступа к хранящимся компьютерным данным с соответствующе-

[1] В соответствии с ч. 2 ст. 3 Договора о Европейском союзе Союз предоставляет своим гражданам пространство свободы, безопасности и правосудия без внутренних границ, в котором обеспечивается свободное передвижение лиц во взаимосвязи с соответствующими мерами в области контроля внешних границ, предоставления убежища, иммиграции, а также предотвращения и борьбы с преступностью. См.: Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union // Official Journal of the European Union. 7 June 2016. Исходя из положений ст. 67 Договора о функционировании ЕС к элементу «безопасность» отнесены вопросы, касающиеся предотвращения и борьбы с преступностью, полицейского сотрудничества, правового сотрудничества по уголовным делам, а также сближения уголовного законодательства. См.: Войников В. В. Пространство свободы, безопасности и правосудия в системе права ЕС // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 6. С. 91–92.

[2] На данный момент Будапештская конвенция не ратифицирована только одним государством – членом ЕС – Ирландией. См.: Chart of signatures and ratifications of Treaty 185. Convention on Cybercrime (ETS No. 185) // Council of Europe. URL: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

го согласия или к общедоступным данным[1] и активное участие ЕС в разработке Второго факультативного протокола к Будапештской конвенции о расширении сотрудничества и раскрытии электронных доказательств, принятого 17 ноября 2021 г. комитетом министров Совета Европы[2].

На данный момент основным механизмом ЕС, позволяющим внедрять практику получения доступа к электронным доказательствам при взаимодействии компетентных органов государств – членов ЕС и крупнейших поставщиков онлайн-услуг, является проект «Сириус»[3]. Проект «Сириус» был инициирован в 2017 г. Интернет-форумом ЕС[4] и Еврокомиссией (ЕК) в связи с растущей ролью электронных доказательств в уголовном процессе и необходимостью их получения от ПОУ. С учетом того,

---

[1] Статья 32. Трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным. Сторона может без согласия другой Стороны:

a) получать доступ к общедоступным (открытому источнику) компьютерным данным независимо от их географического местоположения;

b) получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему. См.: Будапештская конвенция 2001 г. // Официальный сайт Совета Европы. URL: https://www.coe.int/ru/web/-conventions/full-list//conventions/rms/0900001680081580.

[2] Протокол обеспечивает правовую основу для раскрытия информации о регистрации доменных имен и для прямого сотрудничества с поставщиками услуг для получения информации об абонентах, эффективные средства для получения информации об абонентах и данных о трафике, оперативное сотрудничество в чрезвычайных ситуациях, инструменты взаимопомощи, а также гарантии защиты персональных данных. См.: New Treaties // Council of Europe. URL: https://www.coe.int/en/web/conventions/new-treaties.

[3] SIRIUS // Europol. URL: https://www.europol.eu-ropa.eu/media-press/-newsroom/news/europol-launches-sirius-plat-form-to-facilitate-online-investigations.

[4] Интернет-форум ЕС основан в 2015 г. Гендиректоратом ЕК по миграции и внутренним делам в целях предупреждения распространения террористического и экстремистского контента в сети Интернет с помощью государственно-частного партнерства между представителями правоохранительных структур, гражданского общества ЕС и поставщиками онлайн-услуг.

что крупнейшие провайдеры онлайн-услуг базируются преимущественно в США[1], в практическом плане «Сириус» выступает прежде всего в качестве механизма поддержки реализации Соглашения ЕС–США о взаимной правовой помощи по уголовным делам 2003 г.[2] и мер по трансграничному доступу к электронным уликам, утвержденных в 2017 г. Советом ЕС по юстиции и внутренним делам[3].

Таким образом, проект «Сириус» призван способствовать укреплению прямого взаимодействия между правоохранительными и судебно-следственными органами стран – членов ЕС, с одной стороны, и зарубежными ПОУ – с другой. В связи с этим характерно, что проект все более востребован среди сотрудников органов юстиции, нуждающихся во вспомогательных инструментах при проведении расследований противоправных деяний, подразумевающих поиск электронных доказательств. Свидетельством этому является заключение в декабре 2020 г. Соглашения между Европолом и Агентством ЕС по сотрудничеству в области уголовного правосудия (Евроюст) о совместном участии обоих агентств в проекте «Сириус»[4] сроком до июня 2024 г. Это делает Евроюст, а заодно и входя-

[1] Наибольшее число обращений правоохранительных органов в 2020 г. было адресовано американским ИТ-гигантам: Google (включая Gmail и YouTube), Facebook (Instagram и WhatsApp), Microsoft (Skype), PayPal и Apple, а также японской Rakuten (Viber), словацкой Azet.sk.и мальтийской Melita.

[2] Agreement on extradition between the European Union and the United States of America // EUROPA. EUR-Lex. URL: https://eur-lex.europa.eu/eli/-agree_internation/2003/516(1)/oj.

[3] European Commission: European Commission welcomes the Council's commitment to improve information exchange and border management, 8 June 2017 // European Union. URL: https://www.europeansources.info/record/justice-and-home-affairs-council-8-9-june-2017/.

[4] Europol and Eurojust sign new contribution agreement expanding cooperation on the SIRIUS project // Europol. URL: https://www.europol.europa.eu/media-press/newsroom/news/euro-pol-and-eurojust-sign-new-contribution-agreement-expanding-cooperation-sirius-project.

щую в его структуру Европейскую судебную сеть (EJN), полноправными бенефициарами проекта.

Кроме того, в рамках проекта «Сириус» в первой половине 2020 г. Агентство ЕС по подготовке сотрудников правоохранительных органов (СЕПОЛ), используя собственную образовательную онлайн-платформу LEEd[1], начало проведение онлайн-тренингов по повышению квалификации сотрудников с целью приобретения ими навыков направления запросов на неотложное раскрытие информации в адрес зарубежных ПОУ, включая международно-правовые аспекты этих процедур[2].

С точки зрения оперативно-технической стороны проект «Сириус» – это межведомственная онлайн-платформа, созданная в рамках Европола для сотрудников правоохранительных и судебно-следственных органов стран – членов ЕС, а также государств, имеющих соглашения об оперативном сотрудничестве с Агентством[3], которая позволяет обмениваться передовым опытом и знаниями в области расследований преступлений, совершаемых в онлайн-среде или с помощью ИТ-технологий; обладает базой данных корпоративных нормативных документов, предоставленных крупнейшими ПОУ[4] в отношении их взаимодействия с госорганами, в том числе документов, содержа-

---

[1] From eNet to LEEd: CEPOL launches brand new eLearning // European Union Agency for Law Enforcement Training (CEPOL) URL: https://www.cepol.europa.eu/media/news/enet-leed-cepol-launches-brand-new-elearning-platform.

[2] CEPOL launches SIRIUS e-Evidence Series in collaboration // European Union Agency for Law Enforcement Training (CEPOL). URL:https://www.cepol.europa.eu/media/news/cepol-launches-sirius-e-evidence-series-collaboration-europol-eurojust.

[3] Доступ к «Сириусу» осуществляется через Платформу Европола для экспертов (Europol Platform for Experts – EPE), однако он ограничен лишь компетентными структурами государств – членов ЕС и стран, подписавших соглашения об оперативным сотрудничестве с Европолом и с Евроюстом. См.: SIRIUS project. SIRIUS Cross-Border Access To Electronic Evidence // Europol. URL: https://www.europol.europa.eu/operations-services-and-innovation/sirius-project.

[4] Airbnb, Apple, Automattic, Cloudflare, Dropbox, Facebook, Google, LinkedIn, Microsoft, Snapchat, Twitter, Verizon Media и др.

щих описание процедур раскрытия данных по запросам властей; содержит программное обеспечение, позволяющее оперативно анализировать информацию, полученную от ПОУ, а также оптимизировать составление и направление запросов к ПОУ.

Необходимо отметить некоторую статистику по состоянию на конец 2021 г.:

– доступ к инструментам проекта имелся у более чем 5,5 тыс. экспертов – сотрудников правоохранительных и судебно-следственных органов 46 стран;

– взаимодействие в рамках «Сириуса» было налажено с 55 провайдерами интернет-услуг, о деятельности которых в справочной системе проекта имеются необходимые информационные материалы, а также реестр контактов более чем 800 ИТ-компаний;

– специальные тренинги в рамках проекта прошли свыше 1,5 тыс. профильных сотрудников[1].

Анализируя проект «Сириус» и рассматривая практику ЕС о направлении прямых запросов к ПОУ по раскрытию требуемых для конкретных уголовных дел данных, следует отметить исключительную добровольность со стороны ПОУ в отношении предоставления информации, позволяющую компании отказаться от ответа на запрос.

В случае отказа ПОУ в добровольном порядке предоставлять базовые данные о пользователе и данные трафика, а также если внутреннее законодательство страны – члена ЕС устанавливает, что официальное направление обращения за взаимной правовой помощью является условием признания данных в качестве доказательства в ходе судебного разбирательства, применяется инструментарий взаимной правовой помощи, предусмотренный международно-правовыми двусторонними и многосторонними

[1] Обзор ситуации в Европейском союзе с внедрением практики получения доступа к электронным доказательствам (по состоянию на ноябрь 2021 г.).

соглашениями о правоохранительном и судебно-следственном сотрудничестве.

Среди причин отказов ПОУ в предоставлении тех или иных данных эксперты выделяют следующие:

– предоставление запрашивающей стороной неверных идентификаторов лица (адрес электронной почты, номер телефона, URL-адрес и имя пользователя) или предоставление лишь ссылки на учетную запись лица, которые на ряде платформ могут не являться уникальными и изменяться пользователем;

– запросы требуют предоставления слишком широкого перечня данных;

– запрашиваются отсутствующие у провайдера данные;

– для ответа на запрос требуется использование каналов взаимной правовой помощи;

– запрашивающая сторона не обосновала запрос ссылкой на свое действующее законодательство;

– получившее запрос юридическое лицо не контролирует запрашиваемые данные (многие ПОУ имеют национальные подразделения и размещают серверы в других странах);

– ошибочные или несвоевременные действия при направлении запросов на сохранение данных.

Кроме того, ПОУ в качестве основных сложностей при взаимодействии с компетентными органами государств отмечают следующее:

– поступление запросов на иностранном языке;

– коллизия профильных законодательств запрашивающего и отвечающего государств, что препятствует предоставлению данных и нередко вынуждает провайдеров устанавливать собственные требования в отношении запросов от иностранных властей с учетом применимого законодательства, а также особенностей своих услуг и продуктов;

– незнание запрашивающими властями характера услуг и продуктов, предлагаемых компаниями;

– необходимость проверки подлинности запросов и проведения юридической экспертизы обстоятельств, требующих неотложного ответа.

Необходимо отметить, что у большинства провайдеров хранящиеся данные классифицируются на три основные категории:

– базовая информация о пользователе (имя, фамилия, номер телефона, адрес электронной почты);

– данные трафика (IP-адреса, журналы подключений, метаданные);

– переданные данные (электронные письма, сообщения, фотографии и т. п.).

Несмотря на то, что страны – члены ЕС, а также США при определении типов данных основываются на положениях Будапештской конвенции о киберпреступности 2001 г., ПОУ собирают данные, прежде всего, ориентируясь на свои бизнес-потребности и типы оказываемых ими услуг, что нередко приводит к различной интерпретации категорий таких данных.

Что касается предоставления информации со стороны ПОУ в обстоятельствах, требующих неотложного ответа, то здесь также нет однозначного толкования алгоритма действий. Так, например, в случаях, когда компетентные органы, мотивируемые серьезными обстоятельствами, например связанными с угрозой жизни человека, направляют провайдеру запросы на неотложное раскрытие информации[1], американские ПОУ в таких случаях должны руководствоваться положениями уголовного законодательства США, определяющего чрезвычайные обстоятельства как ситуацию, «связанную с опасностью гибели или серьезного физического увечья любого человека», которая

[1] Это тип прямых запросов о добровольном предоставлении информации, посредством которых компании могут давать информацию без содержания переданных данных иностранным правоохранительным и судебно-следственным органам в ускоренном порядке, в том числе в течение нескольких минут или часов.

требует «раскрытия информации без задержки»[1]. Однако в силу того, что такое сотрудничество носит по-прежнему добровольный характер, ПОУ могут выдвигать дополнительные условия к подобным неотложным запросам иностранных властей. Как правило, выдвигается требование предоставить как можно больше информации о расследовании и обосновать, почему требуется немедленный доступ к конкретному набору данных.

Следует отметить, что не только со стороны ПОУ выдвигаются и обосновываются проблемы, препятствующие реализации прямых запросов в рамках добровольного раскрытия информации. Со стороны представителей правоохранительных и судебно-следственных органов стран – членов ЕС отмечены следующие основные сложности в работе с ПОУ:

– высокая продолжительность ожидания ответа при использовании каналов ВПП (в среднем около 10 месяцев);

– отсутствие четких правил, определяющих политику провайдеров в отношении запросов иностранных властей, или их чрезмерная сложность;

– отсутствие у сотрудников специальных технических навыков или незнание ими специфического пользовательского лексикона;

– отсутствие доверия со стороны компаний к запрашивающей стране;

– языковой барьер;

– отсутствие у компаний стандартизации одних и тех же процессов, связанных с обработкой запросов от компетентных органов ЕС.

[1] U.S. Code. Title 18. Crimes and criminal procedure. Part I. Crimes Chapter 121. Stored wire and electronic communications and transactional records access Section 2702. (c) Exceptions for Disclosure of Customer Records. Voluntary disclosure of customer communications or records. Legal Information Institute. URL: https://www.law.cornell.edu/uscode/text/18/2702.

Недостаток стандартизации при направлении запросов зарубежным ПОУ связан не только с многообразием подходов к этому вопросу со стороны компаний, но и с отсутствием в ряде стран – членов ЕС или в отдельных подразделениях полицейских, следственных или судебных органов специальных единых контактных пунктов, способных профессионально решать значительную часть проблем.

Для наиболее эффективного внедрения практики получения доступа к электронным доказательствам среди рекомендуемых мер, которые эксперты Европола и Евроюста считают необходимым принять государственным и негосударственным структурам, вовлеченным в процесс предоставления электронных улик, следует выделить следующие:

– правоохранительным органам при направлении соответствующего запроса предлагается использовать разработанные в рамках проекта «Сириус» стандартизированные типовые формуляры для запросов на сохранение и раскрытие данных в рамках добровольного сотрудничества[1];

– всем странам – членам ЕС для оптимизации процесса направления запросов рекомендовано учредить профильные Единые контактные пункты[2];

– следственным органам государств – членов ЕС предлагается назначить контактное лицо, курирующее проблематику электронных улик и соответствующее взаимодействие с Евроюстом;

– провайдерам цифровых услуг следует активнее взаимодействовать с проектом «Сириус», пополняя платформу актуаль-

[1] В разработке данных формуляров участвовали эксперты УНП и Исполнительного директората КТК ООН, а также Европейской судебной сети и Агентства ЕС по подготовке сотрудников правоохранительных органов (СЕПОЛ). Доступ (ограниченного характера) к ним предлагается получить через портал проекта «Сириус».

[2] В 2020 г. действовали в 15 странах – членах ЕС.

ными корпоративными документами, регламентирующими взаимодействие с зарубежными органами государственной власти;

– в случае отклонения запроса со стороны ПОУ предлагается сообщать властям причину отказа, что позволит запрашивающему органу определить, следует ли подавать новый запрос, надо ли предоставлять дополнительные сведения или же следовать путем формирования иной доказательной базы.

Проанализированные сложности процесса получения доступа к электронным уликам в условиях их нахождения в иностранной, прежде всего американской, юрисдикции уже длительное время решаются государствами – членами ЕС посредством точечного укрепления профильной международно-правовой и собственной нормативной базы, в том числе через ведение переговоров с США по проекту соглашения ЕС–США об облегчении доступа к электронным уликам при проведении уголовных расследований, а также вовлеченности Евросоюза в переговорный процесс по Второму дополнительному протоколу к Будапештской конвенции по киберпреступности, также нацеленного на упрощение этих процедур (открыт к подписанию с мая 2022 г.).

Практически параллельно ЕК представила два законодательных предложения по улучшению трансграничного сбора электронных доказательств: Регламент о европейских ордерах на предоставление и сохранение электронных улик по уголовным делам и Директиву о назначении представителей поставщиков онлайн-услуг с целью сбора доказательств в уголовном процессе.

До принятия международно-правовых основ прямого принудительного исполнения запросов правоохранительных органов к провайдерам ИТ-услуг предлагаемая проектом «Сириус» техническая помощь, направленная на упрощение взаимодействия правоохранителей с зарубежными ПОУ, сохраняет свою актуальность.

ВЫВОДЫ И ПРЕДЛОЖЕНИЯ

Указом Президента Российской Федерации от 12 апреля 2021 г. № 213 утверждены Основы государственной политики Российской Федерации в области международной информационной безопасности. Основной тенденцией развития государственной политики в рассматриваемой сфере является ее нацеленность на формирование системы международной информационной безопасности, способной эффективно противодействовать угрозам стратегической стабильности в условиях равноправного стратегического партнерства в глобальном информационном пространстве[1].

На международном уровне Российская Федерация является активным и авторитетным участником международного взаимодействия по обеспечению информационной безопасности. В 1998 г. Россия впервые инициировала обсуждение проблематики МИБ на международном уровне в рамках ООН. К настоящему времени выработано значительное количество российских инициатив в рассматриваемой области, обсуждение которых проходит на площадке ООН: правила ответственного поведения государств в глобальном информационном пространстве; концепция конвенции ООН об обеспечении международной информационной безопасности; конвенция о сотрудничестве в сфере противодействия информационной преступности; концепция безопасного функционирования и развития сети Интернет.

Кроме того, Россия выступает за развитие сотрудничества в данной области в рамках таких переговорных площадок, как ШОС, ОБСЕ, БРИКС, а также региональных организаций, прежде всего ОДКБ и СНГ.

---

[1] Бойко С. Основы государственной политики Российской Федерации в области международной информационной безопасности: регулирование и механизмы реализации // Международная жизнь. URL: https://interaffairs.ru/-jauthor/material/2102.

Российская Федерация выступает за широкий подход к определению содержания понятия «международная информационная безопасность», который включает как технические аспекты (безопасность информационных сетей и систем), так и обширный круг политико-идеологических аспектов (манипулирование информацией, пропаганда посредством глобальных информационных сетей, информационное воздействие), а также механизмы борьбы с преступностью в данной сфере.

К угрозам МИБ согласно Основам государственной политики Российской Федерации в области международной информационной безопасности относится широкий перечень проблем, среди которых имеются позиции, относящиеся к компетенции МВД России и определяющие активный вклад в развитие эффективной государственной политики в области МИБ в части совершенствования международного сотрудничества, направленного на противодействие угрозе использования ИКТ в преступных целях (п. 8, «г»)[1].

В Основах закреплено, что «…достижение цели государственной политики в области МИБ осуществляется путем решения задач по развитию на глобальном, региональном, многостороннем и двустороннем уровнях сотрудничества Российской Федерации с иностранными государствами по вопросам формирования системы обеспечения международной информационной безопасности, а также противодействия основным угрозам международной информационной безопасности» (п. 10). Данный глобальный аспект определяет основные направления развития и совершенствования сотрудничества МВД России со стратегическими партнерами Российской Федерации по вопросам противодействия угрозе использования ИКТ в преступных целях.

[1] Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // НПП «Гарант-сервис». URL: https://www.garant.ru/products/ipo/prime/doc/400473497/.

Поиск универсального решения противодействию глобальной киберпреступности в современных условиях возможен только путем переговоров в формате ООН. Именно поэтому Россия вместе с единомышленниками выступает за выработку универсальных норм, которые разделяли бы все заинтересованные стороны и которые закладывали бы основы эффективного и транспарентного международного сотрудничества по борьбе с этой угрозой с учетом интересов всех без исключения стран и основывалась на принципах суверенного равенства сторон и невмешательства во внутренние дела государств.

В соответствии с принятой 27 декабря 2019 г. резолюцией 74/247 Генассамблея ООН учредила Спецкомитет для разработки конвенции ООН о сотрудничестве в сфере противодействия использованию информационно-коммуникационных технологий в преступных целях.

Россия 27 июля 2021 г. в Вене внесла в Спецкомитет проект первого в истории универсального договора о противодействии использованию информационно-коммуникационных технологий в преступных целях[1].

Первая сессия Спецкомитета прошла в штаб-квартире ООН в Нью-Йорке с 28 февраля по 11 марта 2022 г., вторая – в Вене с 30 мая по 10 июня 2022 г., третья – в Нью-Йорке с 29 августа по 9 сентября 2022 г., четвертая – в Вене с 9 по 20 января 2023 г. *(прил. 13)*. К настоящему времени переговорный процесс инициирован, принята так называемая «Дорожная карта», определяющая порядок работы Спецкомитета, ведется обсуждение консолидированного переговорного документа, предложенного председателем Спецкомитета Ф. Мебарки в качестве основы будущей конвенции. Работу над итоговым проектом всеобъем-

[1] О внесении в Спецкомитет ООН российского проекта универсальной международной конвенции по противодействию использованию ИКТ в преступных целях // МИД России. URL: https://archive.mid.ru/foreign_policy/-news//asset_publisher/.

лющей международной конвенции о борьбе с использованием информационно-коммуникационных технологий в преступных целях планируется завершить в 2024 г. в ходе 78-й сессии Генассамблеи ООН.

В соответствии с Указом Президента Российской Федерации от 21 декабря 2016 г. № 699 «Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации» (с изм. и доп., вступ. в силу с 01.01.2022) МВД России согласно своим полномочиям «участвует в пределах своей компетенции в разработке и реализации основных направлений государственной политики Российской Федерации в области международной информационной безопасности»[1].

Анализ основных направлений развития и совершенствования сотрудничества по линии МВД России со стратегическими партнерами Российской Федерации по вопросам противодействия угрозе использования информационно-коммуникационных технологий в преступных целях позволил прийти к следующим выводам:

1. В современных условиях развития мирового сообщества ключевым приоритетом России является развитие сотрудничества с государствами – участниками СНГ и дальнейшее укрепление межгосударственного взаимодействия на пространстве СНГ. В условиях устойчивого роста преступлений в сфере ИКТ на территориях государств – участников СНГ осуществляется консолидация усилий по противодействию угрозам, возникающим в информационном пространстве. Ключевым междуна-

[1] Указ Президента Российской Федерации от 21 декабря 2016 г. № 699 «Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации» (с изм. и доп., вступ. в силу с 01.01.2022) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_209309/.

родным договором, определяющим правовые основы взаимодействия государств –участников СНГ в борьбе с преступностью в сфере ИКТ, является Соглашение о сотрудничестве в борьбе с преступлениями в сфере информационных технологий в рамках СНГ 2018 г. Его вступление в силу позволило создать современные правовые механизмы практического взаимодействия российских компетентных органов с коллегами из других стран – участников СНГ для эффективного предупреждения, выявления, пресечения, расследования и раскрытия преступлений в сфере информационных технологий.

Установлено, что для МВД России перспективным направлением дальнейшего развития международного правоохранительного сотрудничества по противодействию использования ИКТ в преступных целях выступает обмен данными в электронном виде с правоохранительными органами зарубежных государств. В настоящее время в рамках СНГ ведется активная работа по заключению двусторонних соглашений в указанной области. Например, в 2018 г. подписано Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел.

В качестве предложения разработаны и обоснованы положения по созданию узкопрофильной структуры по проблематике борьбы с преступлениями в сфере ИТ – Центра по противодействию преступлениям в сфере информационных технологий СНГ, который позволит координировать совместное правоохранительное взаимодействие государств – участников СНГ в лице их компетентных органов.

Таким образом, в рамках СНГ сформировано единое правовое пространство в сфере ИКТ, но при этом требуется совершенствование институциональных механизмов, обеспечивающих взаимодействие компетентных правоохранительных органов

государств в данной сфере и создание специализированного отраслевого органа СНГ по вопросам противодействия преступлениям в сфере ИТ.

2. Российская Федерация осуществляет активное взаимодействие с зарубежными партнерами по формированию правовых и институциональных основ сотрудничества в сфере информационной безопасности и противодействия преступности в данной области на евразийском пространстве по линии Шанхайской организации сотрудничества[1].

Сотрудничество государств в области обеспечения международной информационной безопасности на уровне ШОС инициировано в результате блокирования работы ГПЭ ООН, деятельность которой была «заморожена» до 2009 г.[2] Начиная с 2006 г. и до настоящего времени государства – члены ШОС предприняли ряд важных шагов по формированию основ региональной системы международной информационной безопасности.

Под эгидой ШОС был заключен первый в мире международный договор – Соглашение между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г., направленный на комплексное противодействие угрозам международной информационной безопасности, связанным с использованием ИТ в противоправных целях.

В Соглашении определены основные направления сотрудничества, среди которых комплекс мер в области обеспечения международной информационной безопасности, а также не-

---

[1] Концепция внешней политики Российской Федерации (утв. Президентом Российской Федерации 30 ноября 2016 г.) // Официальный сайт МИД России. URL: https://www.mid.ru/foreign_policy/ official_documents//asset_publisher/CptICkB-6BZ29/content/id/-2542248.

[2] Проблематика международной информационной безопасности на площадках ШОС и БРИКС // Официальный сайт ШОС. URL: http://www.infoshos.ru/ru/?idn=20567.

сколько уголовно-правовых направлений: противодействие угрозам использования ИКТ в террористических целях; противодействие информационной преступности.

Под эгидой ШОС сформирована комплексная позиция противодействия преступности в сфере ИТ в привязке к обеспечению МИБ. Стремлений по разработке регионального акта по борьбе с информационным проявлением преступности государства – члены ШОС не выражают. В данном направлении они привержены идее разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях конвенции под эгидой ООН[1].

Однако анализ декларативных документов ШОС подтверждает готовность государств – членов ШОС укреплять сотрудничество в области борьбы с преступлениями в информационной сфере посредством организации мониторинга потенциальных угроз в информационном пространстве и повышения эффективности противодействия подобным угрозам[2].

С учетом специфики первоначальных задач, стоящих перед ШОС, – пресечение так называемых «трех зол» (актов терроризма, сепаратизма и экстремизма в Средней Азии) – Организация проводит масштабную работу по борьбе с такими проявлениями в киберпространстве. Практическая деятельность по обнаружению и противодействию террористической активности в информационном пространстве, пресечению распространения террористической идеологии и пропаганды в сети Ин-

[1] О заявлении Совета глав государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности // Официальный сайт МИД России. URL: https://www.mid.ru/foreign_policy/-news/-/asset_publisher/-cKNonk-JE02Bw/ content/id/4420179.

[2] Астанинская декларация глав государств – членов Шанхайской организации сотрудничества 2017 г. // Официальный сайт Президента Российской Федерации. URL: // http://www.kremlin.ru/supplement/5206 ; Циндаоская декларация Совета глав государств – членов ШОС 2018 г. // Официальный сайт Президента Российской Федерации. URL: http://www.kremlin.ru/supplement/5315.

тернет осуществляется на базе Региональной антитеррористической структуры ШОС.

Перспективными направлениями развития ШОС в исследуемой сфере являются не только правовые концепции, например связанные с разработкой конвенции безопасного функционирования и развития сети Интернет, нацеленной на противодействие киберпреступности и предупреждение угроз информационной безопасности, но и проекты по совершенствованию институциональных механизмов взаимодействия по борьбе с преступностью, в том числе, в сфере информационных технологий, в частности создание Центра информационной безопасности на базе РАТС. Представляется, что реализация обозначенной инициативы станет логическим продолжением при развитии тенденции создания специализированных структур в исследуемой области, а также значительно повысит эффективность деятельности ШОС по противодействию угрозам информационной безопасности и преступлениям в сфере ИТ.

На повестке дня в рамках ШОС стоят задачи по реализации Плана взаимодействия государств – членов ШОС по вопросам обеспечения международной информационной безопасности на 2022–2023 гг. В документе представлен ряд правоохранительных сфер сотрудничества и определены механизмы по их реализации, способствующие противодействию преступлениям в сфере ИТ в рамках ШОС: п. 7 «Взаимодействие в правоохранительной сфере по расследованию преступлений, связанных с использованием ИКТ, в том числе в террористических целях»; п. 11 «Разработка и осуществление согласованной политики и организационно-технических процедур по реализации возможностей использования электронной цифровой подписи и защиты информации при трансграничном информационном обмене.

Последнее направление особенно актуально с точки зрения правоохранительного аспекта по противодействию угрозе использования информационно-коммуникационных технологий

в преступных целях, поскольку в настоящее время остро стоит проблема информационного обмена между МВД России и правоохранительными органами иностранных государств, в том числе в аспекте допустимости электронных доказательств, полученных по электронным каналам связи.

3. Сотрудничество со странами БРИКС является стратегическим направлением внешней политики Российской Федерации, что подчеркнуто в Концепции внешней политики 2016 г., утвержденной Президентом Российской Федерации В. В. Путиным.

На современном этапе одним из важнейших и перспективных направлений сотрудничества в рамках данного формата становятся ИКТ, а в более широком плане – «цифровая экономика». Взаимодействие в данном направлении в рамках БРИКС будет содействовать реализации национальных интересов в информационной сфере, определенных в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

Значимость сотрудничества в данной сфере подчеркнута в Концепции участия России в объединении БРИКС, прямо устанавливающей, что одной из основных наших целей является поэтапное создание общего информационного пространства государств – участников БРИКС[1].

С целями выработки практических предложений, касающихся основных областей сотрудничества, а также координации позиций государств объединения на различных площадках была сформирована Рабочая группа экспертов по вопросам безопасности в сфере использования ИКТ как специализированный орган по проблематике ИКТ.

---

[1] Концепция участия Российской Федерации в объединении БРИКС от 15 апреля 2013 г. // НПП «Гарант-сервис». URL: https://www.garant.ru/products/ipo/prime/doc/70257510/.

Начиная с 2014 г. главы государств в ежегодных Декларациях по итогам саммитов подтверждают «приверженность выработке универсального и имеющего обязательную юридическую силу международно-правового документа в данной области», фиксируют желание «изучать возможности для сотрудничества в области борьбы с киберпреступлениями» и обязуются «сотрудничать в выявлении возможностей для осуществления совместных действий по решению общих проблем безопасности в сфере использования ИКТ».

Консолидированная позиция экспертов государств – участников БРИКС позволяет объединять усилия для отстаивания собственных подходов в рамках деятельности экспертных групп на площадке ООН по вопросам международной информационной безопасности и противодействия преступности в сфере ИКТ.

В перспективной повестке объединения – развитие практического сотрудничества между странами БРИКС в области МИБ, в том числе посредством реализации «Дорожной карты» практического сотрудничества стран БРИКС в обеспечении безопасности в сфере использования ИКТ и в рамках деятельности рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ[1].

Кроме того, перспективным направлением является формирование нормативно-правовых рамок для сотрудничества стран БРИКС по вопросам МИБ, а также рассмотрение и подготовка соответствующих предложений, в том числе о разработке межправительственного соглашения БРИКС о сотрудничестве в области обеспечения безопасности в сфере использования ИКТ и двусторонних соглашений между государствами объединения.

В отношении пятистороннего соглашения БРИКС по МИБ следует отметить, что с 2014 г. Российская Федерация на про-

[1] Делийская декларация (г. Нью-Дели, Индия, 9 сентября 2021 г.) // Национальный комитет по исследованию. БРИКС. URL: https://nkibrics.ru/pages/summit-docs.

тяжении многих лет пытается последовательно добиться подписания пятистороннего соглашения в сфере информационной безопасности под эгидой БРИКС. Рабочий проект данного документа был официально распространен российской стороной в апреле 2015 г. и представлен в ходе заседания Рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ. Делегации заслушали подробную презентацию проекта соглашения, высказали свои комментарии и взяли документ на проработку. При этом к предметному рассмотрению и согласованию распространенного Россией проекта страны не приступили. Российской Федерации следует продолжать работу над проектом соглашения по кибербезопасности в БРИКС, стремясь достичь консенсуса с партнерами.

Что касается развития отношений в рамках двустороннего сотрудничества Российской Федерации с государствами – участниками БРИКС в области обеспечения безопасности в сфере использования ИКТ, то следует отметить, что к настоящему времени по данной тематике заключены соглашения со всеми партнерами. Вместе с тем Российской Федерации предстоит дальнейшая проработка взаимодействия с Бразилией и ЮАР по двусторонни соглашениям в области обеспечения МИБ, поскольку заключенные с данными государствами договоры до сих пор не вступили в силу. Как представляется, на данном направлении могут возникнуть сложности ввиду присоединения ЮАР и Бразилии (февраль 2022 г.) к Будапештской конвенции 2001 г.

Актуальной тенденцией в развитии сотрудничества между участниками БРИКС в вопросах обеспечения использования сферы ИКТ явилось проведение в августе 2021 г. 1-го семинара по цифровой криминалистике для стран БРИКС в рамках председательства Индии[1]. Мероприятие позволило объединить ши-

[1] 1st Workshop on Digital Forensics for BRICS Countries // BRICS information portal. URL: https://infobrics.org/post/33914.

рокое экспертное сообщество из стран БРИКС, представителей правительств, экспертов правоохранительных органов, специалистов по информационной безопасности в рамках обсуждения широкого круга вопросов, связанных с обработкой цифровых доказательств, защиты данных и конфиденциальности, криминалистическим анализом новых технологий, а также обсуждением будущих проблем цифровой криминалистики и разработками по их преодолению.

В качестве предложения представляется возможным инициировать от имени Российской Федерации позицию по ежегодному проведению таких научно-экспертных мероприятий на территории председательствующего государства с целью обмена передовым опытом эффективного использования цифровой криминалистики в гражданских/уголовных или административных расследованиях. Такие мероприятия уже проводились. Так, в августе 2021 г. состоялся 1-й семинар по цифровой криминалистике для стран – участников БРИКС в рамках председательства Индии.

Необходимо отметить общность подходов государств в формате ШОС и БРИКС к формированию системы международной информационной безопасности. Принятые в 2019 г. 73-й сессией Генеральной Ассамблеи ООН российские проекты резолюций «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» и «Противодействие использованию информационно-коммуникационных технологий в преступных целях» аккумулировали идеи, ранее отраженные в итоговых документах саммитов упомянутых объединений, и открывали качественно новый этап дискуссии на главной международной площадке – Организации Объединенных Наций[1].

[1] Бойко С. Проблематика международной информационной безопасности на площадках ШОС и БРИКС // Международная жизнь. URL: https://inter-affairs.ru/news/show/21480.

4. Активное сотрудничество в исследуемой области на постсоветском пространстве осуществляется также в рамках Организации Договора коллективной безопасности. В частности, в Стратегии коллективной безопасности ОДКБ на период до 2025 г. отмечается, что одним из ключевых факторов, отнесенных к современным вызовам и угрозам, является использование информационных и коммуникационных технологий в преступных целях[1].

Государства – члены ОДКБ проводят последовательную комплексную политику одновременного развития правовых и организационных основ укрепления МИБ и противодействия преступной деятельности в информационной сфере как одной из угроз, подрывающих информационную безопасность. При этом, развивая свои коллективные и правовые основы в данных областях, государства – члены Организации выступают за продвижение универсальной системы ответственного поведения государств в новом, активно формирующемся информационном пространстве под эгидой ООН, а также заявляют о приверженности разработке под эгидой ООН конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях в соответствии с профильной резолюцией Генассамблеи ООН[2].

---

[1] Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 г. : утверждена Решением Совета коллективной безопасности Организации Договора о коллективной безопасности от 14 октября 2016 г. // Официальный сайт ОДКБ. URL: https://odkb-csto.org/documents/statements/strategiya_kollektivnoy_bezopasnosti_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_na_period_do_/#loaded.

[2] Заявление министров иностранных дел государств – членов ОДКБ о координации совместных усилий в сфере информационной безопасности, включая противодействие использованию информационно-коммуникационных технологий в террористических и других преступных целях, от 15 сентября 2021 г. // Официальный сайт ОДКБ. URL: https://odkb-csto.org/documents/state-ments/-zayavlenie-ministrov-inostrannykh-del-gosudarstv-chlenov-odkb-o-koordinatsii-sovmestnykh-usiliy-v-sf/?#loaded.

В 2017 г. было подписано Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности. В ст. 3 рассматриваемого договора в качестве основных угроз информационной безопасности выступают: использование информационно-коммуникационных технологий террористическими и экстремистскими организациями, организованными преступными группами (сообществами), а также осуществление противоправной деятельности с использованием информационно-коммуникационных технологий.

Важным вкладом в коллективные усилия государств – членов ОДКБ в борьбу с вызовами их коллективной безопасности в условиях роста информационных угроз является План мероприятий по развитию скоординированной информационной политики в интересах государств – членов Организации Договора о коллективной безопасности от 2018 г.[1] Среди прочего указанный документ предусматривает противодействие угрозам использования информационных и коммуникационных технологий для осуществления противоправных действий в отношении государств – членов ОДКБ, а также проведение мероприятий, направленных на формирование общественного сознания

[1] Решение Совета коллективной безопасности Организации Договора о коллективной безопасности «О Плане мероприятий по развитию скоординированной информационной политики в интересах государств – членов Организации Договора о коллективной безопасности» // Документы, принятые по итогам сессии Совета коллективной безопасности Организации Договора о коллективной безопасности 8 ноября 2018 г. // Официальный сайт Президента Российской Федерации. URL: http://www.kremlin.ru/supplement/5357.

с целью неприятия идеологии международных террористических и религиозно-экстремистских проявлений[1].

В общем спектре вызовов и угроз безопасности государств – членов ОДКБ на одно из центральных мест постепенно выдвигается угроза их информационному суверенитету. В последние годы на национальном уровне в государствах – членах ОДКБ происходит все большее осознание масштабов этой угрозы и необходимости выработки комплексных мер противодействия ей[2]. Эта задача нашла отражение в утвержденной Президентом Российской Федерации 5 декабря 2016 г. Доктрине информационной безопасности Российской Федерации; принятой Постановлением Совета Безопасности Республики Беларусь 18 марта 2019 г. Концепции информационной безопасности Республики Беларусь; утвержденной 3 мая 2019 г. постановлением Правительства Кыргызстана Концепции информационной безопасности Кыргызской Республики на 2019–2023 гг. Аналогичные по смыслу нормы и принципы закреплены в национальном законодательстве других государств – членов ОДКБ. С учетом этого

[1] Последний аспект чрезвычайно важен для государств – членов ОДКБ, особенно тех, что расположены в Центрально-азиатском регионе. Они испытывают на себе мощное воздействие международных террористических организаций, занимающихся через СМИ и Интернет вербовкой своих сторонников с прицелом на их последующее использование для дестабилизации внутриполитической ситуации в указанных государствах. Учитывая высокий уровень интернет-проникновения в государствах – членах ОДКБ, которое быстрыми темпами растет с каждым годом, социальные сети в настоящее время служат той средой, в которой разворачивается серьезная борьба за умы, в первую очередь, молодых людей. См.: Киселев А. О современных подходах к развитию системы информационной безопасности в формате ОДКБ // Союзники. ОДКБ. URL: https://odkb-info.org/about_odkb/ekspertnoe-mnenie/?ELEMENT_ID=81.

[2] Выступление Исполняющего обязанности Генерального секретаря ОДКБ В. Семерикова на «круглом столе» в Государственной Думе Российской Федерации на тему: «Развитие информационно-коммуникационного сотрудничества на пространстве ОДКБ». 21.06.2019 г. // Официальный сайт ОДКБ. URL: https://odkb-csto.org/secretary_general/appearance/vystuplenie-ispolnyayu-shchego-obyazannosti-generalnogo-sekretarya-odkb-vale-riya-semerikova-na-kruglo/.

весьма своевременной и актуальной представляется задача гармонизации национального законодательства государств – членов в части, касающейся противодействия угрозам их суверенитету в информационной сфере, а также разработка правовых актов на эту тему в формате Организации. Оптимальной площадкой для решения этой задачи, на наш взгляд, могла бы стать Парламентская Ассамблея ОДКБ, обладающая для этого необходимым опытом и соответствующим экспертным потенциалом.

В свете проведенного анализа в качестве перспективы представляется необходимым инициировать участие, в первую очередь, государств – участников СНГ, не входящих в ОДКБ, в реализации операций «ПРОКСИ». ОДКБ не только располагает наработанными практиками по взаимодействию государств – членов Организации по противодействию преступной деятельности в информационной сфере, но и готова делиться опытом проведения специальных оперативно-профилактических операций в данной сфере. Данный аспект определяет позицию Организации в привлечении международных и региональных организаций, отдельных государств к наблюдению за ходом проводимых учений и операций, а также к участию в них. Механизмы взаимодействия и партнерства, наработанные в ОДКБ, позволяют это сделать.

Кроме того, перспектива видится в дальнейшем укреплении сотрудничества с государствами – членами ШОС, БРИКС, СНГ, не входящими в ОДКБ, с целью продвижения инициатив и концепций Российской Федерации на универсальном уровне под эгидой ООН. Для осуществления обмена опытом и информацией по вышеуказанным вопросам поддерживаем предложение о проведении встреч в формате регулярных консультаций экспертов ООН, ОБСЕ и ОДКБ.

5. Помимо многостороннего межгосударственного сотрудничества в рамках различных международных организаций предусмотрен также формат двустороннего взаимодействия

государств по различным аспектам информационной безопасности. Отметим наличие двусторонних межправительственных соглашений о сотрудничестве в области обеспечения МИБ, частью которых являются положения о противодействии использования ИКТ в преступных целях. В частности, такие договоры подписаны от имени Правительства Российской Федерации с правительствами следующих государств: Бразилии, Белоруссии, Кубы, Китая, Индии, ЮАР, Вьетнама, Ирана, Киргизии, Никарагуа, Узбекистана, Азербайджана и Армении.

Двусторонние международные межправительственные соглашения Российской Федерации в исследуемой области имеют сходное содержание. Общим для рассматриваемых двусторонних международно-правовых актов является следующее:

– основаны на общепризнанных принципах и нормах международного права;

– закрепляют ключевые аспекты внешнеполитической позиции России по информационной безопасности и противодействию преступлениям в сфере информационных технологий;

– предусматривают обязательство воздержаться от кибератак в двусторонних отношениях;

– фиксируют право на защиту информационных ресурсов государства от неправомерного использования и несанкционированного воздействия, в том числе от компьютерных атак на них;

– позволяют обеспечить формирование взаимного доверия.

Таким образом, двусторонние международные договоры Российской Федерации по вопросам обеспечения информационной безопасности и противодействия преступлениям в сфере информационных технологий не закрепляют новационных подходов к международно-правовому регулированию рассматриваемой сферы, однако имеют особое значение для развития партнерских отношений между Россией и зарубежными государствами.

В качестве предложения полагаем целесообразным заключение двусторонних договоров с государствами – членами

ШОС и БРИКС по вопросам обеспечения международной информационной безопасности с включением раздела по направлению противодействия использования ИКТ в преступных целях, в том числе путем содействия сотрудничеству между правоохранительными органами государств посредством приближенного к реальному времени обмена информацией и сбора доказательств.

Исследование проблем информационного обмена между МВД России и правоохранительными органами иностранных государств, а также изучение механизмов обмена информацией в рамках расследования преступлений в сфере компьютерной информации между государствами позволили прийти к следующим выводам.

В Российской Федерации, как и во многих государствах, уголовное и уголовно-процессуальное законодательство ориентировано на расследование преступлений, совершаемых в сфере ИТ, а также на использование ИТ в процессе доказывания преступлений и решение процессуальных вопросов в суде. Данная практика выработана несмотря на то, что напрямую законодательством Российской Федерации термины «цифровое доказательство» и «электронное доказательство» не регламентированы. Допустимость доказательств, полученных с использованием ИТ, регулируется общими положениями в отношении традиционных доказательств.

Вместе с тем в последнее время эксперты и специалисты все чаще высказывают позицию о целесообразности закрепления в УПК РФ понятия «электронное доказательство» и «электронный документ», подкрепляя свои доводы практическими проблемами при раскрытии преступлений в сфере ИКТ. Данная ситуация требует правового разрешения посредством внесения изменений в ст. 74 УПК РФ в части закрепления понятия «элек-

тронное доказательство»[1] и возможной разработки криминалистической методики сбора электронных доказательств, определения гарантий подлинности электронно-цифровых документов.

Как отмечают эксперты, разрешать вопросы организации обмена электронными документами при оказании правовой помощи допустимо следующими путями:

– заключение международных договоров или внесением изменений в действующие двусторонние и многосторонние договоры Российской Федерации;

– принятие модельных законов, которые содержат положения рекомендательного характера, адресованные государствам – участникам международной организации, направленные на гармонизацию национального законодательства.

Вторая модель в настоящее время нашла применение в пределах пространства СНГ. В частности, в рамках взаимодействия государств – участников Содружества инициирована работа по созданию единой платформы для обмена правовой информацией в сфере осуществления уголовного судопроизводства. Так, на данный момент уже действует постановление Межпарламентской ассамблеи государств – участников СНГ от 25 ноября 2016 г. № 45-13 «О модельном законе “О трансграничном информационном обмене электронными документами”», которым принят одноименный модельный закон.

Вторым блоком актуальных вопросов является использование ИТ в ходе досудебного и судебного производства по уголовным делам. В настоящее время с учетом зарубежного опыта уголовного судопроизводства в электронном формате прора-

[1] Ряд специалистов предлагают следующую формулировку понятия «электронные доказательства» – это электронный носитель информации, содержащий сведения об обстоятельствах, подлежащих доказыванию по конкретному уголовному делу, и обладающий значительным объемом памяти, простотой передачи и копирования сведений с одного носителя на другой, возможностью удаленного доступа к содержанию электронного носителя и телекоммуникационным системам, полученный в порядке, установленном Уголовно-процессуальным кодексом Российской Федерации.

ботка указанного вопроса постоянно осуществляется в Российской Федерации на межведомственном уровне. МВД России поддержаны идеи совершенствования судебного производства и высказаны предложения о проработке в рамках дорожной карты вопроса цифровизации судебного и досудебного производства по уголовным делам.

Указанные обстоятельства актуализируют дальнейшую комплексную работу сформированных межведомственных рабочих групп по подготовке проекта федерального закона о внесении изменений в Уголовно-процессуальный кодекс Российской Федерации в части регулирования вопросов дистанционного участия в уголовном процессе.

Одной из наиболее значимых перспектив совершенствования работы правоохранительных органов по противодействию преступлениям в сфере ИКТ выступает внедрение различных технических и оперативных инноваций в практическую деятельность сотрудников различных подразделений. В частности, большое значение для МВД России имеет развитие возможностей обмена данными в электронном виде с правоохранительными органами зарубежных государств, в первую очередь по линии СНГ.

В настоящее время между государствами – участниками СНГ проводится работа по заключению двусторонних международных договоров, регламентирующих вопросы сотрудничества между органами внутренних дел по вопросам информационного взаимодействия и обмена информацией в электронном виде. В частности, следует отметить Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел, от 13 декабря 2018 г.[1], а также аналогичные межправительственные договоры, подпи-

[1] Далее – Соглашение с Беларусью 2018 г.

санные Российской Федерацией с Республикой Узбекистан (15 декабря 2020 г.)[1] и Республикой Армения (13 мая 2021 г.)[2]. Отметим не менее важное для Российской Федерации Соглашение между Правительством Российской Федерации и Правительством Республики Южная Осетия об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел (10 ноября 2019 г.).

Данные соглашения допустимо назвать типовыми договорами об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел. Вместе с тем, несмотря на их внешнюю схожесть в содержательном аспекте, по тексту имеются некоторые разночтения и правовые нюансы.

Анализ заключенных Правительством Российской Федерации двусторонних соглашений об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел, с отдельными государствами – участниками СНГ позволил изучить структуру и особенности типовых договоров в данной сфере, а также обосновать их значимость для эффективной реализации Соглашения о сотрудничестве в борьбе с преступлениями в сфере информационных технологий в рамках СНГ 2018 г.

---

[1] Соглашение между Правительством Российской Федерации и Правительством Республики Узбекистан об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел, от 15 декабря 2020 г. не вступило в силу. Далее – Соглашение с Узбекистаном 2020 г.

[2] Соглашение между Правительством Российской Федерации и Правительством Республики Армения об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел Российской Федерации и Полиции Республики Армения, от 13 мая 2021 г. не вступило в силу. Далее – Соглашение с Арменией 2021 г.

Кроме того, полагаем, что для полноценной проработки вопросов защиты информации при информационном взаимодействии и обмене информацией в электронном виде МВД России необходимо прорабатывать возможность заключения с государствами – участниками СНГ всех трех видов технических протоколов, включая протокол защиты информации[1].

В рамках исследования информационного взаимодействия и обмена информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел, между государствами – участниками СНГ выявлены проблемы и перспективы развития вопроса использования электронной подписи как инструмента аутентификации отправителя и подтверждения подлинности содержания запроса. Отметим, что при реализации Соглашения с Беларусью 2018 г. и Соглашения с Южной Осетией 2019 г. в рамках технических протоколов использование электронной подписи в качестве обязательного элемента не указано. В соответствии с п. 9 Технического протокола защиты информации с Беларусью и п. 8 Технического протокола с Южной Осетией 2019 г. передача файлов между компетентными органами, а также подписание передаваемых файлов электронной подписью (при взаимном решении сторон о необходимости ее использования) осуществляется с использованием компонента «Деловая почта» программного комплекса ViPNet Client, который мы рассматривали ранее.

Вместе с тем, современные тенденции развития международной правовой помощи по уголовным делам служат импульсом к регулированию цифровой подписи и электронного документооборота. Для государств – участников СНГ данная проблематика не является абсолютно новым направлением вза-

[1] В настоящее время такие протоколы разработаны в соответствии с Соглашением с Беларусью 2018 г. и с Соглашением между Правительством Российской Федерации и Правительством Республики Южная Осетия об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел 2019 г.

имодействия, поскольку были приняты Модельный закон СНГ «Об электронной цифровой подписи» и Модельный закон СНГ «Об электронном документе», согласно которому электронная подпись является обязательным реквизитом электронного документа, используемым для идентификации отправителя электронного документа другими субъектами электронного документооборота; национальным законодательством или договором могут быть установлены требования по использованию конкретных видов электронных подписей в электронном документе (ст. 6).

При этом, как отмечают специалисты, основными факторами, затрудняющими трансграничное использование электронной цифровой подписи для целей придания электронному документу юридической силы документа, подписанного собственноручно, являются юридическая и техническая несовместимость. Техническая несовместимость препятствует взаимодействию систем удостоверения подлинности. Юридическая несовместимость может иметь место в случаях, когда нормативная правовая база государств, между которыми должен осуществляться обмен документами, подписанными ЭЦП, предусматривает различные требования в отношении удостоверения подлинности документов и признания их действительности, содержит терминологические различия основных понятий, различия в требованиях к квалифицированной электронной подписи.

Как представляется, данная проблема успешна решена в нормативном и техническом плане в пределах информационного пространства государств – членов Евразийского экономического союза, являющихся одновременно государствами – участниками СНГ. В частности, в рамках ЕАЭС была разработана Интегрированная информационная система, предназначенная для обеспечения межгосударственного обмена данными и электронными документами в рамках Союза, создания общих

для государств-членов информационных ресурсов, реализации общих процессов, а также обеспечения деятельности ЕАЭС.

Обеспечение трансграничного обмена имеющими юридическую силу электронными документами в интегрированной системе реализуется на основе применения создаваемой службы доверенной третьей стороны – организации, наделенной в соответствии с законодательством государств-членов правом осуществлять деятельность по проверке электронной цифровой подписи в электронных документах в фиксированный момент времени в отношении лица, подписавшего электронный документ (Решение Совета Евразийской экономической комиссии от 18 сентября 2014 г. № 73 «О Концепции использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов»).

Представляется целесообразным применение рассмотренных правовых и технических возможностей электронного документооборота и механизмов внедрения электронной цифровой подписи при разработке и заключении межгосударственных соглашений Российской Федерации об информационном взаимодействии, в которых договаривающиеся стороны могут выбрать любой, не противоречащий нормам международного права и национального законодательства способ дистанционной передачи запросов о правовой помощи и исполнения материалов по ним.

Обмен информацией в электронном виде может осуществляться между компетентными органами после создания технических и юридических условий для такого обмена, в том числе путем определения в соглашении об информационном взаимодействии порядка признания электронной подписи иностранного государства.

В рамках дальнейшего развития международно-правовых основ сотрудничества государств – участников СНГ в сфере информационного взаимодействия и обмена информацией

в электронном виде целесообразно развивать два параллельных и взаимодополняющих процесса организации электронного документооборота между заинтересованными государствами – участниками СНГ.

Во-первых, это продолжение работы по совершенствованию и согласованию Концепции по созданию Единой электронной платформы СНГ для обмена информацией, разработка которой инициирована Министерством юстиции Республики Узбекистан (*см. § 4.1*).

Во-вторых, необходимо инициировать проработку вопроса по трансграничному информационному взаимодействию с заинтересованными сторонами, чьи технические и организационно-правовые ресурсы позволяют наладить электронный документооборот. Как отмечает эксперты, рассмотрение организации защищенного канала связи между двумя государствами – участниками СНГ позволит апробировать новые способы взаимодействия для дальнейшего внедрения на более широком уровне интеграции, выявив потенциальные организационные или технические сложности, которые невозможно учесть при разработке Концепции.

Более того, по мере разработки и апробации основ сотрудничества государств – участников СНГ в сфере информационного взаимодействия и обмена информацией в электронном виде представляется перспективным не ограничиваться пространством государств – участников СНГ, а расширять географию двустороннего взаимодействия с учетом активных позиций отдельных государств, заинтересованных в организации системы электронного документооборота с Российской Федерацией.

6. На данный момент времени основным механизмом ЕС, позволяющим внедрять практику получения доступа к электронным доказательствам при взаимодействии компетентных органов государств – членов ЕС и крупнейших поставщиков онлайн-услуг, является проект «Сириус». Проект был инициир-

рован в 2017 г. Интернет-форумом ЕС и Еврокомиссией в связи с растущей ролью электронных доказательств в уголовном процессе и необходимостью их получения от поставщиков онлайн-услуг.

С учетом того, что крупнейшие провайдеры онлайн-услуг базируются преимущественно в США[1], в практическом плане «Сириус» выступает, прежде всего, в качестве механизма поддержки реализации Соглашения ЕС–США о взаимной правовой помощи по уголовным делам 2003 г. и мер по трансграничному доступу к электронным уликам, утвержденных в 2017 г. Советом ЕС по юстиции и внутренним делам.

Следует отметить, что «Сириус» – это межведомственная онлайн-платформа, созданная в рамках Европола для сотрудников правоохранительных и судебно-следственных органов стран – членов ЕС, а также государств, имеющих соглашения об оперативном сотрудничестве с Агентством[2], которая позволяет обмениваться передовым опытом и знаниями в области расследований преступлений, совершаемых в онлайн-среде или с помощью ИТ-технологий; обладает базой данных корпоративных нормативных документов, предоставленных крупнейшими ПОУ в отношении их взаимодействия с госорганами, в том числе документов, содержащих описание процедур раскрытия данных по запросам властей; содержит программное обеспечение, позволяющее оперативно анализировать инфор-

[1] Наибольшее число обращений правоохранительных органов в 2020 г. было адресовано американским ИТ-гигантам: Google (включая Gmail и YouTube), Facebook (Instagram и WhatsApp), Microsoft (Skype), PayPal и Apple, а также японской Rakuten (Viber), словацкой Azet.sk.и мальтийской Melita.

[2] Доступ к «Сириусу» осуществляется через Платформу Европола для экспертов (Europol Platform for Experts – EPE), однако он ограничен лишь компетентными структурами государств – членов ЕС и стран, подписавших соглашения об оперативным сотрудничестве с Европолом и Евроюстом. См.: SIRIUS project. SIRIUS Cross-Border Access To Electronic Evidence. Update date: 28 Jan 2022 // Europol. URL: https://www.europol.europa.eu/operations-services-and-innovation/sirius-project.

мацию, полученную от ПОУ, а также оптимизировать составление и направление запросов к ПОУ.

Анализируя проект «Сириус» и рассматривая практику ЕС о направлении прямых запросов к ПОУ по раскрытию требуемых для конкретных уголовных дел данных, следует отметить исключительную добровольность со стороны ПОУ в отношении предоставления информации, позволяющую компании отказаться от ответа на запрос.

Среди причин отказов ПОУ в предоставлении тех или иных данных эксперты выделяют следующие:

– предоставление запрашивающей стороной неверных идентификаторов лица (адрес электронной почты, номер телефона, URL-адрес и имя пользователя) или предоставление лишь ссылки на учетную запись лица, которые на ряде платформ могут не являться уникальными и изменяться пользователем;

– запросы требуют предоставления слишком широкого перечня данных;

– запрашиваются отсутствующие у провайдера данные;

– для ответа на запрос требуется использование каналов взаимной правовой помощи;

– запрашивающая сторона не обосновала запрос ссылкой на свое действующее законодательство;

– получившее запрос юридическое лицо не контролирует запрашиваемые данные (многие ПОУ имеют национальные подразделения и размещают серверы в других странах);

– ошибочные или несвоевременные действия при направлении запросов на сохранение данных.

Кроме того, ПОУ в качестве основных сложностей при взаимодействии с компетентными органами государств отмечают следующее:

– поступление запросов на иностранном языке;

– коллизия профильных законодательств запрашивающего и отвечающего государств, что препятствует предоставле-

нию данных и нередко вынуждает провайдеров устанавливать собственные требования в отношении запросов от иностранных властей с учетом применимого законодательства, а также особенностей своих услуг и продуктов;

– незнание запрашивающими властями характера услуг и продуктов, предлагаемых компаниями;

– необходимость проверки подлинности запросов и проведения юридической экспертизы обстоятельств, требующих неотложного ответа.

В случае отказа ПОУ в добровольном порядке предоставлять базовые данные о пользователе и данные трафика, а также если внутреннее законодательство страны –члена ЕС устанавливает, что официальное направление обращения за взаимной правовой помощью является условием признания данных в качестве доказательства в ходе судебного разбирательства, применяется инструментарий взаимной правовой помощи, предусмотренный международно-правовыми двусторонними и многосторонними соглашениями о правоохранительном и судебно-следственном сотрудничестве государств – членов ЕС.

Со стороны представителей правоохранительных и судебно-следственных органов стран – членов ЕС отмечены следующие основные сложности в работе с ПОУ:

– высокая продолжительность ожидания ответа при использовании каналов ВПП (в среднем около 10 месяцев);

– отсутствие четких правил, определяющих политику провайдеров в отношении запросов иностранных властей, или их чрезмерная сложность;

– отсутствие у сотрудников специальных технических навыков или незнание ими специфического пользовательского лексикона;

– отсутствие доверия со стороны компаний к запрашивающей стране;

– языковой барьер;

– отсутствие у компаний стандартизации одних и тех же процессов, связанных с обработкой запросов от компетентных органов ЕС.

Проанализированные сложности процесса получения доступа к электронным уликам в условиях их нахождения в иностранной, прежде всего американской, юрисдикции уже длительное время решаются государствами – членами ЕС посредством точечного укрепления профильной международно-правовой и собственной нормативной базы, в том числе через ведение переговоров с США по проекту соглашения ЕС–США об облегчении доступа к электронным уликам при проведении уголовных расследований, а также вовлеченности Евросоюза в переговорный процесс по Второму дополнительному протоколу к Будапештской конвенции по киберпреступности, нацеленного на упрощение этих процедур (открытие документа к подписанию было определено на май 2022 г.).

Практически параллельно Еврокомиссия представила два законодательных предложения по улучшению трансграничного сбора электронных доказательств: Регламент о европейских ордерах на предоставление и сохранение электронных улик по уголовным делам и Директиву о назначении представителей поставщиков онлайн-услуг с целью сбора доказательств в уголовном процессе.

Как представляется, изученные механизмы внедрения практики получения доступа к электронным доказательствам с адаптацией под российскую действительность заслуживают внимания профильных ведомств Российской Федерации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Международные правовые акты и документы

1. Устав Организации Объединенных Наций от 26 июня 1945 г. // Официальный сайт ООН. – URL: http://www.un.orgru/-documents/charter.

2. Венская конвенция о праве международных договоров от 23 мая 1969 г. // СПС «КонсультантПлюс». – URL: http://-www.consultant.ru/document/consdoc_LAW_12754.

3. Конвенция ООН против транснациональной организованной преступности от 15 ноября 2000 г. // Официальный сайт ООН. – URL: http://www.un.org/ru/documents/decl_conv/conventions/orgcrime.

4. Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. // НПП «Гарант-сервис». – URL: http://base.garant.ru/ 4089723.

5. Конвенция Совета Европы о киберпреступности от 23 ноября 2001 г. // НПП «Гарант-сервис». – URL: http://base.garant.-ru/4089723.

6. Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий от 21 декабря 2010 г. // Asian School of Cyber Laws. – URL: https://www.-asianlaws.org/.

7. Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам от 22 января 1993 г. // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_ LAW_5942/.

8. Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г. // Законодательство стран СНГ. – URL: http://base.-spinform.ru/showdoc.fwx?rgn= 110821.

9. Соглашение между правительствами государств – членов ШОС о сотрудничестве в области обеспечения информационной безопасности от 16 июня 2009 г. // Официальный сайт

ШОС. – URL: https://ccdcoe.org/sites/default/files/documents/-SCO-090616-IISAgreementRussian.

10. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г. // Официальный сайт МИД России. – URL: http://www.mid.ru/foreign_policy/international_contracts/2_contract//storage-viewer/bilateral/page-35/-43921.

11. Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилия о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности от 14 мая 2010 г. // Официальный сайт МИД России. – URL: https://www.mid.ru/.

12. Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности от 25 декабря 2013 г. // НПП «Гарант-сервис». – URL: http://base.garant.ru/70593484/.

13. Соглашение между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности от 11 июля 2014 г. // НПП «Гарант-сервис». – URL: http://base.garant.ru/70593488/.

14. Соглашение между Правительством Российской Федерации и Правительством Республики Индия о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий от 15 октября 2016 г. // НПП «Гарант-сервис». – URL: http://base.garant.ru/-71516368/.

15. Соглашение между Правительством Российской Федерации и Правительством Южно-Африканской Республики о сотрудничестве в области обеспечения международной ин-

формационной безопасности от 4 сентября 2017 г. // Официальный сайт МИД России. – URL: https://www.mid.ru/.

16. Соглашение между Правительством Российской Федерации и Правительством Социалистической Республики Вьетнам о сотрудничестве в области обеспечения международной информационной безопасности от 6 сентября 2018 г. // Официальный сайт МИД России. – URL: https://www.mid.ru/.

17. Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел от 13 декабря 2018 г. // Официальный сайт МИД России. – URL: https://www.mid.ru/.

18. Соглашение между Правительством Российской Федерации и Правительством Республики Узбекистан об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел от 15 декабря 2020 г. // Официальный сайт МИД России. – URL: https://www.mid.ru/.

19. Соглашение между Правительством Российской Федерации и Правительством Республики Армения об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел Российской Федерации и Полиции Республики Армения от 13 мая 2021 г. // Официальный сайт МИД России. – URL: https://www.mid.ru/.

20. Соглашение между Правительством Российской Федерации и Правительством Исламской Республики Иран о сотрудничестве в области обеспечения информационной безопасности от 26 января 2021 г. // Официальный сайт МИД России. – URL: https://www.mid.ru/.

21. Соглашение между Правительством Российской Федерации и Правительством Киргизской Республики о сотрудниче-

стве в области обеспечения международной информационной безопасности от 25 февраля 2021 г. // Официальный сайт МИД России. – URL: https://www.mid.ru/.

22. Соглашение между Правительством Российской Федерации и Правительством Республики Никарагуа о сотрудничестве в области обеспечении международной информационной безопасности от 19 июля 2021 г. // Официальный сайт МИД России. – URL: https://www.mid.ru/.

23. Соглашение между Правительством Российской Федерации и Правительством Республики Узбекистан о сотрудничестве в области обеспечения международной информационной безопасности от 18 ноября 2021 г. // Официальный сайт МИД России. – URL: https://www.mid.ru/.

24. Соглашение между Правительством Российской Федерации и Правительством Республики Армения о сотрудничестве в области обеспечения информационной безопасности от 19 апреля 2022 г. // Официальный сайт МИД России. – URL: https://www.mid.ru/.

25. Соглашение между Правительством Российской Федерации и Правительством Азербайджанской Республики о сотрудничестве в области обеспечения международной информационной безопасности от 24 июня 2022 г. // Официальный сайт МИД России. – URL: https://www.mid.ru/.

26. Душанбинская декларация двадцатилетия ШОС от 17 сентября 2021 г. // Официальный сайт ШОС. – URL: http://rus.sectsco.org/news/20210917/779142.html.

27. Пекинская декларация БРИКС от 23 июня 2022 г. // Национальный комитет по исследованию. БРИКС. – URL: https://nkibrics.ru/pages/summit-docs.

28. Заявление глав государств – членов Шанхайской организации сотрудничества по международной информационной безопасности от 15 июня 2006 г. // Официальный сайт ШОС. – URL: http://infoshos.ru/ru/?id=94.

29. Постановление межпарламентской ассамблеи государств – участников Содружества Независимых Государств от 25 ноября 2016 г. № 45-13 «О модельном законе «О трансграничном информационном обмене электронными документами» // Информационная система «Континент». – URL: http://-continent-online.com/Document/?doc_id=37590479.

30. Резолюция Генеральной Ассамблеи ООН 74/130 от 30 июля 2018 г. «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Доклад Генерального секретаря ООН // Официальный сайт ООН. – URL: https://www.unodc.org/documents/Cybercrime/SG_-report/V1908184_R.pdf.

31. Решение о базовой организации государств – участников СНГ по подготовке кадров в сфере борьбы с преступлениями, совершаемыми с использованием информационных технологий, по образовательным программам высшего образования и дополнительным профессиональным программам // Официальный сайт Исполнительного комитета СНГ. – URL: http://-www.cis.minsk.by/reestr/ru/index.html#reestr/view/text?doc=6075.

32. Решение Совета Евразийской экономической комиссии от 18 сентября 2014 г. № 73 «О Концепции использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов» // СПС «КонсультантПлюс». – URL: http://www.consultant.-ru/document/cons_doc_LAW_169491/.

33. Решение Коллегии Евразийской экономической комиссии от 27 сентября 2016 г. № 105 «О Стратегии развития трансграничного пространства доверия» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_-LAW_205236/.

34. Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 г. Утверждена Решением Совета коллективной безопасности Организации Договора о коллективной безопасности от 14 октября

2016 г. // Официальный сайт ОДКБ. – URL: https://odkbcsto.org/-docments/statements/strategiya_kollektivnoy_bezopasnosti_organi-zatsii_dogovora_o_kollektivnoy_bezopasnosti.

35. Модельный закон «Об электронной цифровой подписи» (принят на шестнадцатом пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ 9 декабря 2000 г.) // Информационная система «Континент». – URL: http://-continent-online.com/Document/?doc_id=1022916&# pos=0;0.

36. Модельный закон «Об электронном документе» (Приложение к постановлению Межпарламентской Ассамблеи государств – участников СНГ от 29 ноября 2013 г. № 39-18) // Информационная система «Континент». – URL: http://continent-online.com/Document/?doc_id=31527037&#pos=3;-55.

37. Agreement on extradition between the European Union and the United States of America // EUROPA. EUR-Lex. – URL: https://eur-lex.europa.eu/eli/agree_internation/2003/516(1)/oj.

Внутригосударственные нормативные правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/-document/cons_doc_ LAW_28399/.

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ : УК : Федеральный закон № 63-ФЗ : принят Государственной Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г. (ред. от 08.03.2022) // НПП «Гарант-сервис». – URL: http://base.garant.ru/5761986.

3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ : УПК : Федеральный закон № 174-ФЗ : принят Государственной Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г. (ред. от 08.12.2020) //

СПС «КонсультантПлюс». – URL: http://www. consultant.ru/document/cons_doc_LAW_34481.

4. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // СПС «КонсультантПлюс». – URL: http://www.-consultant.ru/document/cons_doc_LAW_110165/.

5. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (с изм. и доп.) // НПП «Гарант-сервис». – URL: http://base.garant.ru/10104229/.

6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. – 2006. – № 31.

7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_6180.

8. Федеральный закон от 1 июля 2021 г. № 237-ФЗ «О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_388782/.

9. Федеральный закон от 30 декабря 2021 г. № 501-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_405493/.

10. Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации 30 ноября 2016 г.) // Официальный сайт МИД России. – URL: https://-www.mid.ru/.

11. Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // НПП «Гарант-сервис». – URL: https://www.garant.ru/products/ipo/prime/doc/40/.

12. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс». – URL: http://-www.consultant.ru/document/cons_doc_LAW_389271/.

13. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/-cons_doc_LAW_216363/.

14. Концепция участия Российской Федерации в объединении БРИКС от 15 апреля 2013 г. // НПП «Гарант-сервис». – URL: https://www.garant.ru/products/ipo/prime/doc/70257510/.

15. Решение коллегии Министерства внутренних дел Российской Федерации от 28 мая 2021 г. № 2 «О состоянии и мерах по повышению эффективности и качества предварительного следствия в органах внутренних дел», объявленное приказом МВД России от 15 июня 2021 г. № 447 // СПС «КонсультантПлюс». – URL: http://www.consultant.ru.

Литература

1. Бойко, С. М. Проблематика международной информационной безопасности на площадках ШОС и БРИКС / С. М. Бойко // Международная жизнь. – URL: https://interaffairs.-ru/news/show/21480.

2. Волеводз, А. Г. К вопросу о системе единого правового регулирования международной информационной безопасности и противодействия посягающим на нее преступлениям / А. Г. Волеводз // XII Конвент РАМИ. Специальная секция: международная информационная безопасность: новая геополитическая реальность. – URL: https://risa.ru/images/12theses/-0-1/8-volevodz.pdf.

3. Всестороннее исследование проблемы киберпреступности // Официальный сайт УНП ООН. – URL: https://www.unodc.-org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf.

4. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : в 2 ч. Ч. 1 / [А. В. Аносов и др.]. – М. : Академия управления МВД России, 2019. – 208 с.

5. Дремлюга, Р. И. Интернет-преступность : монография / Р. И. Дремлюга. – Владивосток : Издательство Дальневосточного университета, 2008. – 238 с.

6. Евдокимов, К. Н. Проблемы квалификации и предупреждения нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) : монография / К. Н. Евдокимов. – Иркутск : Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. – 223 с.

7. Жданов, Ю. Н. Полиция будущего / Ю. Н. Жданов, В. С. Овчинский. – М. : Международная полицейская ассоциация, 2018. – 166 с.

8. Зиновьева, Е. С. Дипломатическое наступление России в области информационной безопасности / Е. С. Зиновьева // Официальный сайт МГИМО МИД России. – URL:https://mgimo.ru/about/news/experts/diplomaticheskoe-nastuplenie-rossii-v-oblasti-informatsi-on-noy-bezopasnosti/#5.

9. Зиновьева, Е. С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности / Е. С. Зиновьева // Вестник МГИМО Университета. – 2016. – 4 (49). – С. 235–247.

10. Информационный бюллетень о деятельности стран БРИКС в области научно-технического и инновационного сотрудничества во второй половине 2020 г. – Секретариат Совета НТИ БРИКС, 2020. – 49 с.

11. Калиниченко, И. А. О приоритетных направлениях подготовки кадров для органов внутренних дел Российской Федерации в условиях информатизации общества / И. А. Калини-

ченко // Вестник Московского университета МВД России. – 2020. – № 3. – С. 11–14.

12. Капустин, А. Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности / Я. А. Капустин // Журнал зарубежного законодательства и сравнительного правоведения. – 2017. – № 6. – С. 44–51.

13. Касенова, М. Б. Международное сотрудничество и управление использованием интернета / М. Б. Касенова // Международное право и международные организации. – 2014. – № 1. – С. 6–15.

14. Киберпространство БРИКС: правовое измерение : монография / [И.И. Шувалов и др.] ; под. ред. Д. Руйпин, Т. Я. Хабриева. – М. : Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2017. – 336 с.

15. Лантух, Э. В. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации / Э. В. Лантух, В. С. Ишигеев, О. П. Грибунов // Всероссийский криминологический журнал. – 2020. – Т. 14. – № 6. – С. 882–890.

16. Зиновьева, Е. С. Международная информационная безопасность: проблемы многостороннего и двустороннего сотрудничества : монография / Е. С. Зиновьева. – М. : МГИМО Университета, 2021. – 280 с.

17. Международная информационная безопасность. Теория и практика : учебник для вузов : в 3 т. Т. 1 / [А. В. Бирюков и др.] ; под общ. ред. А. В. Крутских. – 2 изд., доп. – М. : Аспект Пресс, 2021. – 384 с.

18. Мысина, А. И. Международно-правовое регулирование сотрудничества государств по противодействию преступлениям в сфере информационных технологий : дис. ... канд. юрид. наук : 12.00.10 / А. П. Мысина. – М. : Московский университет МВД России имени В.Я. Кикотя, 2021.

19. Новые способы совершения преступлений в сфере информационных технологий на территории государств – участников СНГ : аналитический обзор / [И. Б. Колчевский и др.]. – М. : ВНИИ МВД России, 2018. – 76 с.

20. Оганов, А. А. Основные направления по противодействию киберпреступлениям в отношении несовершеннолетних с использованием киберпространства / А. А. Оганов // Вестник экономической безопасности. – 2019. – № 3. – С. 193–199.

21. Осипенко, А. Л. Государственно-частное партнерство в сфере противодействия киберпреступности / А. Л. Осипенко // Вестник Воронежского института МВД России. – 2016. – № 4. – С. 37–44.

22. Осипенко, А. Л. Новое оперативно-разыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления / А. Л. Осипенко // Вестник Воронежского института МВД России. – 2016. – № 3. – С. 83–90.

23. Противодействие преступлениям, совершаемым в сфере информационных технологий : учебник для студентов высших учебных заведений / [И. А. Калиниченко и др.] ; под науч. ред. И. А. Калиниченко. – М. : Инфра-М, 2023. – 640 с.

24. Пузырева, Ю. В. Уголовно-процессуальные и оперативно-разыскные проблемы использования электронных доказательств и электронных данных в борьбе с преступлениями в сфере информационно-коммуникационных технологий / Ю. В. Пузырева, Е. Е. Бардина // Оперативно-разыскная деятельность и современность : сборник научных трудов / под ред. В. С. Овчинского. – М. : Инфра-М, 2022. – С. 233–242.

25. Пузырева, Ю. В. Оперативно-разыскное обеспечение сотрудничества Российской Федерации с партнерами по СНГ, ШОС, ОДКБ по вопросам противодействия преступлениям в сфере информационно-коммуникационных технологий / Ю. В. Пузырева, Е. Е. Бардина ; под ред. В. С. Овчинского //

Оперативно-разыскная деятельность и современность : сборник научных трудов. – М. : Инфра-М, 2022. – С. 338–362.

26. Пузырева, Ю. В. Международное полицейское сотрудничество по вопросам раскрытия и расследования преступлений в сфере информационных технологий : монография / Ю. В. Пузырева, А. И. Мысина. – М. : Инфра-М, 2020. – 92 с.

27. Пузырева, Ю. В. Международное сотрудничество в борьбе с преступностью : учебное пособие / Ю. В. Пузырева, Д. Д. Шалягин. – М. : Московский университет МВД России имени В.Я. Кикотя, 2019. – 119 с.

28. Русскевич, Е. А. Уголовное право и «цифровая преступность». Проблемы и решения : монография / Е. А. Русскевич. – М. : Научная мысль, 2019. – 227 с.

29. Талимончик, В. П. Международно-правовое регулирование отношений информационного обмена / В. П. Талимончик. – М. : Юридический центр – Пресс, 2011. – 490 с.

30. Фильченко, А. П. Противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий : монография / А. П. Фильченко, В. Ю. Жандров. – М. : Рязанский филиал Московского университета МВД России имени В.Я. Кикотя, 2018. – 110 с.

31. Чернухин, Э. О. О российских инициативах в области противодействия использованию информационно-коммуникационных технологий в преступных целях / Э. О. Чернухин // Международная жизнь. – 2021. – № 2. – С. 146–151.

32. Шалягин, Д. Д. Организация информационного обмена между правоохранительными органами государств – членов ЕС в рамках расследования преступлений в сфере информационно-коммуникационных технологий / Д. Д. Шалягин, Ю. В. Пузырева, Е. Е. Бардина ; под ред. В. С. Овчинского // Оперативно-разыскная деятельность и современность : сборник научных трудов. – М. : Инфра-М, 2022. – С. 290–300.

ПРИЛОЖЕНИЯ

Приложение 1

Цели международных региональных договоров по борьбе с преступлениями в сфере информационно-коммуникационных технологий, а также положения проекта Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях

Международный договор	Цели соглашения
Конвенция Совета Европы о киберпреступности (2001 г.)	Отдельной статьи по целям нет. В преамбуле основной целью обозначено повышение эффективности расследований и процессуальных действий в отношении преступлений, связанных с компьютерными системами и компьютерными данными, а также обеспечение возможности сбора доказательств совершения преступления в электронной форме
Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (2018 г.)	Отдельной статьи по целям нет. «…в целях обеспечения эффективной борьбы с преступлениями в сфере информационных технологий…стремясь создать правовые основы сотрудничества правоохранительных органов Сторон в борьбе с преступлениями в сфере информационных технологий…» (преамбула)

Международный договор	Цели соглашения
Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (2021 г.)	Содействие принятию и укреплению мер, направленных на эффективное предупреждение преступлений и иных противоправных деяний в сфере ИКТ и борьбу с ними; предотвращение действий, направленных против конфиденциальности, целостности и доступности ИКТ, и предупреждение злоупотреблений в сфере использования ИКТ путем обеспечения наказуемости деяний, охватываемых настоящей Конвенцией, и предоставления полномочий, достаточных для эффективной борьбы с такими преступлениями и иными противоправными деяниями, путем содействия выявлению и расследованию таких деяний и преследованию за их совершение как на внутригосударственном, так и на международном уровнях и путем разработки договоренностей о международном сотрудничестве; повышение эффективности и развитие международного сотрудничества, в том числе в контексте подготовки кадров и оказания технической помощи в предупреждении преступлений в сфере ИКТ и борьбе с ними (ст. 2).

Международный договор	Цели соглашения
	Продвигать и укреплять меры по предотвращению и борьбе с использованием ИКТ в преступных целях / киберпреступности, защищая при этом пользователей ИКТ от таких преступлений; продвигать, облегчать и поддерживать международное сотрудничество в предотвращении и борьбе с использованием ИКТ в преступных целях / киберпреступности; предоставить практические инструменты для расширения технической помощи между государствами-участниками и наращивания потенциала национальных органов по предотвращению и борьбе с использованием ИКТ в преступных целях / киберпреступности, а также усилить меры по содействию обмену информацией, опытом и передовой практикой

Приложение 2

Сферы применения международных региональных договоров по борьбе с преступлениями в сфере информационно-коммуникационных технологий, а также положения проекта Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях

Международный договор	**Сфера применения**
Конвенция Совета Европы о киберпреступности (2001 г.)	Статья 14. Сфера применения процессуальных норм
Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий (2010 г.)	Статья 3. Области применения Конвенции. Если не указано иное, настоящая Конвенция применяется к правонарушениям в области информационных технологий с целью их предотвращения, расследования и судебного преследования в следующих случаях: – когда совершено более чем в одном государстве; – при совершении в государстве и подготовке, планировании, руководстве или наблюдении в другом государстве или других государствах; – при совершении в государстве с участием организованной пре-

Международный договор	Сфера применения
	ступной группы, осуществляющей свою деятельность более чем в одном государстве; – когда совершено в государстве и имело тяжкие последствия в другом государстве или других государствах
Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (2018 г.)	Статья отсутствует
Проект конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (2021 г.)	Настоящая Конвенция применяется в соответствии с ее положениями к предупреждению, выявлению, пресечению, расследованию и преследованию за четыре преступления и иные противоправные деяния, признанные таковыми в соответствии со ст.ст. 6–29 настоящей Конвенции, а также осуществлению мер по устранению последствий от совершения таких деяний, включая приостановление операций, связанных с активами, приобретенными в результате совершения какого-либо из преступлений и иных про-

Международный договор	Сфера применения
	тивоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией, арест, конфискацию и возвращение доходов от таких преступлений. Для целей осуществления настоящей Конвенции, если в ней не предусмотрено иное, не является необходимым, чтобы в результате совершения указанных в ней преступлений и иных противоправных деяний был причинен имущественный вред (ст. 2)

Приложение 3

Терминология, используемая в международных региональных договорах по борьбе с преступлениями в сфере информационно-коммуникационных технологий, в проекте Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях

Международный договор	Закрепленная терминология
Конвенция Совета Европы о киберпреступности (2001 г.)	Компьютерная система; компьютерные данные; поставщик услуг; данные о потоках (ст. 1)
Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем (2003 г.)	Расистские и ксенофобские материалы (ст. 2)
Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий (2010 г.)	Информационные технологии; данные; информационная программа; информационная система; информационная сеть; сайт; информация подписчи-

Международный договор	Закрепленная терминология
	ка; поставщик услуг; захват (ст. 2)
Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (2018 г.)	Вредоносная программа; информационные технологии; информационная система; компьютерная система; компьютерная информация; несанкционированный доступ к информации (ст. 1)
Проект конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (2021 г.)	Арест имущества; бот-сеть; вредоносная программа; детская порнография; доходы; информационно-коммуникационные технологии; информационно-телекоммуникационные сети; имущество; информация; конфискация; компьютерная атака; цифровая информация; критическая информационная инфраструктура; объекты критической инфраструктуры; поставщик услуг; технические параметры трафика; устройство ИКТ; электронное доказательство (ст. 4)

Приложение 4

Составы противоправных деяний, подлежащих криминализации в международных региональных договорах по борьбе с преступлениями в сфере информационно-коммуникационных технологий, а также в проекте Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях

Международные договоры	Криминализация
Конвенция Совета Европы о киберпреступности (2001 г.)	*Подраздел 1*. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем: – противозаконный доступ (ст. 2); – неправомерный перехват (ст. 3); – воздействие на данные (ст. 4); – воздействие на функционирование системы (ст. 5); – противозаконное использование устройств (ст. 6). *Подраздел 2*. Правонарушения, связанные с использованием компьютерных средств: – подлог с использованием компьютерных технологий (ст. 7); – мошенничество с использованием компьютерных технологий (ст. 8).

Международные договоры	**Криминализация**
	Подраздел 3. Правонарушения, связанные с содержанием данных: правонарушения, связанные с детской порнографией (ст. 9). *Подраздел 4*. Правонарушения, связанные с нарушением авторского права и смежных прав: правонарушения, связанные с нарушением авторского права и смежных прав (ст. 10). *Подраздел 5*. Дополнительные виды ответственности и санкции: покушение, соучастие или подстрекательство к совершению преступления (ст. 11)
Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем (2003 г.)	Распространение расистских и ксенофобских материалов посредством компьютерных систем (ст. 3); мотивированная угроза расизма и ксенофобии (ст. 4); расистское и ксенофобское мотивированное оскорбление (ст. 5); отрицание, чрезвычайная минимизация, одобрение или оправдание геноцида или преступлений против человечества (ст. 6); пособничество и подстрекательство (ст. 7)

Международные договоры	Криминализация
Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий (2010 г.)	Несанкционированный доступ (ст. 6); незаконный перехват данных любыми техническими средствами (ст. 7); нарушение целостности данных (ст. 8); неправомерное использование средств информационных технологий (ст. 9); подделка документов (ст. 10); мошенничество, совершенное посредством ввода, изменения, стирания или сокрытия данных, а также нарушения работы электронных инструментов, программ и сайтов (ст. 11); производство, распространение, предоставление, опубликование, покупка, продажа, импорт порнографического материала (ст. 12); другие преступления, связанные с порнографией (ст. 13); нарушение неприкосновенности частной жизни с помощью ИТ (ст. 14); преступления, связанные с терроризмом, совершенные с использованием информационных технологий (ст. 15); преступления, связанные с организованной преступностью, совершенные с использованием информационных технологий: легализация преступных доходов; пропаганда употребления и неза-

Международные договоры	Криминализация
	конного оборота наркотических средств и психотропных веществ; торговля людьми, торговля человеческими органами; незаконный оборот оружия (ст. 16); правонарушения, связанные с авторским правом и смежными правами (ст. 17); незаконное использование электронных платежных средств (ст. 18); покушение на совершение преступлений и соучастие в них (ст. 19); покушение и участие в совершении правонарушения (ст. 20); совершение общеуголовных деяний с помощью ИТ, что является основанием для ужесточения мер ответственности (ст. 21)
Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (2018 г.)	Уничтожение, блокирование, модификация либо копирование информации, нарушение работы информационной (компьютерной) системы путем несанкционированного доступа к охраняемой законом компьютерной информации; создание, использование или распространение вредоносных программ; нарушение правил эксплуатации компьютерной системы лицом, имеющим к ней доступ, повлекшее уничтожение, блокирование или модификацию охра-

Международные договоры	Криминализация
	няемой законом компьютерной информации, если это деяние причинило существенный вред или тяжкие последствия; хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации, либо сопряженное с несанкционированным доступом к охраняемой законом компьютерной информации; распространение с использованием информационно-телекоммуникационной сети Интернет или иных каналов электрической связи порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего; изготовление в целях сбыта либо сбыт специальных программных или аппаратных средств получения несанкционированного доступа к защищенной компьютерной системе или сети; незаконное использование программ для компьютерных систем и баз данных, являющихся объек-

Международные договоры	Криминализация
	тами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб; распространение с использованием информационно-телекоммуникационной сети Интернет или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма (ст. 3)
Проект конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (2021 г.)	Неправомерный доступ к цифровой информации (ст. 6); неправомерный перехват (ст. 7); неправомерное воздействие на цифровую информацию (ст. 8); нарушение функционирования информационно-коммуникационных сетей (ст. 9); создание, использование и распространение вредоносных программ (ст. 10); неправомерное воздействие на критическую информационную инфраструктуру (ст. 11); несанкционированный доступ к персональным данным (ст. 12); незаконный оборот устройств (ст. 13); хищение с использованием ИКТ (ст. 14); преступления, связанные с изготов-

Международные договоры	Криминализация
	лением и оборотом материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием ИКТ (ст. 15); склонение к самоубийству или доведение до его совершения (ст. 16); преступления, связанные с вовлечением несовершеннолетних к совершению противоправных действий, опасных для его жизни и здоровья (ст. 17); создание и использование цифровой информации для введения пользователя в заблуждение (ст. 18); подстрекательство к подрывной или вооруженной деятельности (ст. 19); преступления, связанные с террористической деятельностью (ст. 20); преступления, связанные с экстремистской деятельностью (ст. 21); преступления, связанные с распространением наркотических средств и психотропных веществ (ст. 22); преступления, связанные с незаконным оборотом оружия (ст. 23); реабилитация нацизма, оправдание геноцида или преступлений против мира и человечности (ст. 24); незаконное распростране-

Международные договоры	Криминализация
	ние фальсифицированных лекарственных средств и медицинских изделий (ст. 25); использование ИКТ для совершения деяний, признанных преступлениями в соответствии с международным правом (ст. 26); нарушение авторских и смежных прав с использованием ИКТ (ст. 27); соучастие в преступлении, приготовление к преступлению и покушение на преступление (ст. 28); иные противоправные деяния (ст. 29)

Приложение 5

Процессуальные меры, закрепленные в международных региональных договорах по борьбе с преступлениями в сфере информационно-коммуникационных технологий, а также в проекте Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях

Международный договор	Процессуальные меры
Конвенция Совета Европы о киберпреступности (2001 г.)	Сфера применения процессуальных норм (ст. 14); условия и гарантии (ст. 15); оперативное обеспечение сохранности хранимых компьютерных данных (ст. 16); оперативное обеспечение сохранности и частичное раскрытие данных о потоках информации (ст. 17); распоряжение о предъявлении (ст. 18); обыск и выемка хранимых компьютерных данных (ст. 19); сбор в режиме реального времени данных о потоках информации (ст. 20); перехват данных о содержании (ст. 21)
Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной	Связь между настоящим Протоколом и Конвенцией (ст. 8). Стороны увеличивают сферу применения мер, определенных в ст.ст. 14–21 и 23–35 Конвенции ст.ст. 2–7 настоящего Протокола

Международный договор	**Процессуальные меры**
ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем (2003 г.)	
Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий (2010 г.)	Сфера применения процессуальных положений (ст. 22); оперативное обеспечение сохранности данных, хранящихся в ИТ (ст. 23); оперативное хранение и частичное раскрытие информации об отслеживании пользователей (ст. 24); порядок предоставления информации (ст. 25); проверка хранимой информации (ст. 26); изъятие хранимой информации (ст. 27); оперативный сбор информации об отслеживании пользователей (ст. 28); перехват информации о содержании (ст. 29)
Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (2018 г.)	Нормы отсутствуют

Международный договор	**Процессуальные меры**
Проект конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (2021 г.)	Сфера применения процессуальных норм (ст. 31); условия и гарантии (ст. 32); сбор информации, передаваемой с использованием ИКТ (ст. 33); оперативное обеспечение сохранности накопленной информации в электронной форме (ст. 34); оперативное обеспечение сохранности и частичное раскрытие данных о технических параметрах трафика (ст. 35); распоряжение о предоставлении информации (ст. 36); обыск и выемка информации, хранимой или обрабатываемой в электронной форме (ст. 37); сбор в режиме реального времени технических параметров трафика (ст. 38)

Приложение 6

Правоприменение и юрисдикция согласно положениям международных региональных договоров по борьбе с преступлениями в сфере информационно-коммуникационных технологий, а также проекту Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях

Международный договор	**Правоприменение и юрисдикция**
Конвенция Совета Европы о киберпреступности (2001 г.)	Юрисдикция (ст. 22)
Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем (2003 г.)	Связь между настоящим Протоколом и Конвенцией (ст. 8). Стороны увеличивают сферу применения мер, определенных в ст.ст. 14–21 и 23–35 Конвенции ст.ст. 2–7 настоящего Протокола

Международный договор	**Правоприменение и юрисдикция**
Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий (2010 г.)	Юрисдикция (ст. 30)
Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (2018 г.)	Норма отсутствует
Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (2021 г.)	Юрисдикция (ст. 39)

Приложение 7

Инновационные формы сотрудничества государств в борьбе с преступлениями в сфере информационно-коммуникационных технологий согласно положениям международных региональных договоров по борьбе с преступлениями в сфере информационно-коммуникационных технологий, а также проекту Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях

Международный договор	Международное сотрудничество
Конвенция Совета Европы о киберпреступности (2001 г.)	Общие принципы международного сотрудничества (ст. 23); выдача (ст. 24); общие принципы взаимной помощи (ст. 25); внеплановая информация (ст. 26); процедуры направления запросов о взаимной помощи в отсутствие применимых международных соглашений (ст. 27); конфиденциальность и ограничения на использование информации (ст. 28); неотложное обеспечение сохранности хранящихся компьютерных данных (ст. 29); неотложное раскрытие сохраненных данных о потоках информации (ст. 30); взаимная помощь в отношении доступа к хранящимся электронным данным

Международный договор	Международное сотрудничество
	(ст. 31); трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным (ст. 32); взаимная правовая помощь по сбору данных о потоках в режиме реального времени (ст. 33); взаимная помощь по перехвату данных (ст. 34); сеть 24/7 (ст. 35)
Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем (2003 г.)	В сфере международного сотрудничества отмечена связь между настоящим Протоколом и Конвенцией (ст. 8)
Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий (2010 г.)	Выдача (ст. 31); взаимная правовая помощь (ст. 32); внеплановая информация (ст. 33); порядок сотрудничества и взаимной помощи; запросы (ст. 34); отказ во взаимной помощи (ст. 35); конфиденциаль-

Международный договор	Международное сотрудничество
	ность и ограничения использования (ст. 36); оперативная защита информации, хранящейся в информационных системах (ст. 37); оперативное раскрытие информации (ст. 38); взаимная помощь в отношении доступа к хранимой информации (ст. 38); трансграничный доступ к информации (ст. 40); взаимная помощь в отношении оперативного сбора информации для отслеживания пользователей (ст. 41); взаимная помощь в отношении информации, связанной с содержанием конкретных сообщений (ст. 42); специализированный орган (ст. 43)
Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (2018 г.)	Формы сотрудничества (ст. 5): создание информационных систем и программных продуктов, обеспечивающих выполнение задач по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере ИТ (п. «д» ст. 5); обмен программными продуктами и решениями, используемыми в предупреждении, выявлении, пресечении, раскрытии и расследовании преступлений в сфере ИТ (п. «ж» ст. 5); исполнение запроса о неотложном обеспечении сохранности данных,

Международный договор	Международное сотрудничество
	хранящихся в компьютерных системах (п. «и» ст. 5); запрос об оказании содействия (ст. 6); исполнение запроса (ст. 7); конфиденциальность информации (ст. 8); использование результатов исполнения запросов (ст. 9); передача сведений третьей стороне (ст. 10); отказ в исполнении запроса (ст. 11)
Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (2021 г.)	Общие принципы международного сотрудничества (ст. 46); выдача (ст. 47); отказ в выдаче (Non bis in idem) (ст. 48); взаимная правовая помощь (ст. 49); экстренная взаимная помощь (ст. 50); информация, предоставляемая в инициативном порядке (ст. 51); процедуры направления запросов о взаимной правовой помощи в отсутствие применимых международных договоров (ст. 52); проведение допроса и иных процессуальных действий с использованием систем видеоконференции или телефонной конференции (ст. 53); полномочия дипломатических представительств и консульских учреждений (ст. 54); конфиденциальность и ограничения на использование информации (ст. 55); опе-

Международный договор	Международное сотрудничество
	ративное обеспечение сохранности информации в электронной форме (ст. 59); оперативное предоставление сохраненных технических параметров трафика (ст. 60); взаимная помощь по сбору технических параметров трафика в режиме реального времени (ст. 61); взаимная помощь по сбору информации в электронной форме (ст. 62); совместные расследования (ст. 63); специальные методы расследования (ст. 64); сеть 24/7 (ст. 66)

Приложение 8

Техническая помощь и обмен опытом между государствами в соответствии с положениями международных региональных договоров по борьбе с преступлениями в сфере информационно-коммуникационных технологий, а также проектом Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях

Международный договор	Техническая помощь, обмен опытом
Конвенция Совета Европы о киберпреступности (2001 г.)	Самостоятельные нормы по данному виду взаимоотношений отсутствуют. Имеется только ссылка на оказание «технических консультаций» в рамках работы специализированного контактного центра 24/7 (ч. 1 ст. 35)
Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем (2003 г.)	Самостоятельные нормы по данному виду взаимоотношений отсутствуют

Международный договор	**Техническая помощь, обмен опытом**
Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий (2010 г.)	Самостоятельные нормы по данному виду взаимоотношений отсутствуют. Имеется только ссылка на оказание «технических консультаций» в рамках работы специализированного органа 24/7 (п. «а» ч. 1 ст. 43)
Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (2018 г.)	Самостоятельные нормы по данному виду взаимоотношений отсутствуют
Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (2021 г.)	Общие принципы технической помощи (ст. 75); подготовка кадров (ст. 76); обмен информацией (ст. 77)

Приложение 9

Меры по противодействию преступлениям и иным противоправным деяниям в информационном пространстве в соответствии с положениями международных региональных договоров по борьбе с преступлениями в сфере информационно-коммуникационных технологий, а также проектом Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях

Международный договор	**Профилактические меры**
Конвенция Совета Европы о киберпреступности (2001 г.)	Самостоятельные нормы по данному виду взаимоотношений отсутствуют
Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем (2003 г.)	Самостоятельные нормы по данному виду взаимоотношений отсутствуют

Международный договор	**Профилактические меры**
Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий (2010 г.)	Самостоятельные нормы по данному виду взаимоотношений отсутствуют
Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (2018 г.)	Самостоятельные нормы по данному виду взаимоотношений отсутствуют
Проект конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (2021 г.)	Политика и практика предупреждения преступлений и иных противоправных деяний в сфере использования ИКТ и борьбы с ними (ст. 40); органы по предупреждению преступлений и иных противоправных деяний в сфере использования ИКТ и борьбе с ними (ст. 41); частный сектор (ст. 42); принципы и стандарты поведения частных организаций (ст. 43); повышение информированности общества в сфере предупреждения информационной преступности (ст. 44); меры по защите свидетелей (ст. 45)

Приложение 10

Международные двусторонние соглашения Российской Федерации со странами БРИКС по вопросам информационной безопасности

Наименование соглашения	Субъекты, заключившие соглашение	Сведения о действии соглашения	Краткая характеристика соглашения
ИНДИЯ Российско-индийское межправительственное Соглашение о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий	Заключено 15 октября 2016 г. на полях VIII саммита БРИКС на Гоа (15–16 октября 2016 г.) заместителем Министра иностранных дел Российской Федерации И. В. Моргуловым и Национальным координатором Республики Индии по вопросам кибербезопасности Г. Раем	Вступило в силу 22 января 2017 г.	Создает правовые рамки для диалога заинтересованных ведомств стран по всему спектру вопросов МИБ. В рамках его реализации предполагается проведение на регулярной основе двусторонних межведомственных консультаций
КИТАЙ Соглашение между Правительством Российской	Заключено 8 мая 2015 г. в Москве в ходе визита Председателя КНР Си	Вступило в силу 10 августа 2016 г.	Создает правовые рамки для диалога заинтересованных ведомств двух

Наименование соглашения	Субъекты, заключившие соглашение	Сведения о действии соглашения	Краткая характеристика соглашения
Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения МИБ	Цзиньпиня в Российскую Федерацию Министром иностранных дел Российской Федерации С. В. Лавровым и Министром иностранных дел КНР Ван И.		стран по всему спектру вопросов обеспечения МИБ. В числе приоритетов сотрудничества выделена совместная борьба с использованием информационно-коммуникационных технологий в террористических и иных противоправных целях. Достигнута договоренность об углублении российско-китайского взаимодействия в сфере МИБ на профильных международных форумах, включая ООН, Международный союз электросвязи, ШОС, БРИКС и Региональный форум АСЕАН

Наименование соглашения	Субъекты, заключившие соглашение	Сведения о действии соглашения	Краткая характеристика соглашения
			по безопасности. Предполагается проведение на регулярной основе двусторонних межведомственных консультаций
БРАЗИЛИЯ Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности	Заключено 14 мая 2010 г. в Москве в ходе визита президента Федеративной Республики Бразилии Луиса Инасио Лулы да Силва в Российскую Федерацию Секретарем Совета Безопасности Н. П. Патрушевым и Министром иностранных дел С. Аморимом	В настоящее время Соглашение не вступило в силу в связи с тем, что в Бразилии на данном этапе документ не ратифицирован. Внутригосударственные процедуры в России завершены. Российская сторона готова к синхронному обмену уведомлениями о выполнении в обоих государствах таких процедур, как только они будут завершены в Бразилии. С при-	Создает правовые и организационные основы сотрудничества сторон в области обеспечения международной информационной и коммуникационной безопасности и определяет важность такого сотрудничества для дальнейшего развития двустороннего стратегического партнерства. В Соглашении определены основные формы и механизмы сотрудничества

Наименование соглашения	Субъекты, заключившие соглашение	Сведения о действии соглашения	Краткая характеристика соглашения
		ходом к власти в Бразилии Ж. Болсонаро партнеры ссылаются на необходимость модернизировать двустороннее соглашение и провести дополнительную экспертизу в рамках нового правительства. До настоящего времени никакой дополнительной информации из Бразилиа не поступало	
ЮАР Соглашение между Правительством Российской Федерации и Правительством Южно-Африканской Республики о сотрудничестве в области обеспечения МИБ	Заключено 4 сентября 2017 г. на полях IX саммита БРИКС в г. Сямэне (КНР; 4–5 сентября 2017 г.) Министром иностранных дел Российской Федерации С. В. Лав-	18 сентября 2017 г. МИД России направил ноту Посольству ЮАР в Москве о выполнении внутригосударственных процедур, необходимых для вступления в силу упомянутого Соглашения.	Создает правовые и организационные основы сотрудничества сторон в области обеспечения международной информационной и коммуникационной безопасности

Наименование соглашения	Субъекты, заключившие соглашение	Сведения о действии соглашения	Краткая характеристика соглашения
	ровым и Министром международных отношений и сотрудничества Южно-Африканской Республики М. Нкоана-Машабане	По состоянию на настоящее время ответная нота не поступала. Соглашение не вступило в силу. В феврале 2020 г. Министр госбезопасности ЮАР А. Длодло сообщила, что подписанный текст документа планировалось направить в парламент для утверждения в марте 2020 г., однако из-за распространения Коронавируса это не было сделано. К настоящему времени соглашение так и не ратифицировано	

Приложение 11

Двусторонние международные договоры Российской Федерации об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел

Наименование международного договора / критерии для сравнения	**Соглашение между Правительством Российской Федерации и Правительством Республики Узбекистан об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел, от 15 декабря 2020 г.**	**Соглашение между Правительством Российской Федерации и Правительством Республики Армения об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутрен-них дел Российской Феде-рации и Полиции Республики Армения, от 13 мая 2021 г.**	**Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь об информационном взаимодействии и обмене информацией в электронном виде по вопросам,** относящимся к компетенции органов внутренних **дел, от 13 декабря 2018 г.**
Преамбула	«Правительство Российской Федерации и Правительство …, в дальнейшем именуемые Сторонами, руководствуясь общепризнанными принципами и нормами международного права, желая развивать сотрудничество между компетентными органами государств Сторон по вопросам информационного взаимодействия и обмена информацией в электронном виде, согласились о нижеследующем…»		

<table>
<tr><td rowspan="3">Предмет соглашения (ст. 1)</td><td>Предметом является организация информационного взаимодействия в электронном виде в рамках, действующих в отношениях между Российской Федерацией и Республикой Узбекистан/Армения международных договоров, компетентными органами по выполнению которых определены Министерство внутренних дел Российской Федерации и Министерство внутренних дел Республики Узбекистан / Полиция Республики Армения»</td><td>Предметом являются правовое регулирование и организация взаимодействия компетентных органов государств-Сторон при обмене информацией в электронном виде, в том числе персональными данными, по вопросам, относящимся к компетенции органов внутренних дел, за исключением информации, относящейся к сведениям, составляющим государственную тайну (государственные секреты) государств-Сторон</td></tr>
<tr><td colspan="2">В рамках соглашений не осуществляется обмен информацией, составляющей государственную тайну государств Сторон</td></tr>
<tr><td colspan="2">Взаимный обмен информацией в электронном виде осуществляется с использованием информационных систем, программно-технических средств и (или) за счет доступа компетентного органа государства – другой Стороны к ресурсам информационных систем, находящихся в ведении компетентных органов государств-Сторон</td></tr>
</table>

	Компетентные органы государств-Сторон обязуются содействовать обеспечению безопасности, полноты и достоверности информации, находящейся в информационных системах		
	Правовой основой информационного взаимодействия между компетентными органами государств-Сторон выступают настоящие Соглашения, технические протоколы, национальное законодательство государств-Сторон и международные договоры, участниками которых являются их государства		
Компетентные органы государств-Сторон (ст. 2)	Компетентными органами государств-Сторон по реализации настоящего Соглашения являются: от Российской Федерации – Министерство внутренних дел Российской Федерации; от государств – участников соглашений – национальные компетентные органы в сфере внутренних дел		
		Об изменениях своих компетентных органов каждая из Сторон в течение месяца в письменной форме уведомляет другую Сторону по дипломатическим каналам	
Технические протоколы (ст. 3)	В целях реализации положений настоящего Соглашения уполномоченные подразделения компетентных органов государств Сторон разрабатывают технические протоколы: информационного и технологического взаимодействия; информационного взаимодействия; технологического взаимодействия; защиты информации		
	В технических протоколах определяются: цели обмена информацией; порядок защиты информации; перечень передаваемых и получаемых в электронном виде сведе-		В технических протоколах определяются: перечень передаваемых и получае-

	ний, сроки, технология, порядок их передачи, хранения и уничтожения; сроки установки технических средств, введения в эксплуатацию каналов связи и их обслуживания	мых в электронном виде сведений; технология и порядок передачи, хранения, уничтожения, защиты информации и доступа к ней; сроки установки технических средств, введения в эксплуатацию каналов связи и их обслуживания
	Технические протоколы утверждаются руководителями (начальниками) компетентных органов государств-Сторон	
	Компетентные органы государств-Сторон письменно уведомляют друг друга о готовности к информационному обмену после проведения необходимых подготовительных мероприятий, связанных с выполнением требований технических протоколов	
Компетенция (юрисдикция, полномочия) компетентных органов государств (ст. 4)	Предоставляют и получают в электронном виде информацию, находящуюся в их ведении, и (или) доступ к ресурсам информационных систем на безвозмездной основе в соответствии с техническими протоколами в согласованном ими объеме	Предоставляют и получают в электронном виде информацию (в том числе персональные данные), находящуюся в их ведении, и (или) доступ к ресурсам информационных систем на безвозмездной основе в соответствии с техниче-

		скими протоколами в согласованном ими объеме
	Фиксируют предоставление, получение и уничтожение информации	
	Фиксируют доступ компетентного органа государства – другой Стороны к ресурсам своих информационных систем	
	В соответствии с законодательством каждого из государств-Сторон и международными договорами, участниками которых они являются, обеспечивают защиту информации, получаемой в рамках настоящего Соглашения	
	Используют информацию, полученную в рамках настоящего Соглашения, исключительно в служебных целях и не передают ее третьей стороне без предварительного письменного согласия компетентного органа государства-Стороны, предоставившего информацию	Используют информацию, полученную в рамках настоящего Соглашения, исключительно в служебных целях и не передают ее третьей стороне без предварительного письменного согласия компетентного органа государства-Стороны, предоставившего информацию, за исключением случаев, предусмотренных Соглашением о взаимоотношениях министерств внутренних дел в сфере обмена информацией

		от 3 августа 1992 г. и Соглашением об обмене информацией в сфере борьбы с преступностью от 22 мая 2009 г.
	Соблюдают требования информационной безопасности и правила работы в информационных системах государства – другой Стороны	
	Обращение со сведениями, содержащимися в Межгосударственном информационном банке, осуществляется в соответствии с Соглашением о взаимоотношениях министерств внутренних дел в сфере обмена информацией от 3 августа 1992 г. и Соглашением об обмене информацией в сфере борьбы с преступностью от 22 мая 2009 г.	–
	Защита передаваемой по трансграничным каналам связи информации осуществляется в соответствии с техническим протоколом информационного взаимодействия	Защита передаваемой по трансграничным каналам связи информации, в том числе персональных данных, осуществляется в соответствии с техническим протоколом защиты информации. Требования к защите информации должны соответ-

		ствовать законодательству каждого из государств-Сторон, Соглашению между Правительством Российской Федерации и Правительством Республики Белоруссия о сотрудничестве в области защиты информации от 9 июля 1997 г. и другим международным договорам, участниками которых являются государства-Стороны
	Компетентные органы государств-Сторон обеспечивают полноту, достоверность и актуальность предоставляемой информации	Ответственность за полноту, достоверность и актуальность информации несут должностные лица компетентного органа государства-Стороны, предоставившего информацию, в соответствии с законодательством своего государства

Хранение и уничтожение информации (ст. 5)	Хранение и уничтожение информации осуществляются в соответствии с техническими протоколами, национальным законодательством государств-Сторон и их международными обязательствами, в том числе после прекращения действия настоящего Соглашения. Уничтожение информации из информационных систем осуществляется компетентными органами государств-Сторон, в ведении которых находятся информационные системы	
Ограничение в предоставлении доступа к информации (ст. 6)	Компетентный орган государства-Стороны, предоставляющий информацию, имеет право приостанавливать доступ компетентного органа государства-Стороны, получающего информацию, к информационным системам в случаях выявления нарушения требований информационной безопасности и правил работы в информационных системах. В срок, не превышающий 3 рабочих дней со дня выявления причин, препятствующих осуществлению информационного взаимодействия, компетентный орган государства-Стороны, приостановивший доступ, направляет компетентному органу государства – другой Стороны уведомление в письменной форме с указанием причин, даты начала и срока приостановления доступа. Предоставление информации возобновляется после устранения причин, препятствующих осуществлению информационного взаимодействия	
Расходы сторон (ст. 7)	Стороны самостоятельно несут расходы, которые будут возникать в ходе выполнения настоящего Соглашения, если в каждом конкретном случаен не будет согласован иной порядок	Стороны самостоятельно несут расходы по реализации настоящего Соглашения

Изменения в соглашения (ст. 8)	По согласию Сторон в настоящее Соглашение могут быть внесены изменения, которые оформляются отдельным протоколом, вступающим в силу в порядке, предусмотренном ст. 12 настоящего Соглашения
Рабочий язык (ст. 9)	При реализации положений настоящего Соглашения в качестве рабочего языка используется русский язык
Урегулирование разногласий сторон в отношении соглашений (ст. 10)	Спорные вопросы, возникающие в связи с толкованием или применением положений настоящего Соглашения, решаются путем переговоров и консультаций между компетентными органами государств-Сторон
Права и обязательства из других международных договоров Сторон (ст. 11)	Положения настоящего Соглашения не затрагивают прав и обязательств, вытекающих из других международных договоров, участниками которых являются государства-Стороны
Вступление в силу и прекращение действия соглашений (ст. 12)	Настоящее Соглашение вступает в силу со дня получения по дипломатическим каналам последнего письменного уведомления о выполнении Сторонами внутригосударственных процедур, необходимых для его вступления в силу Настоящее Соглашение прекращает свое действие по истечении 6 месяцев с даты получения одной из Сторон письменного уведомления другой Стороны о намерении прекратить действие настоящего Соглашения

Приложение 12

Сравнительный анализ технических протоколов к двусторонним международным договорам Российской Федерации об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел

Наименование технического протокола / критерии для сравнения	**Технический протокол технологического взаимодействия при обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел**	**Технический протокол защиты информации при информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел**	**Технический протокол информационного взаимодействия при обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел**
Цели	Определяет технологию взаимодействия при реализации информационного обмена между Сторонами в электронном виде	Устанавливает требования в части защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну,	Определяет перечни сведений, находящихся в ведении Сторон и подлежащих передаче в рамках информационного обмена в электронном виде между Сторонами

		при информационном взаимодействии и обмене информацией в электронном виде между Сторонами	
Особенности, технические характеристики	Взаимодействие осуществляется путем обмена сведениями в электронном виде (файловый обмен) с клиентских автоматизированных рабочих мест Сторон в соответствии с Регламентом подключения абонентских пунктов к мультисервисной сети обмена криминалистической информацией между правоохранительными органами (полициями) государств – участников СНГ от 23 марта 2016 г.	Взаимодействие осуществляется путем подключения компетентных органов Сторон к мультисервисной сети обмена криминалистической информацией между правоохранительными органами (полициями) государств – участников СНГ	Применяется после реализации положений протокола технологического взаимодействия и протокола защиты информации
	Разработка схемы информационного взаимодействия и обмена информацией в электронном виде	Разработка схемы защиты информации при обменен информацией в электронном виде	Составление подробных перечней сведений, находящихся в ведении компетентных органов в сфере внутренних дел

			каждой из Сторон, и подлежащих передаче в рамках информационного обмена
		Передача файлов между уполномоченными подразделениями Сторон, а также подписание передаваемых файлов электронной подписью осуществляется с использованием компонента «Деловая почта» программного комплекса российского производства линейки ViPNet Client	Примерное содержание категорий и предоставляемых сведений: 1. По линии экспертно-криминалистической деятельности: 1.1. Сведения о следах рук неустановленных лиц, изъятых с мест нераскрытых тяжких и особо тяжких преступлений. 1.2. Сведения о пулях и гильзах со следами огнестрельного нарезного оружия, изъятых с мест нераскрытых преступлений и происшествий, а также об экспериментальных пулях и гильзах, отстрелянных в изъятом, найденном и добровольно сданном оружии. 1.3. Сведения о самодельном огнестрельном оружии.

			1.4. Сведения о самодельных взрывных устройствах и их составных частях. 1.5. Сведения о поддельных монетах, денежных билетах, бланках ценных бумаг и документов, изымаемых из незаконного оборота. 1.6. Сведения о новых видах наркотических средств, психотропных веществ и их прекурсорах, появившихся в незаконном обороте. 2. По линии Госавтоинспекции: 2.1. Сведения о зарегистрированных транспортных средствах и их владельцах. 2.2. Сведения о выданных водительских удостоверениях. 2.3. Сведения об административных правонарушениях. 3. В рамках ведения централизованных учетов:

			3.1. Сведения о лицах, объявленных в межгосударственный розыск (посредством тиражирования с ежедневной актуализацией сведений). 3.2. Сведения о разыскиваемых транспортных средствах, утраченном и выявленном оружии и ином вооружении (посредством тиражирования с ежедневной актуализацией сведений). 3.3. Сведения о похищенных предметах, имеющих культурную ценность (по запросам). 3.4. Сведения о похищенных и изъятых номерных вещах, и документах (по запросам). 3.5. Сведения о неопознанных трупах (по запросам). 4. Обзорная информация по актуальным проблемам деятельности правоохранительных органов зарубежных стран.

			5. Сборник «Переводы материалов о практике деятельности правоохранительных органов зарубежных стран» (по мере выпуска). 6. В сфере правового обеспечения: 6.1. Сведения о законодательных и иных нормативных правовых актах Российской Федерации в сфере внутренних дел. 6.2. Сведения о результатах научно-исследовательских работ по вопросам осуществления правотворческой деятельности. 6.3. Сведения о методических пособиях по организации правовой работы. 6.4. Сведения о модернизации договорно-правовых основ международного сотрудничества по вопросам, относящимся к компетенции органов внутренних дел Российской Федерации.

			6.5. Сведения о совершенствовании нормативно-правового регулирования деятельности органов внутренних дел Российской Федерации. 6.6. Сведения об осуществлении организационно-методического руководства правовой работой и контроля за нормотворческой деятельностью в подразделениях МВД России. 6.7. Сведения о создании и внедрении в практику органов внутренних дел Российской Федерации автоматизированных информационно-справочных правовых систем. 6.8. Сведения об осуществлении информационно-правового обеспечения органов внутренних дел Российской Федерации. 7. Информация, запрашиваемая в рамках уголовных дел, полу-

			чение которой не требует выполнения следственных действий, (по запросу). 8. Информация, запрашиваемая по материалам проверок (по запросу). 9. Информация по материалам проверок и уголовным делам, представляющая взаимный интерес (по мере установления обстоятельств, имеющих значение для рассмотрения материалов проверок и расследования уголовных дел). 10. Информация о гражданах государств-Сторон, привлеченных к административной ответственности на территории Российской Федерации

Приложение 13

Обзор субстантивных сессий Специального межправительственного комитета Организации Объединенных Наций по разработке всеобъемлющей Международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (2022–2023 гг.)

Дата проведения субстантивной сессии Специального комитета	Общая характеристика проведенного мероприятия и итоги
28 февраля – 11 марта 2022 г., Нью-Йорк (США)	В первой сессии, проходившей в гибридном формате, приняли участие профильные эксперты из более чем 160 государств и 200 неправительственных организаций, представляющих политические и правоохранительные структуры, а также академическое, научное и бизнес-сообщество. Российская межведомственная делегация была представлена экспертами МИД России, Генеральной прокуратуры Российской Федерации, Следственного комитета Российской Федерации, МВД России, Министерства юстиции Российской Федерации, Министерства цифрового развития Российской Федерации и ФСБ России. Одним из первых в общеполитических дискуссиях было оглашено приветственное обращение Министра иностранных дел Российской Федерации С. В. Лаврова участникам Спецкомитета. В нем была подчеркнута созидательная роль России в создании данной переговорной площадки и задан конструктивный тон дальнейшей профессиональной дискуссии с прицелом на достижение выработки столь необходимой конвенции в полном соответствии с установленными Генассамблеей ООН

Дата проведения субстантивной сессии Специального комитета	Общая характеристика проведенного мероприятия и итоги
	мандатом и сроками. В соответствии с одобренной повесткой дня Спецкомитет последовательно рассмотрел вопросы целей и охвата будущей универсальной Конвенции. Консенсусом утверждена ее структура, состоящая из 8 глав. Согласованы модальности работы Спецкомитета на 2022–2024 гг. В соответствии с планом предполагается проведение шести субстантивных сессии в Вене и Нью-Йорке, а также межсессионных консультаций в том числе с участием официально зарегистрированных НПО и частного сектора. Состоялся насыщенный обмен мнениями по ключевым элементам проекта. Наибольшую актуальность, по мнению государств-участников, приобрели вопросы защиты суверенитета, юрисдикции, разработки универсального понятийного аппарата, усиления международного сотрудничества при раскрытии трансграничных преступлений, а также технического содействия и подготовки кадров. В качестве национального вклада Российская Федерация в очередной раз обратила внимание участников первой субстантивной сессии на собственный проект универсальной конвенции по противодействию информпреступности, соавторами которого стал Китай и еще ряд государств. Большинство его элементов нашло широкое отражение в выступлениях различных делегаций и вошло в окончательные документы первой сессии Спецкомитета. Главным итогом первой сессии можно считать полноценный запуск практической работы над универсальной конвенцией, который долго откладывался по различным причинам. Излишняя политизация и попытки навязать однобокие правила уступили место многосторонней и конструктивной дипломатии с тесным привлечением ведущих экспертов со всего мира. Заработал предложенный Россией открытый инклю-

Дата проведения субстантивной сессии Специального комитета	Общая характеристика проведенного мероприятия и итоги
	зивный и транспарентный процесс переговоров по комплексной борьбе с киберкриминалом под эгидой ООН. Спецкомитет задает новые ориентиры, объединив самый передовой опыт в области противодействия информпреступности[1]
30 мая – 10 июня 2022 г., Вена (Австрия)	Во второй сессии приняли участие свыше 120 государств и порядка 200 неправительственных организаций, а также академическое, научное и бизнес-сообщество. Российская межведомственная делегация была представлена экспертами МИД России, Генеральной прокуратуры Российской Федерации, Следственного комитета Российской Федерации, МВД России, Министерства юстиции Российской Федерации, Минцифры России и ФСБ России. В ходе мероприятия государства-участники обменялись мнениями относительно наполнения первых трех глав будущей конвенции, посвященных вопросам криминализации, общим положениям, процессуальным мерам и правоохранительной деятельности. Обсудили необходимость разработки этого международно-правового инструмента в соответствии с резолюцией Генеральной Ассамблеи ООН 75/282. В ходе дискуссии по повестке дня, в выступлениях целого ряда делегаций нашли отражение ссылки на российский проект универсальной конвенции по противодействию информпреступности, внесенный в Спецкомитет 21 июля 2021 г. Главным

[1] О первой сессии Спецкомитета ООН по разработке всеобъемлющей конвенции по противодействию информационной преступности. 12.03.2022 // Официальный сайт МИД России. URL: https://www.mid.ru/ru/foreign_policy/international_-safety/1803908/.

Дата проведения субстантивной сессии Специального комитета	Общая характеристика проведенного мероприятия и итоги
	итогом второй субстантивной сессии является запуск экспертного диалога между правоохранительными органами государств-участников по ключевым элементам будущей конвенции[1]
29 августа – 9 сентября 2022 г., Нью-Йорк (США)	В работе третьей сессии Спецкомитета приняли участие 118 государств – членов ООН и более 110 неправительственных организаций, представителей академического, научного и бизнес-сообществ. Российская межведомственная делегация включала экспертов МИД России, Генеральной прокуратуры Российской Федерации, Следственного комитета Российской Федерации, МВД России, Министерства юстиции Российской Федерации, Минцифры России и ФСБ России. Ввиду очередного вопиющего нарушения со стороны США обязательств как принимающей страны штаб-квартиры ООН и невыдачи въездных виз большая часть наших экспертов подключалась к мероприятию по видеосвязи. В ходе сессии государства-участники обменялись мнениями относительно наполнения составных частей будущей конвенции, касающихся международного сотрудничества, технической помощи, мер предупреждения, механизма осуществления конвенции, заключительных положений и преамбулы. С учетом первых трех сессий Председатель Спецкомитета Ф. Мебарки разработает и представит консолидированный «нулевой» проект будущего международно-правового договора, который будет рассмот-

[1] О второй сессии Спецкомитета ООН по разработке всеобъемлющей конвенции по противодействию информационной преступности. 16.02.2022 // Официальный сайт МИД России. URL: https://www.mid.ru/ru/foreign_policy/news/-1818160/.

Дата проведения субстантивной сессии Специального комитета	Общая характеристика проведенного мероприятия и итоги
	рен государствами-членами в ходе четвертой и пятой сессий Спецкомитета (в Вене 9–20 января и 11–23 апреля 2023 г.)[1]
9–20 января 2023 г., Вена (Австрия)	В работе четвертой сессии Спецкомитета приняли участие более 170 государств – членов ООН и неправительственных организаций, представителей академического, научного и бизнес-сообществ. Основным итогом сессии стал запуск работы над текстом конвенции на основе подготовленного председателем консолидированного переговорного документа, который включает широкий перечень криминализуемых деяний и процедурных положений. Повесткой дня сессии было предусмотрено рассмотрение первых трех глав консолидированного переговорного документа («Общие положения», «Криминализация», «Процессуальные меры и правоприменение»). Председателем Спецкомитета в переговорном документе выделены 16 неконсенсусных статей, по которым в соответствии с утвержденной на заседании методологией запущена работа четырех неформальных рабочих групп – по ст.ст. 26–32 (вопросы терроризма, экстремизма, незаконного оборота наркотиков, оружия, распространения фальсифицированных лекарственных средств и медицинских изделий), по ст.ст. 15, 16 (преступления, связанные с персональными данными), по ст.ст. 40 и 47–49 (юрисдикция, сбор трафика в режиме реального време-

[1] О сессии Спецкомитета ООН по разработке всеобъемлющей конвенции по противодействию информационной преступности. 10.09.2022 // Официальный сайт МИД России. URL: https://www.mid.ru/ru/foreign_policy/news/1829389/.

Дата проведения субстантивной сессии Специального комитета	Общая характеристика проведенного мероприятия и итоги
	ни, перехват данных, допустимость электронных/цифровых доказательств), по ст. 2 (терминология)[1]
Итоговый текст конвенции Спецкомитет представит Генассамблее ООН в ходе ее 78-й сессии в 2024 г.	

[1] О четвертой сессии Спецкомитета ООН по разработке всеобъемлющей конвенции по противодействию информационной преступности. 23.01.2023 // Официальный сайт МИД России. URL: https://www.mid.ru/tv/?id=1849347&lang=ru.

Учебное издание

Пузырева Юлия Владимировна,
кандидат юридических наук, доцент

Бардина Екатерина Евгеньевна

Шалягин Дмитрий Дмитриевич,
кандидат юридических наук, доцент

Направления деятельности МВД России по повышению эффективности международного сотрудничества в борьбе с преступлениями в сфере информационно-коммуникационных технологий в рамках реализации Основ государственной политики Российской Федерации в области международной информационной безопасности

Редактор *Васильевых Е. М.*
Корректор *Абилова Ф. А.*
Компьютерная верстка *Абилова Ф. А., Табунова Е. А.*

Формат 60х84/ 1/16.
Усл. печ. л. 15.
Подписано в печать 13.06.2023. Заказ № 51.
Тираж 57 экз. 1-й завод

Отпечатано в Полиграфическом центре
Московского университета МВД России имени В.Я. Кикотя
https://мосу.мвд.рф, e-mail: support_mosu@mvd.ru