На правах рукописи

Мысина Анастасия Ильинична

МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ СОТРУДНИЧЕСТВА ГОСУДАРСТВ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Специальность 12.00.10 – Международное право; Европейское право

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата

юридических наук

Москва – 2021

Работа выполнена на кафедре прав человека и международного права Федерального государственного казенного образовательного учреждения высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя».

Научный руководитель: кандидат юридических наук, доцент
Пузырева Юлия Владимировна

Официальные оппоненты: **Бирюков Павел Николаевич**,
доктор юридических наук, профессор, заведующий кафедрой международного и евразийского права ФГБОУ ВО «Воронежский государственный университет»

Степанян Армен Жоресович,
кандидат юридических наук, доцент кафедры интеграционного и европейского права ФГБОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)»

Ведущая организация: ФГАОУ ВО «Российский университет дружбы народов»

Защита состоится «28» октября 2021 г. в 11 часов 00 минут на заседании диссертационного совета Д 203.019.01, созданного на базе ФГКОУ ВО «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя» по адресу: 117997, г. Москва, ул. Академика Волгина, 12, учебно-лекционный комплекс № 2, зал заседаний диссертационного совета.

С диссертацией можно ознакомиться в библиотеке и на официальном сайте ФГКОУ ВО «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя» (http://diss.mosu-mvd.com/ru/).

Автореферат разослан «___» _____ 2021 г.

Ученый секретарь
диссертационного совета
кандидат юридических наук, доцент Ф.О. Вертлиб

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертационного исследования. В настоящее время преступления в сфере информационных технологий представляют реальную угрозу общественным отношениям на внутригосударственном уровне, а также международному правопорядку. Организованные преступные группы применяют новые технологические средства в противоправных целях, причиняя ущерб физическим и юридическим лицам. Указанные преступления отличаются высокой степенью латентности и во многих случаях приобретают транснациональный характер, что обусловливает наличие определенных трудностей в их раскрытии и расследовании, а также актуализирует необходимость консолидации усилий компетентных органов государств.

Проблема противодействия преступлениям в сфере информационных технологий неоднократно рассматривалась в документах региональных международных организаций, Организации Объединенных Наций (далее – ООН) и на Конгрессах ООН по предупреждению преступности и уголовному правосудию. Следует также отметить, что сотрудничество в исследуемой области определено как одно из стратегических условий, способствующих достижению Целей в области устойчивого развития[1].

Несмотря на значимость исследуемой проблематики, в настоящее время государствам не удалось выработать согласованные подходы к противодействию преступлениям в сфере информационных технологий и заключить соответствующий международный договор под эгидой ООН. При этом региональное международно-правовое регулирование характеризуется фрагментарностью и разрозненностью. Указанные факторы снижают эффективность межгосударственного взаимодействия и актуализируют

[1] Цели в области устойчивого развития являются своеобразным призывом к действию, исходящим от всех государств, направленным на улучшение благосостояния человечества. Они приняты в 2015 г. в рамках Повестки дня в области устойчивого развития на период до 2030 г. // Официальный сайт ООН. URL: https://www.un.org/sustainabledevelopment/ru/about/development-agenda/ (дата обращения: 14.03.2021).

необходимость анализа международно-правовых основ противодействия преступлениям в сфере информационных технологий.

Особо важное значение для осуществления эффективного противодействия преступлениям в сфере информационных технологий имеют институциональные механизмы сотрудничества, поскольку они обеспечивают координацию межгосударственного взаимодействия. В этой связи представляется значимым исследование сложной системы элементов институциональных основ сотрудничества государств по противодействию преступлениям в сфере информационных технологий, а также тенденций развития межгосударственного взаимодействия в рассматриваемой сфере.

Значительная роль при осуществлении международного сотрудничества по противодействию преступлениям в сфере информационных технологий отводится государственно-частному партнерству, поскольку в настоящее время в компетентных правоохранительных органах различных государств наблюдается нехватка специализированных кадров, владеющих необходимыми навыками использования информационных технологий, и недостаточная технологическая оснащенность сотрудников правоохранительных органов специальными средствами и программным обеспечением. Обозначенные обстоятельства обуславливают необходимость исследования современного состояния и перспективных направлений развития данного аспекта многоуровневого взаимодействия.

Международное сотрудничество по противодействию преступлениям в сфере информационных технологий представляется актуальным для Российской Федерации, активно выступающей за укрепление межгосударственного взаимодействия в рассматриваемой области. Исследование вклада России в развитие правовых и институциональных основ противодействия преступлениям в сфере информационных технологий имеет значение для всех сфер общественной жизни и отвечает приоритетам внешней политики Российской Федерации.

При осуществлении раскрытия и расследования транснациональных преступлений в сфере информационных технологий правоохранительные органы сталкиваются с рядом проблем, в том числе относительно установления места совершения преступления и юрисдикции, использования цифровых доказательств, полученных от компетентных органов иностранных государств и т.д. В связи с чем особую актуальность приобретает определение перспектив совершенствования деятельности правоохранительных органов Российской Федерации по раскрытию и расследованию преступлений в сфере информационных технологий.

Кроме того, повышенный интерес ученых-международников вызывают вопросы обеспечения информационной безопасности, как элемента международной безопасности, а также понятия «киберпреступность» и «компьютерные преступления». Вместе с тем, недостаточно внимания уделяется категории «преступления в сфере информационных технологий» в рамках международного сотрудничества по противодействию преступности (включая профилактику, предупреждение, пресечение, раскрытие и расследование преступлений, минимизацию ущерба и ликвидацию последствий). При этом в проведенных исследованиях не нашли отражения современные угрозы и тенденции развития международно-правового регулирования сотрудничества государств по противодействию преступлениям в сфере информационных технологий, определяющие задачи международного сотрудничества в исследуемой области.

Таким образом, актуальность настоящего диссертационного исследования обусловливается тем, что ряд ключевых аспектов международно-правового регулирования сотрудничества государств по противодействию преступлениям в сфере информационных технологий до сих пор оставался без комплексной международно-правовой оценки.

Цель диссертационного исследования заключается в выявлении закономерностей и особенностей международно-правового регулирования

сотрудничества государств по противодействию преступлениям в сфере информационных технологий.

Для достижения поставленной цели в ходе исследования решались следующие **научные задачи**:

- раскрыть проблемы развития понятийного аппарата международного сотрудничества по противодействию преступлениям в сфере информационных технологий;
- дать характеристику международно-правовых основ сотрудничества государств в исследуемой области;
- установить закономерности функционирования институционального механизма ООН по противодействию преступлениям в сфере информационных технологий;
- выявить особенности развития региональных институциональных основ сотрудничества государств по противодействию преступлениям в сфере информационных технологий;
- определить закономерности развития институциональных механизмов сотрудничества государств по противодействию преступлениям в сфере информационных технологий в рамках международных полицейских организаций;
- выявить перспективные направления развития государственно-частного партнерства по противодействию преступлениям в сфере информационных технологий;
- установить наиболее актуальные перспективы совершенствования деятельности правоохранительных органов Российской Федерации по раскрытию и расследованию преступлений в сфере информационных технологий.

Объектом исследования выступают международно-правовые отношения, складывающиеся в процессе сотрудничества субъектов международного права по противодействию преступлениям в сфере информационных технологий.

Предмет исследования охватывает правовые, институциональные и доктринальные основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий.

Степень научной разработанности темы исследования. Проблематика противодействия преступлениям в сфере информационных технологий является комплексной, в связи с чем активно изучается специалистами различных областей современной науки. За последние годы российскими учеными-правоведами защищен ряд диссертаций, в которых фундаментально исследованы отдельные аспекты сотрудничества государств по противодействию преступлениям в сфере информационных технологий. К ним относятся работы В.П. Талимончик[2] О.В. Мозолиной[3], К.В. Прокофьева[4], В.И. Федулова[5].

Значительный вклад в исследование международного сотрудничества в борьбе с преступностью в сфере информационных технологий внесли ученые-международники, а также специалисты в области криминологии, политических наук и различных отраслей национального права.

На монографическом уровне отдельные вопросы, связанные с противодействием преступлениям в сфере информационных технологий, исследованы в трудах В.М. Быкова, Р.И. Дремлюги, К.Н. Евдокимова, В.Ю. Жандрова, А.Я. Капустина, М.Б. Касеновой, Ю.В. Пузыревой, Е.А. Русскевича, А.П. Фильченко, Т.Я. Хабриевой, В.Н. Черкасова[6].

---

[2] Талимончик В.П. Международно-правовое регулирование отношений в сфере информации: дис. ... докт. юрид. наук 12.00.10. – СПб., 2013.

[3] Мозолина О.В. Публично-правовые аспекты международного регулирования отношений в Интернете: дис. ... канд. юрид. наук: 12.00.10. – М., 2008.

[4] Прокофьев К.В. Международно-правовые проблемы обеспечения международной информационной безопасности в сети Интернет: дис. ... канд. юрид. наук: 12.00.10. – М., 2009.

[5] Федулов В.И. Международно-правовые аспекты защиты компьютерной информации: дис. ... канд. юрид. наук 12.00.10. – М., 2006.

[6] См., например: Касенова М.Б. Управление Интернетом. Международно-правовой механизм: монография. – СПб.: Центр гуманитарных инициатив, 2013; Русскевич Е.А. Уголовное право и «цифровая преступность». Проблемы и решения: монография – М: ИНФРА-М, 2019; Киберпространство БРИКС: правовое измерение: монография. / И.И. Шувалов, Т.Я. Хабриева, Фэн Цзинжу и др.; отв. ред. Дэн Руйпин, Т.Я. Хабриева; сост.

Ряд работ посвящен различным аспектам противодействия преступлениям в сфере информационных технологий, таким как: вопросы обеспечения информационной безопасности (И.Л. Бачило, Е.С. Зиновьева, А.В. Крутских, И.П. Михнев, А.А. Стрельцов, В.П. Шерстюк); уголовно-правовой анализ современных проблем (С.Д. Бражник, С.Ю. Бытько, А.Г. Волеводз, М.А. Ефремова, Т.Л. Тропина); перспективы развития правового регулирования информационной сферы и международного сотрудничества в данной области (А.Х. Абашидзе, П.Н. Бирюков, А.А. Ефремов, Ю.Н. Жданов, М.В. Ильяшевич, К.О. Кебурия, М.В. Мажорина, В.Б. Наумов, В.С. Овчинский, И.М. Рассолов, А.М. Солнцев, А.Ж. Степанян)[7].

Методологическую основу исследования составляют общие методы познания, такие как: формально-логический (в процессе анализа результатов сотрудничества государств по противодействию преступлениям в сфере информационных технологий), системно-структурный (в целях определения особенностей функционирования институциональных механизмов противодействия преступлениям в сфере информационных технологий, а также актуальных тенденций их развития), эмпирический (в целях выработки рекомендаций по совершенствованию действующих механизмов противодействия преступлениям в сфере информационных технологий), а также частно-научные методы: формально-юридический (в ходе исследования вопросов системы толкования норм международного и внутригосударственного права, регулирующих вопросы противодействия преступлениям в сфере информационных технологий) и сравнительно-правовой (в целях определения особенностей действующих региональных международных договоров, для выявления имеющихся правовых коллизий, предложения путей их разрешения

Жун Фу, Н.М. Бевеликова. – М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2017.

[7] См., например: Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции. дис. … докт. полит. наук: 23.00.04 – М., 2019; Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: Юрлитинформ, 2001.

и определения наиболее актуальных международных норм по противодействию преступлениям в сфере информационных технологий).

Теоретическую основу диссертации составляют научные труды отечественных и зарубежных ученых.

Так, теоретические аспекты, связанные с противодействием преступлениям в сфере информационных технологий и сотрудничеством государств в исследуемой области, нашли отражение в работах таких отечественных авторов как: А.Х. Абашидзе, М.М. Бирюков, П.Н. Бирюков, И.П. Блищенко, С.В. Бородин, А.Г. Волеводз, Л.Н. Галенская, Е.Г. Ляхов, Р.А. Каламкарян, А.Я. Капустин, Ю.М. Колосов, И.И. Котляров, Т.М. Лопатина, И.И. Лукашук, И.М. Рассолов, Г.И. Тункин, Т.Я. Хабриева, С.В. Черниченко, М.Л. Энтин и другие.

Значимый вклад в исследование теоретических проблем сотрудничества государств по противодействию преступлениям в сфере информационных технологий внесли следующие зарубежные ученые: Д. Бец, Л.Р. Блэнк, Л. Гринберг, С. Гудман, Х.Х. Деннисс, А. Камал, Г. Кершишниг, Дэн Руйпин и другие.

Нормативно-правовую основу исследования составляют Конвенция ООН против транснациональной организованной преступности 2000 г., Конвенция Совета Европы (далее – СЕ) о киберпреступности 2001 г., Конвенция АС о кибербезопасности и защите персональных данных 2014 г., 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., Соглашение между правительствами государств – членов Шанхайской организации сотрудничества (далее – ШОС) о сотрудничестве в области обеспечения информационной безопасности 2009 г., международные акты мягкого права, принятые в рамках международных организаций, материалы международных конференций, посвященных рассматриваемой проблеме, национальное законодательство Российской Федерации и ряда других

государств в области противодействия преступлениям в сфере информационных технологий.

Эмпирическую основу исследования составляют статистические и аналитические данные о результатах деятельности правоохранительных органов Российской Федерации и международных организаций по противодействию преступлениям в сфере информационных технологий.

Научная новизна отражается в следующих результатах исследования:

- авторское определение понятия «преступление в сфере информационных технологий», разработанное с учетом широкого подхода к толкованию в целях уточнения предмета сотрудничества государств по противодействию данному виду преступлений;

- авторская типология преступлений в сфере информационных технологий, включающая семь типов, выделяемых в зависимости от объекта и предмета преступного посягательства;

- международно-правовая характеристика несогласованности современных подходов относительно регулирования сотрудничества государств по противодействию преступлениям в сфере информационных технологий с учетом отсутствия универсального международного договора, а также фрагментарности и разрозненности положений региональных источников;

- выявление особенностей функционирования институциональных механизмов сотрудничества государств по противодействию преступлениям в сфере информационных технологий, которые позволяют получить наиболее полное представление о современном состоянии и роли тех или иных институциональных механизмов в осуществлении межгосударственного взаимодействия в рассматриваемой области;

- выявление особенностей формирования в различных международных организациях специализированных структур, деятельность которых направлена на противодействие преступлениям в сфере информационных технологий посредством разработки передовых решений относительно методик цифровой

криминалистики, раскрытия и расследования преступлений, содействия правоохранительным органам государств в извлечении, сохранении и анализе данных, изъятых с цифровых устройств, проведения учебных мероприятий, прогнозирования криминальных угроз, организации сотрудничества правоохранительных органов с частными партнерами и научным сообществом;

- обоснование необходимости учреждения Центра по противодействию преступлениям в сфере информационных технологий СНГ, создание которого позволит повысить эффективность международного сотрудничества в данном направлении на пространствах государств – участников СНГ;

- международно-правовая характеристика государственно-частного партнерства по противодействию преступлениям в сфере информационных технологий с учетом возрастающей потребности в оперативной реализации информационно-аналитических и технических задач, нехватки специализированных кадров, а также недостаточной технологической оснащенности сотрудников правоохранительных органов;

- предложения относительно приведения российского уголовного законодательства в соответствие с терминологией, используемой в Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 г., учет которых может способствовать достижению наиболее полного понимания содержания преступлений в сфере информационных технологий и предотвращению избыточного закрепления статей и квалифицирующих признаков в Особенной части Уголовного кодекса Российской Федерации, криминализирующих различные противоправные деяния, совершаемые с использованием информационных технологий;

- введение в научный оборот в авторском переводе аутентичных международно-правовых текстов универсальных и региональных международных организаций, связанных с противодействием преступлениям в сфере информационных технологий.

Научная новизна диссертационного исследования находит свое выражение в следующих **положениях, выносимых на защиту:**

1. Под преступлением в сфере информационных технологий следует понимать противоправное общественно опасное виновно совершенное уголовно наказуемое деяние, причиняющее вред или создающие опасность причинения вреда личности, государству или международному сообществу, предметом посягательства которого являются информационные технологии и/или которое совершено с использованием информационных технологий.

2. Сформировалась тенденция международно-правового закрепления новационных форм сотрудничества государств по противодействию преступлениям в сфере информационных технологий. К таковым, 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.

3. Функционирование институционального механизма ООН по противодействию преступлениям в сфере информационных технологий осуществляется с учетом следующих тенденций: возрастающая необходимость реализации эффективного международного сотрудничества; увеличение роли нормативно-правовых основ межгосударственного взаимодействия и возможностей правоохранительных органов; взаимосвязанность преступлений в сфере информационных технологий с транснациональной организованной преступностью, в том числе с терроризмом; потребность в согласовании положений о криминализации, процессуальных полномочиях правоохранительных органов, а также о вопросах определения юрисдикции и получения цифровых доказательств; повышение актуальности оперативного реагирования на запросы о взаимной правовой помощи; активизация разработки практических мер по минимизации угроз для детей, возникающих в сфере информационных технологий.

4. Потребность в активизации регионального сотрудничества на пространствах государств – участников СНГ предопределяет необходимость создания Центра по противодействию преступлениям в сфере информационных технологий, к компетенции которого следует отнести: организацию проведения согласованных межведомственных профилактических, оперативно-разыскных мероприятий и специальных операций по противодействию преступлениям в рассматриваемой сфере; участие в разработке межгосударственных программ по борьбе с преступлениями в сфере информационных технологий; содействие государствам – участникам в подготовке кадров, специализирующихся в области противодействия преступлениям в сфере информационных технологий.

5. Деятельность международных полицейских организаций по противодействию преступлениям в сфере информационных технологий характеризуется наличием следующих закономерностей: возрастающая актуальность разработки передовых решений в области цифровой криминалистики; потребность в прогнозировании криминальных угроз; необходимость развития сотрудничества с частными партнерами и научным сообществом; повышенная значимость способности оперативного реагирования в случаях противоправного воздействия на объекты критической информационной инфраструктуры; важность разработки и реализации эффективных мер предупреждения преступлений в сфере информационных технологий; уделение особого внимания противодействию распространению материалов о сексуальном насилии над детьми; активизация борьбы с функционированием Интернет-платформ, предусматривающих возможность торговли наркотиками, оружием, данными банковских карт, поддельными документами и другими запрещенными или ограниченными в обороте товарами и услугами.

6. Развитие государственно-частного партнерства является значимой тенденцией международного сотрудничества по противодействию преступлениям в сфере информационных технологий. К числу наиболее перспективных направлений данного взаимодействия следует отнести:

разработку программного обеспечения для выявления предупреждения и пресечения киберугроз; организацию мероприятий по мониторингу информационных ресурсов; развитие аналитических технологий для обработки массивов информации; проведение компьютерных экспертиз; осуществление сбора цифровых доказательств; сотрудничество в области подготовки и переподготовки специализированных кадров, совершенствование правовых основ, регулирующих вопросы противодействия преступлениям в сфере информационных технологий. Указанные направления государственно-частного партнерства являются наиболее актуальными, поскольку компенсируют сформировавшуюся в правоохранительных органах нехватку специальных навыков, а также оборудования и программного обеспечения, необходимых для эффективного противодействия преступности и имеют значение для успешной реализации мер противодействия преступлениям в сфере информационных технологий, разработанных международными организациями.

7. В целях совершенствования сотрудничества правоохранительных органов Российской Федерации с компетентными органами зарубежных государств по раскрытию и расследованию преступлений в сфере информационных технологий следует активизировать: заключение соглашений об информационном взаимодействии и обмене информацией в электронном виде по вопросам, относящимся к компетенции органов внутренних дел; использование потенциала межгосударственных следственно-оперативных групп; разработку международных стандартов, которым должны соответствовать доказательства, полученные из информационного пространства, и результаты проведения соответствующих экспертиз.

8. В целях приведения российского уголовного законодательства в соответствие с терминологией, используемой в Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 г., необходимо внести следующие изменения в Уголовной кодекс Российской Федерации: в названии главы 28

слова «компьютерной информации» заменить словами «информационных технологий»; исключить из названий, а также из текста статей 272-274.1 слова «компьютерных», «компьютерной». Кроме того, в главу 28 следует включить статью 274.2 «Преступления, совершаемые с использованием информационных технологий», и изложить ее в следующей редакции:

«Преступления, которые содержатся в других главах Особенной части настоящего Кодекса и совершаются с использованием информационных технологий, квалифицируются согласно положениям соответствующих статей и не требуют дополнительной криминализации».

Теоретическая значимость диссертационного исследования определяется актуальностью и новизной исследуемой проблемы и заключается в том, что результаты исследования вносят определенный вклад в развитие доктрины международного права в части, касающейся сотрудничества государств по противодействию преступлениям в сфере информационных технологий. Материалы исследования могут дополнить теоретическую основу таких отраслей международного публичного права, как международное уголовное право и право международных организаций.

Практическая значимость диссертационного исследования заключается в том, что основные положения и выводы, сформулированные в результате его проведения, могут быть использованы:

- в деятельности международных организаций по разработке новых и дополнению действующих международно-правовых актов;

- в деятельности российских внешнеполитических органов при подготовке проектов международных документов по вопросам противодействия преступлениям в сфере информационных технологий;

- в деятельности правоохранительных органов Российской Федерации и зарубежных государств по противодействию преступлениям в сфере информационных технологий;

- в осуществлении преподавательской деятельности и последующей научно-исследовательской работы.

Апробация результатов исследования. Материалы и результаты исследования освещались в период с 2018 года по 2021 год в ходе семи международных, девяти всероссийских и одной межвузовской конференций.

Результаты диссертационного исследования внедрены в учебный процесс и в научную деятельность Московского университета МВД России имени В.Я. Кикотя, а также в практическую деятельность Национального центрального бюро Интерпола МВД России.

Структура диссертации включает введение, три главы, объединяющие семь параграфов, заключение и список использованной литературы.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность диссертационного исследования, определяются его объект, предмет, цель и научные задачи, также выделяются теоретические и методологические основы работы, формулируются научная новизна и положения, выносимые на защиту, раскрываются теоретическая и практическая значимость диссертационного исследования, апробация его результатов.

Первая глава – «Теоретико-правовые аспекты формирования юридических основ сотрудничества государств по противодействию преступлениям в сфере информационных технологий» – посвящена исследованию проблем международно-правового регулирования, связанных с развитием понятийного аппарата и формированием правовых основ межгосударственного взаимодействия в рассматриваемой сфере.

В ***первом параграфе*** – *«Проблемы развития понятийного аппарата международного сотрудничества по противодействию преступлениям в сфере информационных технологий»* – раскрываются различные подходы относительно понятий, используемых в рассматриваемой сфере и составов противоправных деяний, подлежащих криминализации, формулируются авторские предложения относительно заявленной проблематики.

Диссертантом уделяется внимание различным точкам зрения в отношении терминологии, применяемой в исследуемой области. Обосновывается необходимость использования широкого подхода к определению преступлений в сфере информационных технологий, в соответствии с которым к противоправным деяниям в данной сфере необходимо относить как преступления, предметом посягательства которых являются информационные технологии, так и преступления, совершаемые с использованием информационных технологий. Предлагается международно-правовое закрепление и введение в научный оборот авторского понятия «преступление в сфере информационных технологий», под которым следует

понимать противоправное общественно опасное виновно совершенное уголовно наказуемое деяние, причиняющее вред или создающие опасность причинения вреда личности, государству или международному сообществу, предметом посягательства которого являются информационные технологии и/или которое совершено с использованием информационных технологий. Приводится соотношение понятий «преступление в сфере информационных технологий», «угроза информационной безопасности», «кибепреступление», «преступление в сфере компьютерной информации», «Интернет-преступление».

Диссертантом разработана авторская типология преступлений в сфере информационных технологий, включающая семь типов, каждый из которых сопровождается соответствующими примерами из российского и зарубежного уголовного законодательства: преступления, основным предметом посягательства которых являются информационные технологии; преступления против личности, совершаемые с использованием информационных технологий; преступления в сфере экономики, совершаемые с использованием информационных технологий; преступления против общественной безопасности и общественного порядка, совершаемые с использованием информационных технологий; преступления против государственной власти, совершаемые с использованием информационных технологий; преступления против военной службы, совершаемые с использованием информационных технологий; преступления против мира и безопасности человечества, совершаемые с использованием информационных технологий. В качестве основания представленной типологии выступают объект и предмет преступного посягательства.

Анализ зарубежного уголовного законодательства позволил выделить три основных варианта криминализации преступлений в сфере информационных технологий: разработка специального нормативного правового акта, закрепление специальной главы или раздела в уголовном кодексе, криминализация преступлений в сфере информационных технологий по тексту

всего уголовного законодательства, не предусматривающая наличия специальной главы. Наиболее распространенным вариантом криминализации преступлений в сфере информационных технологий является закрепление составов противоправных деяний в рамках специальной главы уголовного кодекса. Такой подход находит отражение и в Уголовном кодексе Российской Федерации (далее – УК РФ).

В целях приведения российского уголовного законодательства в соответствие с терминологией, используемой в Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 г. предлагается внести следующие изменения в Уголовной кодекс Российской Федерации: в названии главы 28 слова «компьютерной информации» заменить словами «информационных технологий»; исключить из названий, а также из текста статей 272-274.1 слова «компьютерных», «компьютерной». Кроме того, в главу 28 следует включить статью 274.2 «Преступления, совершаемые с использованием информационных технологий», и изложить ее в следующей редакции:

«Преступления, которые содержатся в других главах Особенной части настоящего Кодекса и совершаются с использованием информационных технологий, квалифицируются согласно положениям соответствующих статей и не требуют дополнительной криминализации».

Второй параграф *– «Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий»* – посвящен исследованию проблемы заключения универсального международного договора в рассматриваемой области, а также ключевых положений международно-правовых актов, регулирующих противодействие преступности в данной сфере.

Диссертантом раскрыта проблема отсутствия универсального международного договора, координирующего сотрудничество государств по противодействию преступлениям в сфере информационных технологий, в

частности, исследованы позиции государств по данному вопросу и сформулированы следующие выводы.

1. Многие государства – члены ООН (например, Соединенные Штаты Америки, Канада, Великобритания) отмечают, что реализация положений Конвенции СЕ о киберпреступности 2001 г. обеспечивает эффективные результаты, в связи с чем разработки международного договора под эгидой ООН не требуется, и рекомендуют всем другим государствам присоединиться к Будапештской конвенции, поскольку: Конвенция СЕ о киберпреступности 2001 г. получила признание 63 государств из всех региональных групп международного общества; следует сосредоточить внимание на увеличении количества участников Конвенции СЕ о киберпреступности 2001 г. в целях недопущения потенциального дублирования усилий; в настоящее время Будапештская конвенция является ведущим международным документом по киберпреступности и обеспечивает прочную правовую основу международного сотрудничества в борьбе с киберпреступностью, а также предусматривает конкретные меры, доказавшие свою эффективность на практике.

2. Государства – члены ООН, которые не являются участниками Будапештской конвенции (более половины государств современного международного сообщества, среди которых: Российская Федерация, Республика Беларусь, Китайская Народная Республика, Индия и др.), придерживаются противоположной точки зрения по следующим основаниям: в процессе разработки Конвенции СЕ о киберпреступности 2001 г. принимало участие ограниченное количество государств, в связи с чем не учтены интересы всех государств – членов ООН; ст. 32 Конвенции СЕ 2001 г. о трансграничном доступе к хранящимся компьютерным данным позволяет различным спецслужбам без официального уведомления проводить операции в компьютерных сетях иностранных государств; рассматриваемая Конвенция не охватывает вопросы противодействия использованию информационных технологий в террористических целях, в то время как ООН провозглашает обозначенную проблему в качестве одного из приоритетных направлений

развития международного сотрудничества в исследуемой сфере; государства, которые не согласны принять обязательства, предусмотренные Будапештской конвенцией, пользуются в лучшем случае лишь региональными правовыми основами, что снижает эффективность международного сотрудничества.

Тем не менее, в рамках 74-й сессии Генеральной Ассамблеи ООН большинством голосов одобрена Резолюция A/RES/74/247 от 27 декабря 2019 г., предусматривающая учреждение специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. В рамках работы Спецкомитета предусмотрено проведение восьми сессий в Вене с августа 2021 г. по конец июня 2024 г. и представление текста конвенции в виде проекта резолюции Генеральной Ассамблее ООН для рассмотрения и принятия на семьдесят девятой сессии в 2024 г.

Автором установлено, что в связи с отсутствием универсального международного договора по противодействию преступлениям в сфере информационных технологий особое значение приобретает правовой анализ региональных источников, в частности, Конвенции СЕ о киберпреступности 2001 г., Соглашения между правительствами государств – членов ШОС о сотрудничестве в области обеспечения информационной безопасности 2009 г., Конвенции ЛАГ о борьбе с преступлениями в сфере информационных технологий 2010 г., Конвенции АС о кибербезопасности и защите персональных данных 2014 г. и Соглашения о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 г. Результаты юридического анализа обозначенных международных договоров свидетельствует о том, что:

- основной целью заключения международно-правовых актов в исследуемой области, является повышение эффективности сотрудничества государств по противодействию преступлениям в сфере информационных технологий, главным образом, посредством формирования международно-

правовых основ и согласования деятельности правоохранительных органов;

- закономерность анализируемых международных договоров заключается в закреплении специфических понятий, имеющих значение для рассматриваемой сферы, вместе с тем наблюдается несогласованность терминов, используемых в различных источниках;

- разрозненность перечней составов преступлений, закрепленных в региональных международных договорах, регулирующих сотрудничество государств по противодействию преступлениям в сфере информационных технологий, обусловлена расхождением подходов к осуществлению межгосударственного взаимодействия в различных регионах;

- наблюдается тенденция международно-правового закрепления новационных форм сотрудничества государств, специфических для сферы информационных технологий, среди которых: оперативное обеспечение сохранности и частичное раскрытие данных о потоках информации; сбор в режиме реального времени данных о потоках информации; взаимная помощь в отношении информации, связанной с содержанием конкретных сообщений;

- несогласованность положений исследуемых международных договоров относительно закрепляемых понятий, перечней составов преступлений, подлежащих криминализации, а также форм межгосударственного взаимодействия затрудняет сотрудничество между государствами из разных регионов, поскольку общепринятые подходы на сегодняшний день по данным вопросам отсутствуют.

Учет предложений, разработанных автором в параграфе 1.1., может способствовать преодолению несогласованности положений международных договоров, регулирующих сотрудничество государств в рассматриваемой сфере.

Двусторонние международные договоры России в исследуемой области достаточно схожи по содержанию и характеризуются тем, что они: основаны на общепризнанных принципах и нормах международного права; закрепляют ключевые аспекты сотрудничества государств по обеспечению

информационной безопасности и противодействию преступлениям в сфере информационных технологий; предусматривают обязательство воздержаться от кибератак; фиксируют право на защиту информационных ресурсов государства от неправомерного использования и несанкционированного воздействия; позволяют обеспечить формирование взаимного доверия.

Вторая глава – «Система институциональных механизмов сотрудничества государств по противодействию преступлениям в сфере информационных технологий» – посвящена исследованию особенностей и закономерностей развития институциональных механизмов межгосударственного взаимодействия в рамках заявленной проблематики, функционирующих в различных международных организациях.

В ***первом параграфе*** *– «Институциональный механизм сотрудничества государств по противодействию преступлениям в сфере информационных технологий, сформированный в Организации Объединенных Наций» –* проанализированы основные форматы межгосударственного взаимодействия в исследуемой области под эгидой ООН.

Диссертантом отмечается, что основными элементами институционального механизма ООН по противодействию преступлениям в сфере информационных технологий являются специализированные структуры, к числу которых представляется целесообразным отнести: Группу правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности; Рабочую группу по международной информационной безопасности открытого состава; Группу экспертов для проведения всестороннего исследования проблемы киберпреступности; Специальный межправительственный комитет экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Каждой из обозначенных специализированных структур отводится определенная роль. При этом в своей деятельности они учитывают результаты, достигнутые в данном направлении другими

структурами, а также органами и специализированными учреждениями ООН, что позволяет исключить дублирование усилий и наиболее эффективно осуществлять международное сотрудничество по противодействию преступлениям в сфере информационных технологий на универсальном уровне.

Анализ резолюций и аналитических документов по противодействию преступлениям в сфере информационных технологий различных органов ООН позволил соискателю выявить основные черты институционального механизма ООН, работа которого сосредоточена, главным образом, на инициативах по совершенствованию международно-правовых основ, стратегических направлений и концепций противодействия преступлениям в сфере информационных технологий, а также планов работы по их реализации. При этом главные органы определяют задачи и тенденции развития международного сотрудничества, а специализированные структуры осуществляют изучение основных проблем, потенциальных угроз в данной сфере и выработку практических мер по достижению поставленных задач.

Исследование докладов о результатах деятельности специализированных структур ООН по противодействию преступлениям в сфере информационных технологий позволило определить наиболее актуальные практические меры, разработанные в данной сфере, такие как: создание контактных центров для реализации сотрудничества государств по противодействию преступлениям в сфере информационных технологий; разработка механизмов проведения двусторонних, региональных, субрегиональных и многосторонних консультаций; укрепление доверия в рамках региональных и многосторонних форумов; создание международной базы данных с наилучшими практиками по развитию национального законодательства и совершенствованию стратегий в рассматриваемой сфере; создание дополнительных механизмов для рассмотрения запросов о правовой помощи по уголовным делам о преступлениях в сфере информационных технологий; развитие возможностей проведения цифровых экспертиз.

Второй параграф *– «Вклад Российской Федерации в формирование региональных институциональных основ сотрудничества государств по противодействию преступлениям в сфере информационных технологий»* **–** посвящен исследованию инициатив России относительно совершенствования институциональных механизмов межгосударственного взаимодействия в исследуемой области с региональными партнерами на примере СНГ и ШОС.

В условиях устойчивого роста преступлений в сфере информационных технологий на территориях государств – участников СНГ осуществляется консолидация усилий по противодействию угрозам, возникающим в информационном пространстве. В частности, Совет министров внутренних дел СНГ (далее – СМВД) совместно с Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств – участников СНГ (далее – БКБОП) осуществляют работу по следующим основным направлениям: совершенствование правовых основ международного сотрудничества в области борьбы с преступлениями, совершаемыми с использованием информационных технологий; развитие взаимодействия с международными организациями и центрами, занимающимися противодействием преступлениям, совершаемым с использованием информационных технологий; развитие сотрудничества в области разработки, производства, поставки и оказания помощи государствам – участникам по внедрению специальных программно-технических средств, необходимых для обнаружения, фиксации, изъятия и исследования следов преступлений, совершаемых с использованием информационных технологий; развитие и использование Объединенного банка данных органов безопасности и специальных служб государств – участников СНГ по борьбе с организованной преступностью и др.

Изучение задач, решаемых СМВД совместно с БКБОП по противодействию преступлениям в сфере информационных технологий, позволило сделать вывод о том, что они носят преимущественно технический, информационный и нормативный характер. Вместе с тем в настоящее время

возникла необходимость перехода от координации и связанного с ней информационного обеспечения к согласованному правоохранительному взаимодействию государств. В этой связи, диссертантом предлагается создание Центра по противодействию преступлениям в сфере информационных технологий СНГ, к компетенции которого, прежде всего, следует отнести организацию проведения согласованных межведомственных профилактических, оперативно-разыскных мероприятий и специальных операций по противодействию преступлениям в рассматриваемой сфере.

Не менее активно Россия осуществляет взаимодействие с зарубежными партнерами на евразийском пространстве по линии ШОС. Начиная с 2006 г. государства – члены ШОС предприняли ряд важных шагов по формированию основ региональной системы международной информационной безопасности. В частности, значимым событием стало учреждение Группы экспертов по международной информационной безопасности, в результате деятельности которой разработано Соглашение между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности 2009 г. Кроме того, ШОС удалось разработать Правила поведения в области обеспечения международной информационной безопасности. Данный документ стал первым официальным представлением согласованной позиции Российской Федерации и ее партнеров по ШОС, основанной на идее необходимости регулирования поведения государств в информационном пространстве.

Анализ декларативных документов ШОС подтверждает готовность государств – членов укреплять сотрудничество в области борьбы с преступлениями в информационной сфере посредством организации мониторинга потенциальных угроз в информационном пространстве и повышения эффективности противодействия подобным угрозам. Практическая деятельность по противодействию террористической активности в информационном пространстве осуществляется на базе Региональной антитеррористической структуры ШОС (далее – РАТС). Исследование

результатов ее деятельности позволило сделать вывод о том, что на протяжении многих лет при координирующей роли РАТС успешно проходят совместные учения компетентных органов по выявлению и пресечению использования сети Интернет в террористических целях. Данные учения позволяют осуществлять обмен опытом по установлению личности пользователей, осуществляющих распространение материалов террористического характера, исследованию изъятого у них оборудования и сбору электронных доказательств.

В результате анализа итогов саммитов ШОС последних лет диссертантом определена перспектива создания Центра информационной безопасности на базе РАТС. Представляется, что реализация указанной инициативы станет логическим продолжением тенденции создания специализированных структур в исследуемой области, а также значительно повысит эффективность противодействия преступлениям в сфере информационных технологий.

В ***третьем параграфе*** – *«Институциональные механизмы полицейского сотрудничества по противодействию преступлениям в сфере информационных технологий»* – проанализированы основополагающие элементы механизмов межгосударственного взаимодействия, функционирующих под эгидой Интерпола и региональных полицейских организаций.

Автором установлено, что основным элементом институционального механизма Интерпола по противодействию преступлениям в сфере информационных технологий является Глобальный комплекс инноваций. Исследование аналитических документов, разработанных Глобальным комплексом, позволило выявить следующие ключевые тенденции противодействия преступлениям в сфере информационных технологий под эгидой Интерпола: возрастание роли прогнозирования криминальных угроз; актуализация развития сотрудничества с частными партнерами и научным сообществом; необходимость сокращения разрыва в технологических возможностях между различными национальными правоохранительными

органами; появление новационных разновидностей преступлений в результате развития технологий искусственного интеллекта и робототехники.

Следует также отметить деятельность Рабочей группы Интерпола по Даркнету и криптовалютам, решающей актуальные задачи: создания глобальной базы данных криминальных криптовалютных кошельков; сбора и стандартизации данных криптовалютной аналитики; оценки угрозы функционирования таких сетей, как I2P и Freenet. Диссертантом определено, что Рабочая группа по Даркнету и криптовалютам оказывает экспертное практическое содействие государствам – членам в борьбе с преступлениями в сфере информационных технологий, исследуя инструменты противоправной активности и обмениваясь через глобальное экспертное сообщество лучшими практиками раскрытия и расследования преступлений, совершаемых в Даркнете и при помощи криптовалют.

Интерпол организует множество эффективных операций по противодействию преступлениям в сфере информационных технологий. Исследование результатов проведения международных полицейских операций в данной сфере позволило определить наиболее значимые среди них. В частности, ключевую роль играют операции «кибер-всплеска», которые проводятся в целях выявления командных и контрольных серверов, распространяющих различные типы вредоносных программ. Необходимо обратить внимание и на такие операции, как «Goldfish Alpha» по противодействию криптоджекингу (использование ресурсов скомпрометированного устройства для генерации криптовалюты без ведома его владельца) и «Night Fury» по пресечению использования вредоносного программного обеспечения Java Script (похищающего персональные данные покупателей, а также информацию о платежных картах клиентов).

Значительный вклад в раскрытие и расследование преступлений в сфере информационных технологий вносит также Европол, учредивший в 2013 г. Европейский центр киберпреступности (далее – ЕЦК). В ЕЦК работают специальные группы по цифровой криминалистике, стратегическому анализу и

развитию отношений с частными партнерами. Особая роль отводится Совместной рабочей группе по борьбе с киберпреступностью, ключевой задачей которой является координация международных полицейских операций. Анализ деятельности указанных специализированных структур позволил установить, что в совокупности они составляют институциональный механизм Европола по противодействию преступлениям в сфере информационных технологий, который: является ключевым центром сбора оперативной информации и разведданных; позволяет успешно реализовывать трансграничные полицейские операции; обеспечивает комплексную информационно-пропагандистскую функцию; организует взаимодействие правоохранительных органов с частными партнерами и научным сообществом; содействует подготовке специалистов в сфере информационных технологий; предоставляет узкоспециализированные возможности технической и цифровой поддержки государствам – членам. Среди значимых полицейских операций Европола следует отметить, в первую очередь, «IM-RAT» (по противодействию распространению вредоносного программного обеспечения удаленного доступа IM-RAT), «Chemosh» (по борьбе с распространением в зашифрованных группах WhatsApp материалов о сексуальном насилии над детьми).

Африпол также как и другие международные полицейские организации уделяет большое внимание вопросам противодействия преступлениям в сфере информационных технологий. Интерпол оказывает содействие правоохранительным органам африканских государств в разработке и дальнейшей реализации инициативных стратегий, создает технические и оперативные условия для эффективного обмена информацией и повышения навыков по раскрытию и расследованию транснациональных преступлений. Так, начиная с 2017 г., успешно реализуется проект «ENACT» – первый в своем роде проект, охватывающий весь африканский континент. В Африке все чаще встречаются инциденты с вредоносным программным обеспечением. Социальные сети используются для облегчения незаконного ввоза мигрантов, о чем свидетельствует 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.

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. В частности, следует отметить Проект по развитию кибер-потенциала АСЕАН, направленный на укрепление способности государств региона бороться с киберпреступностью, который расширяет возможности сотрудничества государств по вопросам противодействия киберпреступности и обеспечивает основу для улучшения обмена информацией о киберугрозах. Кроме того, установлено, что в данном регионе наблюдаются значительные успехи в организации обучения специализированных кадров, достигнутые во многом благодаря успешной работе Совещания по сотрудничеству в области подготовки сотрудников полиции АСЕАН.

Диссертантом выявлены следующие закономерности деятельности международных полицейских организаций в исследуемой области: возрастающая актуальность разработки передовых решений в области цифровой криминалистики; потребность в прогнозировании криминальных угроз; необходимость развития сотрудничества с частными партнерами и научным сообществом; повышенная значимость способности оперативного реагирования в случаях противоправного воздействия на объекты критической информационной инфраструктуры; важность разработки и реализации эффективных мер предупреждения преступлений в сфере информационных технологий; уделение особого внимания противодействию распространению материалов о сексуальном насилии над детьми; активизация борьбы с функционированием Интернет-платформ, предусматривающих возможность торговли наркотиками, оружием, данными банковских карт и другими запрещенными или ограниченными в обороте товарами и услугами.

Третья глава – «Тенденции международно-правового сотрудничества государств по противодействию преступлениям в сфере информационных технологий» – посвящена изучению наиболее актуальных перспектив в исследуемой области по развитию государственно-частного партнерства и совершенствованию деятельности правоохранительных органов.

В ***первом параграфе*** – *«Развитие государственно-частного партнерства по противодействию преступлениям в сфере информационных технологий»* – проведен анализ современного состояния сотрудничества государств с частными партнерами, компетентными в вопросах обеспечения информационной безопасности.

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

Интерпол, Европол и другие международные полицейские организации являются сторонниками привлечения к межгосударственному взаимодействию частных партнеров. В параграфе рассмотрен вклад в противодействие преступлениям в сфере информационных технологий таких частных партнеров, как Microsoft, Лаборатория Касперского, ПАО Сбербанк, Глобальный форум групп реагирования на компьютерные инциденты и угрозы безопасности.

Изучение специфики деятельности частных партнеров позволило выявить перспективные направления развития государственно-частного взаимодействия в сфере информационных технологий, например, такие как: 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.

Второй параграф *– «Перспективы совершенствования деятельности правоохранительных органов Российской Федерации по раскрытию и расследованию преступлений в сфере информационных технологий»* – посвящен исследованию актуальных направлений развития межгосударственного взаимодействия по линии правоохранительных органов.

Диссертантом рассмотрены современные проблемы раскрытия и расследования преступлений в сфере информационных технологий, с которыми сталкиваются следователи, эксперты-криминалисты и сотрудники оперативных подразделений полиции. Проанализированы различные точки зрения ученых по вопросам развития международного сотрудничества и разработки международных стандартов в исследуемой области, определения юрисдикции, использования цифровых доказательств и др.

Автором установлено, что одной из наиболее значимых перспектив совершенствования работы правоохранительных органов по противодействию преступлениям в сфере информационных технологий выступает внедрение инноваций в практическую деятельность сотрудников различных подразделений. В частности, большое значение для МВД России имеет возможность обмена 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.

С точки зрения активизации международного сотрудничества по раскрытию и расследованию преступлений в сфере информационных технологий широкие перспективы для совершенствования деятельности правоохранительных органов открывает возможность создания межгосударственных следственно-оперативных групп, предусмотренная Соглашением о порядке создания и деятельности совместных следственно-оперативных групп на территориях государств – участников СНГ 2015 г. Рассматриваемый формат взаимодействия позволяет осуществлять: своевременное обнаружение, фиксацию, изъятие и исследование цифровых доказательств; обмен опытом, специальным оборудованием и программным обеспечением; разработку согласованной стратегии раскрытия и расследования преступлений с учетом законодательства государств, компетентные органы которых сформировали совместную следственно-оперативную группу; эффективное решение вопросов юрисдикции.

Кроме того, представляется обоснованным обеспечить возможность эффективного использования при проведении расследований и вынесении судебных решений доказательств, полученных из информационного пространства и проведения соответствующих экспертиз. В частности, на международно-правовом уровне следует закрепить необходимость признания указанных доказательств и экспертиз, полученных от компетентных органов иностранных государств.

При этом особую актуальность представляет разработка международных стандартов относительно терминологии и требований, которым должны соответствовать доказательства и результаты экспертиз. В том числе

необходимо подробное разъяснение на международно-правовом уровне понятий «след», «доказательство» и «экспертиза», которые должны употребляться в сочетании со специальным единым прилагательным, избранным специалистами в сфере судебно-экспертной деятельности из числа таких, как «компьютерный», «цифровой», «электронный», «информационный».

В **заключении** формулируются основные выводы и предложения по итогам диссертационного исследования.

Основные положения диссертации отражены в следующих работах:

Статьи, опубликованные в ведущих рецензируемых научных журналах и изданиях, входящих в перечень ВАК при Минобрнауки России:

1. Мысина А.И. Международно-правовые основы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Международное право. 2019. № 1. С.18-27 (0,4 п.л.).

2. Мысина А.И. К вопросу о региональных правовых основах сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Российская юстиция. 2019. № 5. С. 20-24 (0,5 п.л.).

3. Мысина А.И. Приоритетные направления сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Вестник Московского университета МВД России. 2019. № 6. С. 200-203 (0,3 п.л.).

4. Мысина А.И. Региональные механизмы сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Современное право. 2020. № 1. С. 119-124 (0,5 п.л.).

5. Мысина А.И. Сотрудничество государств по противодействию преступлениям в сфере информационных технологий на платформе Глобального комплекса инноваций Интерпола // Вестник экономической безопасности. 2020. № 2. С. 128-131 (0,2 п.л.).

Статьи, опубликованные в иных изданиях:

1. Мысина А.И. К вопросу о международно-правовом регулировании транснационального сотрудничества в борьбе с преступлениями в сфере информационных технологий // Актуальные проблемы международного сотрудничества в борьбе с преступностью: сборник статей по итогам Международной научно-практической конференции, приуроченной к 20-летию принятия Генеральной Ассамблеей ООН Международной конвенции о борьбе с финансированием терроризма 1999 г. 2019. С. 91-95 (0,2 п.л.).

2. Мысина А.И. Региональные механизмы международного сотрудничества в борьбе с преступлениями в сфере информационных технологий // Актуальные проблемы противодействия органов внутренних дел (полиции) государств – участников Содружества Независимых Государств преступлениям, совершаемым с использованием информационных технологий: сборник научных трудов международной научно-практической конференции. 2019. С. 38-42 (0,2 п.л.).

3. Мысина А.И. Международно-правовое регулирование противодействия финансированию терроризма с использованием информационных технологий // Противодействие терроризму и экстремизму в информационных системах: сборник материалов Всероссийской научно-практической конференции. 2019. С. 46-49 (0,2 п.л.).

4. Мысина А.И. Международное сотрудничество по противодействию компрометации деловой электронной почты // Борьба с киберпреступностью в условиях развития цифрового общества: сборник научных статей Международной конференции. 2019. С. 95-98 (0,2 п.л.).

5. Мысина А.И. Использование Интернета вещей в целях совершения транснациональных преступлений // Вопросы совершенствования правоохранительной деятельности: взаимодействие науки, нормотворчества и практики: сборник материалов III Всероссийской научно-практической конференции молодых ученых. 2020. С. 448-450 (0,1 п.л.).